International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 86 - 90, 2013, ISSN: 2319–8656

Evolving CSP Algorithm in Predicting the Path Loss of Indoor Propagation Models

Anuj Agrawal
PEC University of Technology,
Chandigarh, India

Abstract: Constraint programming is the study of system which is based on constraints. The solution of a constraint satisfaction problem is a set of variable value assignments, which satisfies all members of the set of constraints in the CSP. In this paper the application of constraint satisfaction programming is used in predicting the path loss of various indoor propagation models using chronological backtrack algorithm, which is basic algorithm of CSP. After predicting the path loss at different set of parameters such as frequencies (f), floor attenuation factor (FAF), path loss coefficient (n), we find the optimum set of parameter frequency (f), floor attenuation factor (FAF), path loss coefficient(n) at which the path loss is minimum. The Branch and bound algorithm is used to optimize the constraint satisfaction problem.

Keywords: Path Loss, Indoor Propagation Model, CSP Algorithm, Attenuation Factor.

1. INTRODUCTION

Various research into adaptive algorithm has concerned to find the heuristics which is best suited for solving particular problems from a set of completely specified heuristics. In last few years, the constraint satisfaction programming (CSP) has attracted high attention among experts from many years because of its potential for solving problems. The constraint satisfaction programming approach has been widely used in many academics and research parlance to tackle wide range of search problem. It is defined by finite set of variables, a set of domain and constraints [1]. All CSPs are characterized by the inclusion of a finite set of variables; a set of domain values for each variable; and a set of constraints that are only satisfied by assigning particular domain values to the problem's variables [2]. The CSP deals with the set of values from its domain to the variable in order that no constraint is violated.

A CSP problem includes some variables, and valid values for those variables (we call it domain of the variables) and conflict tables. We must find a solution to assign values to all the variables and those values must satisfy the conflict tables [3]. There are currently two branches of constraint programming, namely constraint satisfaction and constraint solving.

Constraint satisfaction deals with the problem defined over finite domain, on the other hand constraint solving algorithm are based on mathematical techniques. The constraint satisfaction programming (CSP) offers its basic algorithm like backtracking and branch and bound algorithm to solve and optimize the problem. Constraints satisfaction algorithm can be viewed as an iterative procedure that repeatedly assigns domain value to the variables [4].

In this paper problem of finding the path loss of various Empirical indoor wireless propagation models in different environment has been stated as a CSP (constraint satisfaction problem) and has been solved by chronological backtracking algorithm. The branch and bound algorithm then used to optimize the constraint satisfaction problem.

Importance of propagation model is discussed in section II. In section III, methodology and basic algorithm of CSP is explained. Result of indoor model is discussed in section IV.

2. PROPAGATION MODEL

Nowadays cellular phones are used widely for the communication. The number of people using cell phone increases rapidly. Therefore, for an indoor environment an efficient planning and development is surely essential. For the design of indoor wireless services the knowledge of the signal propagation in different environment is demanded. The need for high capacity networks, estimating coverage accurately has become extremely important. Therefore, for more accurate design, signal strength measurement and the path loss measurement must be taken into consideration. Propagation models are used extensively in network planning, particularly for conducting feasibility studies and during initial deployment. Propagation models in wireless communication have focused on predicting the average received signal strength at a given distance from the transmitter as well as the variability of the signal strength in close proximity to a particular location. Propagation models that predict the mean signal strength for an arbitrary transmitter – receiver separation distance are useful in estimating the radio coverage area of transmitter. Propagation model that characterize the rapid fluctuation of the received signal strength over very short travel distances or short time duration are called small scale or fading models. As mobile moves over very small distances, the instantaneous received signal strength may fluctuate rapidly giving rise to small scale fading [5].

These models can be broadly categorized into three types: empirical, deterministic and stochastic. Empirical models are based on

observation and measurement alone. These are mainly used to predict path loss [6]. Empirical models use measurement data to model a path loss equation. To conceive these models, a relationship is found between the received signal strength and other parameters such as distance, path loss exponent, floor loss attenuation factor. The main complexity to model indoor propagation channel is its sensitiveness to indoor environment and less probability of line-of-sight.

In this paper, the concept of constraint satisfaction programming has been implemented on indoor wireless propagation models in order to predicting and optimizing the propagation loss.

Two types of partitions in a building are very important hard and soft partitions. Hard partitions are immobile structures formed as a part of building. Soft partitions can be moved and do not span from the floor to the ceiling. One slope model is the simplest model for determining the path loss in indoor propagation. But it uses distance only to calculate the losses. It does not count floor attenuation, wall attenuation in calculation. It is found that penetration loss due to floor decreases as number of floors increase [5].

Two indoor models, distance dependent path loss model and floor attenuation factor path loss model have been developed. These models have been developed based on the number of floors between transmitter and receiver. The path loss depends upon different obstacles between transmitter and receivers.

3. METHODOLOGY OF CSP

Constraint satisfaction problems (CSPs) representing problems to form a class of models that have a common properties, a set of variables and a set of constraints. A solution to a CSP is a set of variable value assignments, which satisfies all members of the set of constraints in the CSP. In some situations, it is not possible to find a solution satisfy all the constraints belonging to a CSP. Such problems are termed as over constrained problems [7]. The algorithms or techniques that use in constraint satisfaction depend on the kind of constraint being considered. The two algorithms of CSP, chronological backtracking and branch and bound which are used to solve and optimize the wireless empirical propagation models are explained as below:-

Backtracking algorithm:

Backtracking is the basic algorithm to solve CSP. In every step, find a valid value to assign to current variable. If a valid value is found, assign it to current variable and go to next step. If there's no any valid value, back-track to the last variable to assign another value that can lead to the success of finding valid value for current variable [3]. The term backtracking search is used for a depth-first search that chooses values for one variable at a time and backtracks when a variable has no legal values left to assign. In context with the wireless empirical propagation model, we have different types of variables, such as frequency (f), distance (d), path loss exponent (n) etc. After implementation of the backtrack algorithm, we find the path loss of empirical propagation model at different set Frequency(f), distance (d), path loss exponent (n) and floor attenuation factor (FAF). Now after finding the path loss for different set of parameters, we have to find that particular set of parameter at which propagation loss is minimum. For this optimization CSP provides an optimization algorithm called branch and bound algorithm which may be explained as below.

Branch and Bound Algorithm:

A constraint satisfaction optimization problem (CSOP) is defined as CSP, together with an optimization function f. So constraint satisfaction optimization problem is written as: (X, D, C, f) where (X, D, C) represent CSP with a set of variables (X), domain (D) and constraints(C) and f is the optimization function. A bound is nothing but a global variable which is defined according to the minimization or maximization problem, it depends upon the case that either problem needs minimum or maximum value of the function [4]. The branch and bound algorithm in empirical wireless propagation models is used to find that particular set of frequency(f), the distance (d), path loss exponent (n) and floor attenuation factor (FAF) at which propagation loss is minimum. After all the variables are labeled the calculated value of path loss is taken as the f value in branch and bound algorithm. This f value in branch and bound algorithm is compared with the estimated value of the global variable (bound), and if this computed f value is less than the value of the existing bound, it will become the new bound. This procedure will carry on until and unless a minimum value is found and reverse of this procedure is used if we have to find the maximum value [4].

A constraint satisfaction problem is defined as tuple {X,D,C} where,

- X is a finite set of variables,
- D is a finite set of domains, one domain is assigned for each variable, and
- C is the finite set of constraints that restrict certain value assignments [8].

Domains of variables are: frequency, distance, path loss exponent and floor attenuation factor. Constraint is the path loss.

4. RESULT & DISCUSSION

Among numerous propagation models, the following are the most significant ones. The indoor propagation models are:

i. ITU indoor propagation model
ii. Distance dependent path loss model
iii. Floor attenuation factor path loss model

i. ITU indoor propagation model:

Let us analyse the indoor propagation model by taking an example of ITU indoor propagation model. It is also known as ITU model for indoor attenuation. It is a radio propagation model that estimates the path loss inside a room or a closed area inside a building. This model is applicable for the frequency range of 900 MHz to 5.2 GHz. The ITU indoor path loss model is defined as,

$$L = 20 \log f + N \log d + Pf(n) - 28 \quad (1)$$

Where,

N is the distance power loss coefficient.
n is the number of floors between the transmitter and receiver.
Pf (n) is the floor loss penetration factor

For series 1:

f(MHz)	d(m)	N	Pf
915	1-5	1	30

For series 2:

f(MHz)	d(m)	N	Pf
915	1-5	1	33

For series 3:

f(MHz)	d(m)	N	Pf
1900	1-5	1	30

For series 4:

f(MHz)	d(m)	N	Pf
2400	1-5	1	30

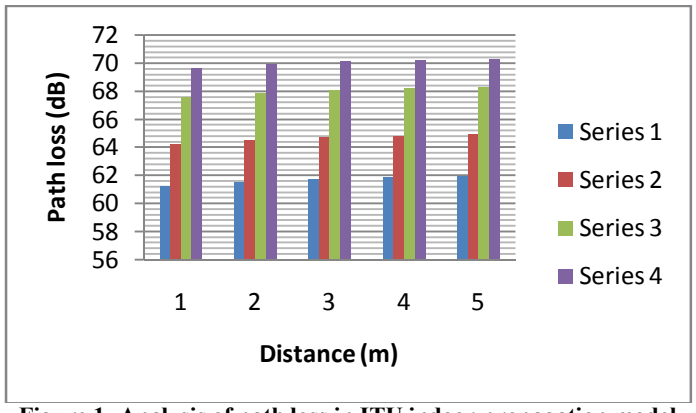


Figure 1- Analysis of path loss in ITU indoor propagation model

From the graphical analysis of figure 1 it can be concluded that the path loss is increased as the distance is increase, as well as floor loss penetration factor increase. It is clear that there is a high increment in the path loss when frequency is changes from 915 MHz to 2400 MHz.

ii. Distance dependent path loss model:

A model used in [9] shows that mean path loss increases exponentially with distance, i.e.,

$$\overline{PL}(d) \propto (\frac{d}{d_0})n \qquad (2)$$

Where $\overline{PL}$ is the mean path loss and n is the mean path loss exponent which indicates the path loss increases exponentially with distance. Absolute mean path loss in decibels is defined as the addition of the path loss at a reference distance d0 and some additional path loss in decibels.

$$\overline{PL}(d)[dB] = PL(d0)[dB] + 10 \text{ X } n \text{ X } \log10(\frac{d}{d_0}) \qquad (3)$$

For this, reference distance is chosen as 1 m and assume that PL(d0) is due to free space propagation from the transmitter to a 1 m reference distance. This leads to 31.67 dB path loss at 915 MHz over a reference distance free space path. The value of n depends on the specific propagation environment. For example, in free space, n is equal to 2, and when obstructions are present, n will have larger value. Table [5] lists path loss exponent obtained in different mobile radio environment.

Table 1. Path loss exponent in different mobile radio environment

Environment	Path Loss Exponent, *n*
Free space	2
Urban are cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

For series 1:

f(MHz)	d(m)	n
915	1-5	2

For series 2:

f(MHz)	d(m)	n
915	1-5	4

For series 3:

f(MHz)	d(m)	n
1900	1-5	4

For series 4:

f(MHz)	d(m)	n
2400	1-5	2

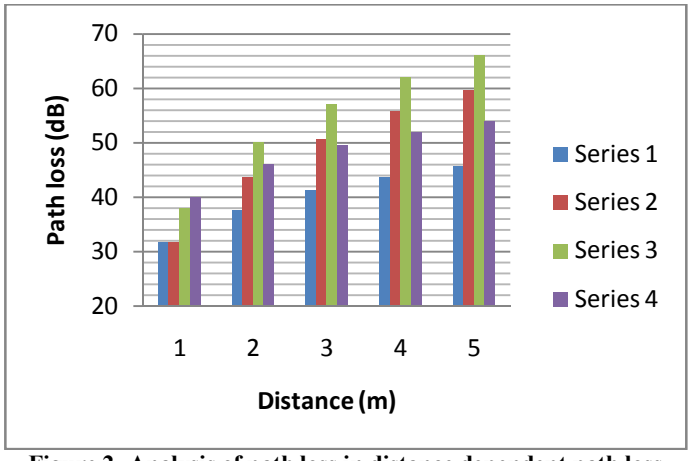


Figure 2- Analysis of path loss in distance dependent path loss model

From the figure 2, it is clear that the mean path loss in distance dependent path loss model increases exponentially with distance. It can also be seen that it is depends on the path loss exponent. The value of n depends on the specific propagation environment.

iii. *Floor attenuation factor path loss model*:

The path loss in multi-floored environments is predicted by a mean path loss exponent that is a function of the number of floors between transmitter and receiver. The value of path loss exponent n (multifloor) is taken from [5].

$$\overline{PL}(d)[dB] = PL(d0)[dB] + 10 \text{ X } n(\text{multifloor}) \text{ X } \log10(\frac{d}{d_0}) \quad (4)$$

The path loss in same floor environment is predicted by a constant floor attenuation factor (in dB). FAF is a function of the number of floors and building type. This FAF is basically added to the mean path loss predicted by a path loss model which uses the same floor path loss exponent for a particular building type. The value of path loss exponent n(same floor) is taken from [5].

$$\overline{PL}(d)[dB] = PL(d0)[dB] + 10 \text{ X } n(\text{same floor}) \text{ X } \log10(\frac{d}{d_0}) + FAF[dB] \quad (5)$$

The attenuation between one floor of the building is greater than the incremental attenuation caused by each additional floor. The average attenuation factors for an identical number of floors between the transmitter and receiver for the two environments differ by 3-8 dB [9].

There are two examples of measuring the path loss with the use of two different models through two floors and three floors building respectively.

For two floors building, the mean path loss exponent for same floor measurement is n = 3.27 and the average floor attenuation factor is FAF = 18.7, the mean path loss exponent for two-floor measurement is n = 5.04. The frequency and reference distance is chosen as 915 MHz and 1 m respectively. Then at a seperation of d = 30m, the predicted path loss is

Using (5),
$\overline{PL}(30)[dB]$ = PL(1m)[dB] + 10 X 3.27(same floor) X log10(30) + 18.7[dB] = 98.67dB

Or using (4),
$\overline{PL}(30)[dB]$ = PL(1m)[dB] + 10 X 5.04(multifloor) X log10(30) = 106.12dB

For three floors building, the mean path loss exponent for same floor measurement is n = 3.27 and the average floor attenuation factor is FAF = 24.4, the mean path loss exponent for three-floor measurement is n = 5.22. The frequency and reference distance is chosen as 915 MHz and 1 m respectively. Then at a seperation of d = 30m, the predicted path loss is

Using (5),
$\overline{PL}(30)[dB]$ = PL(1m)[dB] + 10 X 3.27(same floor) X log10(30) + 24.4[dB] = 104.37dB

Or using (4),
$\overline{PL}(30)[dB]$ = PL(1m)[dB] + 10 X 5.22(multifloor) X log10(30) = 108.78dB

So it is clear from the above explanation that the average attenuation factors for an identical number of floors between the transmitter and receiver for the two buildings differ by 3-8 dB.

5. COMPARISON BETWEEN INDOOR MODELS

In ITU indoor model, as the frequency increases the path loss also increases. Initially losses are high at high frequency but as the partition increases the loss rate is low as compared to at low frequency. The more partition causes the less loss rate. Because of that there is not much variation in lsss for far end partition. The distance dependent path loss model is basically relying on the environment we are working in, because there is a different path loss exponent for a different indoor environment. This model is not suitable if we are taking a wall effect or floor effect. Floor attenuation factor path loss model is the most appropriate model which can be used in predicting the path loss in indoor environment. It uses the two different models mutifloor and same floor environment. Both have different mean path loss exponent. Floor attenuation factor model is most affected by partitions. The attenuation between one floor of the building is greater than the incremental attenuation caused by each additional floor. So it is useful for multi floor building, mainly for the building having more than three floors.

6. CONCLUSION

In the first part of this paper, I briefly introduced about constraint satisfaction, which provides a general basis for constraint satisfaction algorithm. In this paper the various wireless empirical propagation model has been solved at 915 MHz in different environment to find the path loss using the constraint satisfaction algorithm. The models are based on a simple dn exponential path loss vs. distance relationship. I also discussed the main technique to solve CSP, constraint satisfaction optimization algorithm to optimize the different empirical propagation models to find the parameters frequency, distance, path loss exponent, floor attenuation factor at which the path loss is minimum. The models have been shown to be more accurate when considering the different buildings and different environment within the same building separately

7. REFERENCES

[1] Tope R. Karem, H. Anthony Chan, “A low cost design of next generation sonnet/sdh network with multiple constraint”, IEEE, National Research Foundation, 2007.

[2] Stuart Bain, John Thornton, Abdul Sattar, “Evolving algorithm for constraint satisfaction”, IEEE, pp. 265-272, 2004.

[3] Tianbing Lin, Scott Goodwin, "CSP: definition, creation, and algorithms".

[4] Nagendra Sah and Amit Kumar, "CSP algorithm in predicting and optimizing the path loss of wireless empirical propagation models", International Journal of Computer and Electrical Engineering, vol. 1, no. 4, pp. 464-472, October 2009.

[5] Theodore S. Rappaport, "Wireless communications: principles and practice", Second Eddition, PHI Learning Private Limited, 2008.

[6] V.S. Abhayawardhana, I.J. Wassell, D. Crosby, M.P. Sellars, M.G. Brown, "Comparison of Empirical propagation path Loss Models for Fixed Wireless Access Systems", IEEE, 2005.

[7] Srinivas Padmanabhuni, "Extended analysis of intelligent backtracking algorithms for the maximal constraint satisfaction problem", In the proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineernig, pp. 1710-1715, May 1999.

[8] J.I. van Hemert, "Evolving binary constraint satisfaction problem instances that are difficult to solve", National Research Institute for Mathematics and Computer Science, IEEE, pp. 1267-1273, 2003.

[9] Scott Y. Seidel, Theodore S. Rappaport, "914 MHz path loss prediction models for indoor wireless communications in multifloored buildings", In the proceeding of IEEE Transactions on Antennas and Propagation, vol. 40, no. 2, pp. 207-217, Feb 1992

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 91 - 93, 2013, ISSN: 2319–8656

RW-CLOSED MAPS AND RW-OPEN MAPS IN TOPOLOGICAL SPACES

M.Karpagadevi ,
Karpagam College of Engineering,
Coimbatore, India

A.Pushpalatha
Government Arts College,
Udumalpet, India

Abstract: In this paper we introduce rw-closed map from a topological space X to a topological space Y as the image of every closed set is rw-closed and also we prove that the composition of two rw-closed maps need not be rw-closed map. We also obtain some properties of rw-closed maps.
Mathematics Subject Classification: 54C10

Keywords: rw-closed maps, rw-open maps.

---

1. INTRODUCTION

Generalized closed mappings were introduce and studied by Malghan[5].wg-closed maps and rwg-closed maps were introduced and studied by Nagaveni[6].Regular closed maps,gpr-closed maps and rg-closed maps have been introduced and studied by Long[4], Gnanambal[3] and Arockiarani[1] respectively.

In this paper, a new class of maps called regular weakly closed maps (briefly, rw-closed) maps have been introduced and studied their relations with various generalized closed maps. We prove that the composition of two rw-closed maps need not be rw-closed map. We also obtain some properties of rw-closed maps.

S.S. Benchalli and R.S Wali [2] introduced new class of sets called regular weakly - closed (briefly rw - closed) sets in topological spaces which lies between the class of all w - closed sets and the class of all regular g - closed sets.

Throughout this paper (X, τ) and (Y, σ) (or simply X and Y) represents the non-empty topological spaces on which no separation axiom are assumed, unless otherwise mentioned. For a subset A of X, cl(A) and int(A) represents the closure of A and interior of A respectively.

2. PRELIMINARIES

In this section we recollect the following basic definitions which are used in this paper.

Definition 2.1 [2]: A subset A of a topological space (X,τ) is called rw-closed (briefly rw-closed) if $cl(A) \subseteq U$, whenever $A \subseteq U$ and U is regular semiopen in X.

Definition 2.2 [7]: A subset A of a topological space (X,τ) is called regular generalized closed (briefly rg-closed) if $cl(A) \subseteq U$ whenever $A \subseteq U$ and U is regular open in X.

Definition 2.3 [9]: A subset A of a topological space (X,τ) is called weakly closed (briefly w-closed) if $cl(A)) \subseteq U$ whenever $A \subseteq U$ and U is semi open in X.

Definition 2.4 [7] :A map f: $(X, \tau) \to (Y, \sigma)$ from a topological space X into a topological space Y is called rg continuous if the inverse image of every closed set inY is rg-closed in X.

Definition 2.5 [9] :A map f: $(X, \tau) \to (Y, \sigma)$ from a topological space X into a topological space Y is called w-continuous if the inverse image of every closed set in Y is w-closed in X.

Definition 2.6 [5]: A map f: $(X, \tau) \to (Y, \sigma)$ is called g-closed if f(F) is g-closed in (Y, σ) for every closed set F of (X, τ).

Definition 2.7 [8]: A map f: $(X, \tau) \to (Y, \sigma)$ is called w-closed if f(F) is w-closed in (Y, σ) for every closed set F of (X, τ).

Definition 2.8 [1]:A map f: $(X, \tau) \to (Y, \sigma)$ is called rg-closed if f(F) is rg-closed in (Y, σ) for every closed set F of (X, τ).

Definition 2.9 [10]:A map f: $(X, \tau) \to (Y, \sigma)$ is called g-open if f(U) is g-open in (Y, σ) for every open set U of (X, τ).

Definition 2.10 [8]:A map f: $(X, \tau) \to (Y, \sigma)$ is called w-open if f(U) w-open in (Y, σ) for every open set U of (X, τ).

Definition 2.11[1]:A map f: $(X, \tau) \to (Y, \sigma)$ is called rg-open if f(U) rg-open in (Y, σ) for every open set U of (X, τ).

3. Rw-closed maps

We introduce the following definition

Definition : 3.1 A map f : (X, τ) → (Y, σ) is said to be regular weakly (briefly rw-closed) if the image of every closed set in (X, τ) is rw-closed in (Y, σ)

Theorem: 3.2 Every closed map is rw-closed map but not conversely.
Proof: The proof follows from the definitions and fact that every closed set is rw-closed.

Remark: 3.3 The converse of the above theorem need not be true as seen from the following example.
Example : 3.4 Consider X=Y={a,b,c} with topologies τ = {X, ϕ, {c}} and σ = { Y, ϕ, {a}, {b},{a,b}}. Let f: (X, τ) → (Y, σ) be the identity map. Then this function is rw-closed but not closed as the image of closed set {a,b} in X is {a,b} which is not closed set in Y.

Theorem: 3.5 Every rw-closed map is rg-closed map but not conversely.
Proof: The proof follows from the definitions and fact that every rw-closed set is rg-closed.

Remark: 3.6 The converse of the above theorem need not be true as seen from the following example.

Example : 3.7 Consider X=Y={a,b,c,d} with topologies τ = {X, ϕ, {b},{a,b,d}} and σ = {Y,ϕ, {a}, {b},{a,b},{a,b,c}}. Let f: (X,τ) → (Y,σ) be the identity map. Then this function is rg-closed but not rw-closed as the image of closed set {c} in X is {c} which is not rw-closed set in Y.

Theorem: 3.8 Every w-closed map is rw-closed map but not conversely.
Proof: The proof follows from the definitions and fact that every w-closed set is rw-closed.

Remark: 3.9 The converse of the above theorem need not be true as seen from the following example.
Example: **3.10** Consider X=Y= {a,b,c} with topologies τ = {X, ϕ, {c}} and σ = {Y,ϕ, {a}, {b},{a,b}}. Let f : (X, τ) → (Y, σ) be the identity map. Then this function is rw-closed but not w-closed as the image of closed set {a,b} in X is {a,b} which is not closed set in Y.
Theorem: 3.11 A map f: (X,τ) → (Y,σ) is rw-closed if and only if for each subset S of (Y,σ) and each open set U containing $f^{-1}(S) \subset U$, there is a rw-open set of (Y, σ) such that S ⊂ V and $f^{-1}(V) \subset U$.
Proof: Suppose f is rw-closed. Let S ⊂ Y and U be an open set of (X,τ) such that $f^{-1}(S) \subset U$. Now X-U is closed set in (X,τ). Since f is rw-closed, f(X-U) is rw-closed set in (Y,σ). Then V=Y- f(X-U) is a rw-open set in (Y,σ). Note that $f^{-1}(S) \subset U$ implies S ⊂ V and $f^{-1}(V) = X - f^{-1}(f(X-U)) \subset X-(X-U) = U$. That is $f^{-1}(V) \subset U$.

For the converse, let F be a closed set of (X,τ). Then $f^{-1}(f(F)^c) \subset F^c$ and F^c is an open set in (X, τ). By hypothesis, there exists a rw-open set V in (Y,σ) such that $f(F)^c \subset V$ and $f^{-1}(V) \subset F^c$ and so $F \subset (f^{-1}(V))^c$. Hence $V^c \subset f(F) \subset f(((f^{-1}(V))^c) \subset V^c$ which implies $f(V) \subset V^c$. Since V^c is rw-closed, f(F) is rw-closed. That is f(F) rw-closed in (Y,σ) and therefore f is rw-closed.
Remark: 3.12 The composition of two rw-closed maps need not be rw-closed map in general and this is shown by the following example.
Example: 3.13 Consider X=Y= {a,b,c} with topologies τ ={X ,ϕ, {b},{a,b}}, σ ={Y,ϕ, {a}, {b},{a,b}}, η = {Z, ϕ, {a}, {c},{a,c}}. Define f: (X,τ) → (Y,σ) by f(a) = a, f(b) = b and f(c)=c and g : (Y,σ)→ (Z, η) be the identity map. Then f and g are rw-closed maps but their composition g ° f : (X,τ) → (Z, η) is not rw-closed map because F={c} is closed in (X,τ) but g ° f({a}) = g(f({c})) = g({c}) = {c} which is not rw-closed in (Z, η).
Theorem: 3.14 If f : (X, τ) → (Y, σ) is closed map and g : (Y,σ)→ (Z, η) is rw-closed map, then the composition g ° f : (X,τ) → (Z, η) is rw-closed map.
Proof: Let F be any closed set in (X,τ). Since f is closed map, f (F) is closed set in (Y,σ). Since g is rw-closed map, g (f (F)) is rw-closed set in (Z, η). That is g ° f(F) = g(f(F)) is rw-closed and hence g ° f is rw-closed map.
Remark: 3.15 If f : (X, τ) → (Y, σ) is rw-closed map and g : (Y,σ)→ (Z, η) is closed map, then the composition need not be rw-closed map as seen from the following example.
Example: 3.16 Consider X=Y=Z= {a,b,c} with topologies τ ={X ,ϕ, {b},{a,b}}, σ ={Y,ϕ, {a}, {b},{a,b}}, η = {Z, ϕ, {a}, {c},{a,c}}. Define f: (X,τ) → (Y,σ) by f (a) = a, f(b) = b and f(c)=c and g : (Y,σ)→ (Z, η) be the identity map. Then f is rw-closed map and g is a closed map but their composition g ° f : (X,τ) → (Z, η) is not rw-closed map since for the closed set {c}in (X,τ) but g ° f({c}) = g(f({c})) = g({c}) = {c} which is not rw-closed in (Z, η).
Theorem: 3.17 Let (X,τ), (Z,η) be topological spaces and (Y,σ) be topological spac where every rw-closed subset is closed. Then the composition g ° f : (X,τ) → (Z, η) of the rw-closed maps f: (X,τ) → (Y,σ) and g : (Y,σ)→ (Z, η) is rw-closed.
Proof: Let A be a closed set of (X,τ). Since f is rw-closed, f (A) is rw-closed in (Y,σ). Then by hypothesis f (A) is closed. Since g is rw-closed, g (f (A)) is rw-closed in (Z,η) and g (f (A)) = g ° f (A). Therefore g ° f is rw-closed.
Theorem: 3.18 If f: (X,τ) → (Y,σ) is g-closed, g: (Y,σ)→ (Z,η) be rw-closed and (Y,σ) is $T_{1/2}$ – space then their composition g ° f: (X,τ) → (Z,η) is rw-closed map.
Proof: Let A be a closed set of (X,τ). Since f is g-closed, f (A) is g-closed in (Y,σ). Since g is rw-closed, g (f (A)) is rw-closed in (Z,η) and g (f (A)) = g ° f (A).Therefore g ° f is rw-closed.

Theorem: 3.19 Let **f**: (X,τ) → (Y,σ) and g: (Y,σ)→ (Z,η) be two mappings such that their

composition g ° f: $(X,\tau) \to (Z,\eta)$ be rw-closed mapping. Then the following statements are true.

i) If f is continuous and surjective, then g is rw-closed

ii) If g is rw-irresolute and injective, then f is rw-closed.

iii) If f is g-continuous, surjective and (X,τ) is a $T_{1/2}$ – space, then g is rw-closed.

Proof: i) Let A be a closed set of (Y,σ). Since f is continuous, $f^{-1}(A)$ is closed in
$g \circ f (f^{-1}(A))$ is rw-closed in (Z,η). That is g (A) is rw-closed in (Z,η), since f is surjective. Therefore g is rw-closed.

ii) Let B be a closed set of (X,τ). Since g ° f is rw-closed, g ° f (B) is rw-closed in (Z,η).
Since g is rw-irresolute, $g^{-1}(g \circ f (B))$ is rw-closed set in (Y,σ).That is f (B) is rw-closed in (Y,σ), since f is injective. Therefore f is rw-closed.

iii) Let c be a closed set of (Y,σ). Since f is g-continuous, $f^{-1}(c)$ is g-closed set in (X,τ). Since (X,τ) is a $T_{1/2}$ -space, $f^{-1}(c)$ is closed set in (X,τ). Since g ° f is rw-closed (g ° f) $(f^{-1}(c))$ is rw-closed in (Z,η). That is g(c) is rw-closed in (Z,η), since f is surjective. Therefore g is rw-closed.

4. Rw-open maps

Definition: 4.1 A map f: $(X,\tau) \to (Y,\sigma)$ is called a rw-open map if the image f (A) is
rw-open in (Y,σ) for each open set A in (X,τ)

Theorem: 4.2 For any bijection map f: $(X,\tau) \to (Y,\sigma)$ the following statements are equivalent.

i) $f^{-1} : (Y,\sigma) \to (X,\tau)$ is rw-continuous

ii) f is rw-open map and

iii) f is rw-closed map.

Proof: (i) ⇒ (ii) Let U be an open set of (X,τ). By assumption, $(f^{-1})^{-1}(U) = f(U)$ is rw-open in (Y,σ) and so f is rw-open.

(ii) ⇒ (iii) Let F be a closed set of (X,τ). Then F^c is open set in (X,τ). By assumption
$f(F^c)$ is rw-open in (Y,σ) . That is $f(F^c) = f(F)^c$ is rw-open in (Y,σ) and therefore f(F) is rw-closed in (Y,σ). Hence F is rw-closed.

(iii) ⇒ (i) Let F be a closed set of (X,τ). By assumption, f (F) is rw-closed in (Y,σ). But $f(F) = (f^{-1})^{-1}(F)$ and therefore f^{-1} is continuous.

Theorem: 4.3 A map f: $(X,\tau) \to (Y,\sigma)$ is rw-open if and only if for any subset S of (Y,σ) and any closed set of (X,τ) containing $f^{-1}(S)$, there exists a rw-closed set K of (Y,σ) containing S such that $f^{-1}(K) \subset F$.

Proof: Suppose f is rw-open map. Let $S \subset Y$ and F be a closed set of (X,τ) such that $f^{-1}(S) \subset F$. Now X-F is an open set in (X,τ). Since f is rw-open map, f (X-F) is rw-open set in (Y,σ). Then K=Y- f (X-F) is a rw-closed set in (Y,σ). Note that $f^{-1}(S) \subset F$ implies
$S \subset K$ and $f^{-1}(K) = X - f^{-1}(X-F) \subset X-(X-F) = F$. That is $f^{-1}(K) \subset F$.

For the converse let U be an open set of (X,τ). Then $f^{-1}((f(U))^c) \subset U^c$ and U^c is a closed set in (X,τ). By hypothesis, there exists a rw-closed set K of (Y,σ) such that $(f(U))^c \subset K$ and $f^{-1}(K) \subset U^c$ and so $U \subset (f^{-1}(K))^c$. Hence $K^c \subset f(U) \subset f((f^{-1}(K)))^c$ which implies $f(U) = K^c$. Since K^c is a rw-open, f(U) is rw-open in (Y,σ) and therefore f is rw-open map.

4. REFERENCES

[1] Arockiarani. I, Studies on generalizations of generalized closed sets and maps in topological spaces, Ph.D., Thesis, Bharathiar Univ., Coimbatore, 1997.

[2] Benchalli.S.S and Wali.R.S., On Rω-closed sets in topological spaces, Bull.Malays.math.Sci.Soc(2) 30(2) (2007), 99-110.

[3] Gnanambal Y, On Generalized Pre-regular Closed sets in Topological Spaces, Indian J.Pure Appl.Math.,28(1997), 351-360.

[4] Long P.E, and Herington L.L, Basic properties of Regular Closed Functions, Rend.Cir.Mat.Palermo, 27(1978) , 20-28.

[5] Malghan S.R, Generalized Closed maps, J.Karnatk Univ.Sci.,27(1982), 82-88

[6] Nagaveni N, Studies on Generalizations of Homeomorphisms in Topological spaces, Ph.D., Thesis, Bharathiar University, Coimbatore(1999).

[7] Palaniappan N and Rao K C, Regular generalized closed sets, Kyungpook Math. J. 33(1993), 211-219

[8] Sheik John M, A Study on Generalizations of Closed Sets on Continuous maps in Topological and Bitopological Spaces, Ph.D, Thesis Bharathiar University, Coimbatore,(2002)

[9] Sundaram P and Sheik John M, On w-closed sets in topology, Acta Ciencia Indica 4(2000), 389-392

[10] Sundaram P, Studies on Generalizations of Continuous Maps in Topological Spaces, Ph.D, Thesis, Bharathiar University, Coimbatore,(1991).

[11] Vadivel A and Vairamanickam K, rgα-Closed Sets and rgα-Open Sets in Topological spaces, Int.Journal of Math.Analysis, Vol.3, 2009, no.37, 1803-1819.

[12] Vadivel A and Vairamanickam K, rgα-Closed and rgα-Open Maps in Topological spaces, Int.Journal of Math.Analysis, Vol.4, 2010, no.10, 453-468

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 94 - 98, 2013, ISSN: 2319–8656

A Trusted Integrity verification Architecture for Commodity Computers

Angela Francis
Karunya University
Coimbatore,
India

Renu Mary Daniel
Karunya University
Coimbatore,
India

Vinodh Ewards S.E.
Karunya University
Coimbatore,
India

Abstract: Trust is an indispensable part of the computing environment, the validity of any transaction or information depends heavily on the authenticity of the information source. In this context, many mechanisms for ensuring the authenticity of the information source were developed, including password verification and biometrics. But as the attacks are directed towards the computing platform and the applications running on the computer, all these initial security mechanisms are not sufficient. It is essential to ensure before making a secure transaction that the system is in a good state (or say some authorized state) and maintains its integrity throughout the execution time. The emergence of the Trusted Platform Module (TPM) has added to the security feature of a computer. Mechanisms are in place which guarantee system integrity but very little is known about the state of the applications running on them. We propose a system which notifies the user if the integrity of an application is violated and stops it. Our system also compares the current system state with a known good value to ensure platform integrity.

Keywords: Trust; Trusted Platform Module (TPM); Integrity Measurement; Sealing; Application Security

1. INTRODUCTION

Ensuring trust in cyber space has been a prime concern since the epidemic growth of online transactions and communications. Commodity computers are increasingly used to access banking transactions, sending sensitive e-mails, accessing personal and confidential information from remote systems, where it becomes the prime necessity to assure the user that security sensitive operations executes always on secure and trusted state of system. Authenticity of the information source and non-repudiation can be achieved through many mechanisms like passwords, biometrics, digital signatures and cryptographic protocols. These mechanisms ensure that the user is genuine and authorized to view the information. They also guarantee that the integrity of the information during transmission is maintained. But can we know with absolute certainty that the system with which we are communicating is not malicious? In order to establish trust in computer and verify its existence, it is required to know something more other than the authentication. And what is that more requires understanding of the following: what is meant by trusted system? What are the components involved in it? How to boot the system in trusted state? Does booting the system in trusted state guarantee that system will remain in trusted state while execution? As attacks are directed towards the BIOS, boot loader and kernel, maintaining the system integrity is extremely difficult. To ensure that the system is in a trusted state, the Trusted Computing Base (TCB) of the system should be verifiable. But owing to the enormous code comprising the TCB, is it possible to vouch for the integrity of the system during each transaction?

Trusted Computing (Trusted Computing Group, 2007) aims at establishing trust in commodity computers and the transactions performed by them. TCG's Trusted Platform Module (TPM) (Bajikar, 2002) is a cryptoprocessor chip, that computes the current platform state during boot time. But, TPM is a passive device, it does not notify the user if there is any change in the system state. The values stored by it can be used for later verification with a known good state. Many mechanisms like Tboot (Trusted Boot, 2012) and OSLO (Kauer, 2007) were developed to provide trusted boot, where the platform state will be compared to a set of known good measurements. These mechanisms require a system with Intel TXT or AMD SKINIT instruction and virtualization technology support. Our system makes use of the TPM chip's boot time integrity measurement to check if the system is in a trusted state without any additional requirements.

As TPM does not compute the hash of the applications or services in the system it cannot stop a service or application if it is compromised. So, if the applications and services are running alongside untrusted applications, can we guarantee the genuineness of these applications? They can be targeted and compromised. Thus there is a need to provide isolation to the execution of security sensitive code, so that attacks directed towards it during execution can be thwarted. Flicker (McCune et. al., 2008) is one such project which aimed at providing isolated execution of a security sensitive code by switching from untrusted environment to the minimal trusted environment. It ensures run time integrity of security sensitive code. We propose a system in which the application integrity can be verified before launch and stopped if found to be malicious, thus providing a way to extend trust to the application and service level.

2. BACKGROUND

2.1 Trusted System and Trusted Computing Base

There are various definitions which have been proposed to define "trusted system". Schneider (Shirey, 2007) defines trusted system as, "a system that operates as expected, according to design and policy, doing what is required – despite environmental disruption, human user and operator errors, and attacks by hostile parties – and not doing other things."

According to Neumann's definitions (Neumann, 1995), "an object is trusted if and only if it operates as expected."

An important factor in establishing trust in computer system or any computing device is identifying the *trusted computing base* (TCB). It is a totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy (U.S. Department of Defense, 1990) and critical to its security. Any vulnerability or weakness inside the TCB components may potentially affect the security of whole system and hence system may get compromised, whereas the vulnerabilities or weakness (software or hardware) outside the TCB must not affect the security of system beyond the confined area.

Rushby, (1981) defines the trusted computing base as the combination of *kernel* and *trusted* processes. The trusted processes are special process that are allowed to violate the system's access-control rules.

Whereas Lampson et al. (1992) define the TCB of a computer system as simply *"*a small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security*"*.

The Orange Book (Department of Defense, 1985) further explains that [t]he ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

2.2 Boot Time Integrity

The best time to measure the identity of software code is before it starts execution. The identity of these components can be computed by taking the cryptographic hash of its binary as well as any inputs, libraries or configuration files used, also known as measurements. This requires the identity of all software components participate in the current state of computer namely BIOS, boot loader, and operating system (Gu et. al., 2009) (Parno et. al., 2011). The measurements taken at the clean state of system is termed as golden measurements (or golden images).

The software currently in control of the platform is measured by the software which had control of the platform previously. And the currently running software will measure the next software before it start execution. The process of measurement and execution continues till the system reaches to intended state and a chain of trust (Parno et. al., 2011) is thus established. The raises the fundamental question that, who initiated the chain of trust? It must be an immutable piece of code that initiates the chain of trust and forms the foundational root of trust (Parno et. al., 2011). TPM provides a programme code that serves as the Core Root of Trust for Measurement (CRTM), to initiate the measurement chain.

Once these identities (golden measurements) are measured, it can be used to boot the system in some authorized state known as secure boot and trusted boot. Secure boot assumes that measured software is trustworthy and only ensures a secure initial state i.e. at time t0. An immutable piece of code initiates the chain of trust by measuring the initial BIOS, verify against the golden measurement and execute if found correct else halt. Similarly, the boot chain continues till the kernel.

Whereas in trusted boot (techniques first used by Gasser et. al., 1989) chain of trust initiated by secure hardware (co-processor), it measure the next software, accumulate (or append) the measurement in memory and execute the software. It communicates the current state of system to user via attestation and can prove that system is booted in a known configuration, which enables the user to verify the state and establish trust that no malicious software is running.

2.3 Threat Model

The most vulnerable entry point for attacks are software applications as opposed to operating systems and the platform. Application layer hosts a major part of all vulnerabilities that facilitate cyber crime. As these applications are pervasive, they can be exploited to steal sensitive information. For instance, an ordinary user or an adversary may come across a bug in the application and gain access to privileged information. The attacks are mostly directed towards the information and resources being used by the applications, its users and developers. Since processes share information through shared memory regions, these attacks might be used to compromise the operating system through buffer overflows and invalidated input exploits. Changes made to the kernel may not be easily detected and can cause major damage. Thus before the launch of any security sensitive application platform integrity must be verified and the trust chain must be extended to include the applications and services.

3. RELATED WORK

Web browsers and operating systems do not provide any mechanism by which a user can be sure that the sensitive information is reaching the intended destination unaltered. Software-only protection schemes cannot ascertain the integrity of software since it can be corrupted in many ways like improper installation, upgradation and malware attacks.

Flicker is a secure infrastructure that allows the security-sensitive code to run in complete isolation by utilizing the concept of late launch provided by Intel and AMD processors and Dynamic Root of Trust for Measurement (DRTM) provided by TPM v1.2 chips. Flicker (McCune et. al., 2008) allows application developers to focus on the security of their code without blindly trusting an unverifiable quantity of code executing below. Flicker guarantees that the security sensitive code will execute in isolation without requiring a reboot, a change of OS, or a VMM. It can operate at any time and does not require a new OS or even a VMM.

Adding only a few hundred lines to the TCB, Flicker protects fine granules of security-sensitive code. Due to the frequent use of hardware support for a dynamic root of trust for measurement, Flicker incurs significant performance overhead. In situations with demanding performance, several characteristics of Flicker renders it impractical for use. When Flicker session executes, the user thinks that the system has momentarily hanged. TrustVisor (McCune et. al., 2010) aims to achieve high performance for legacy applications and also to protect small security-sensitive code blocks within a potential malicious environment. A special purpose hypervisor called TrustVisor is developed that invokes the security-sensitive code module without trusting the OS or the applications for isolated execution.

4. PROBLEM STATEMENT

Based on the survey of trusted systems and TPM it is found that they mainly guarantee system integrity and very little is known about the state of the applications running on them. As stated earlier most of the work done for protecting the applications focuses on providing isolation for their execution but do not alert the user if any modification to the application is made. If these modifications or alteration are not known at an early stage and corrected then they may serve as vulnerabilities which can be easily attacked. Further, it should be possible to stop the malicious service or application. TPM being a passive device provides measurement and protected storage, but will not interfere with the execution of applications in the system. It only measures and does not provide a mechanism to verify the system integrity.

5. SYSTEM DESIGN

5.1 Work-flow of the System

When the system boots, TPM measures the integrity of the BIOS, bootloader, operating system, etc. which is stored in the Platform Configuration Registers (PCR) from 0-7 (Bajikar, 2002). These PCRs provide a secure storage and can be used for verifying the integrity of the system with the help of the sealing and unsealing mechanism provided by TPM.

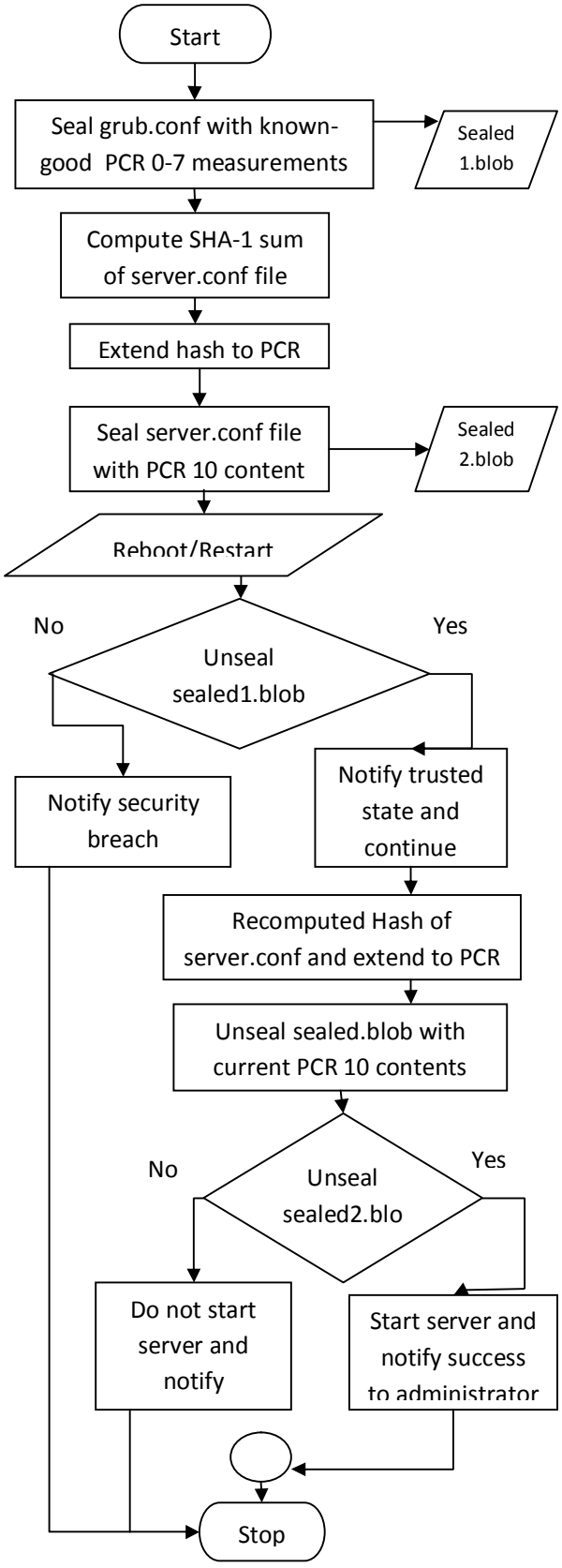


Figure. 1 Work-flow of the System

The same mechanism can be used to verify an application's integrity. We propose a design which notifies a user if any changes are made to the system at every boot and also checks for the integrity of a service or application before it starts.

When the system is in a good state PCR 0-7 have known good measurements. To check for system integrity a system configuration file is sealed with the known good measurements i.e. PCR 0-7. Sealing is a security mechanism provided by the Trusted Platform Module. It allows the data being sealed to be tied to a particular platform state as represented by one or more PCR contents. The Storage Root

Key will be used to encrypt the sealed data and for each sealing and unsealing, SRK password will be prompted by the system. This provides additional security as the private part of the SRK never leaves the TPM chip and is stored in the TPM NV-RAM. Unsealing is possible only if the platform state during unsealing matches the platform state during sealing.

This sealed file is then stored in a secure location. Sealed file in the secure location is attempted to be unsealed using the current PCR 0-7 contents at each system boot. If the unseal operation is successful the output file is written and the administrator is notified that the integrity of the system is maintained. Otherwise, unseal operation fails, output file cannot be written and administrator is notified about the security breach.

Application integrity checking begins by hashing the configuration file of the application or service using the SHA-1 algorithm. The result is then extended to PCR 10 i.e. PCR 10 is updated with the output of the hash and its current value. The following expression denotes the extend operation:

$$PCR \leftarrow Hash\ (PCR \parallel Hash(config\ file))$$

The configuration file is then sealed with the PCR 10 contents, i.e. the clean state measurement of the file.

After sealing the sealed blob will be generated and stored in a secure storage. During system start up, PCRs 0-16 comprising of the static PCRs will be reset to zero. The hash of the configuration file is again computed and extended into PCR 10 and using the current PCR 10 value, unseal operation is attempted. If the configuration file has not been altered, its measurement remains the same. Then, value of PCR 10 during sealing and unsealing remains the same and the sealed file can be successfully unsealed and the service or application is launched. If any modification is made to the configuration file the unseal operation fails, the service is not started and the administrator is notified.

5.2 Experimental Setup

A version 1.2 TPM is required and it must be enabled and activated in the BIOS. The system used for this implementation is HP-Compaq 8100 with Intel Core i5-650 vPro processor. The system is embedded with a TPM. TPM tools and TrouSerS were installed to communicate with the TPM. Our implementation is written in shell script and is assumed to be a part of the Trusted Computing Base (TCB) cause it measures and verifies the application's configuration files before execution. The grub.conf file is sealed with the contents of PCR 0-7 using the following command:

```
tpm_sealdata -i grub.conf -o sealed1.blob -p 0 -p 1 -p 2 -p 3 -p
4 -p 5 -p 6 -p 7
```

The output of the command which is the sealed1.blob file is stored in a secure location viz. a flash drive. Each time a system is booted and before any application or services start the sealed file in the flash drive i.e. sealed1.blob is unsealed using the tpm_unsealdata command.

```
tpm_unsealdata -i sealed1.blob -o unseal1.blob
```

If PCR 0-7 state is not same as it was while sealing then unseal operation fails. The administrator or user is notified about the state of the system.

For measuring and extending the application configuration to a PCR we use TrouSerS Programming (Challener, 2011). The command line arguments provided to the PCR extend program are shown in the following expression:

```
./pcr_extend.exe -p 10 -v `sha1sum app.conf`
```

where, third argument tells which PCR will be extended and the fifth argument is the hash of the configuration file which will be extended. For experimental purpose we use Apache Web Server to verify its integrity before it starts. After extending, the apache.conf file is then sealed with the contents of PCR 10 using the tpm_sealdata command. The command is as follows:

```
tpm_sealdata -i apache.conf -o sealed2.blob -p 10
```

The output of the command which is the sealed file is stored in a secure location viz. a flash drive. Each time a system is booted and before Apache starts the hash of the configuration file is taken and extended to PCR 10, then the sealed file in the flash drive i.e. sealed.blob is unsealed using the tpm_unsealdata command.

```
tpm_unsealdata -i sealed.blob -o unseal.blob
```

If PCR 10 state is not same as it was while sealing then unseal operation fails. The Web server is then stopped and the alteration is notified to the user.

6. RESULTS AND DISCUSSION

One of our design goals for the system was to notify the user if any change is made to the platform and configuration file of the application. The changes made, if notified at an early stage can be corrected and the system will be protected from prospective danger or invasion from attacks. We achieved this by executing a startup script assumed to be a part of the TCB using sealing and unsealing to check for integrity. This increases the size of the TCB by few lines. Currently some

features are still unimplemented such as non-bypassability i.e. the startup script should not be changed by any user.

7. FUTURE WORK AND CONCLUSION

The system was designed to ensure the launch-time integrity of an application or service using the security features provided by the TPM. As the script is assumed to be part of the TCB, we have implemented a simple mechanism for verifying boot-time integrity of the system. Also, we are working towards ensuring the non-bypassability aspect of the system. The script is security critical and can be invoked as the Piece of Application Logic in Flicker (McCune et. al., 2008), to provide isolation during execution.

We have worked towards extending the trust aspect provided by the TPM to the application and services in the system. We have explored the extent to which the chain of trust is currently being made and have designed a system to ensure the integrity of applications before being started.

8. ACKNOWLEDGMENTS

The authors gratefully acknowledge the support of the faculty in Karunya University towards this research.

9. REFERENCES

[1] Trusted Computing Group, Incorporated, 2007. TCG specification architecture overview.

[2] Bajikar, S. 2002. Trusted Platform Module (TPM) based Security on Notebook PCs White Paper. Intel Corporation.

[3] Trusted Boot, sourceforge.net, Sept. 12, 2007. [Online]. Available: http://sourceforge.net/projects/tboot [Accessed: Aug. 10, 2012].

[4] Kauer, B. 2007. OSLO: Improving the Security of Trusted Computing. In Proceedings of 16th USENIX Security Symposium.

[5] McCune, J. M., Parno, B. J., Perrig, A., Reiter, M. K., and Isozaki, H. 2008. Flicker: An Execution Infrastructure for TCB Minimization. In Proceedings of 3rd ACM EuroSys European Conference on Computer Systems, pp. 315-328.

[6] Shirey, R. 2007. RFC 4949 – Internet Security Glossary, Version 2 (IETF).

[7] Neumann, P. G. 1995. Architectures and formal representations for secure systems, SRI Project 6401, Deliverable A002 (Computer Science Laboratory, SRI International).

[8] U.S. Department of Defense. 1990. Glossary of Computer Security Terms (Aqua Book) (National Computer Security Center, Fort Meade).

[9] Rushby, J. 1981. Design and Verification of Secure Systems. In 8th ACM Symposium on Operating System Principles. Pacific Grove, California, US. pp.12–21.

[10] Lampson, B., Abadi, M., Burrows, M., and Wobber E. 1992. Authentication in Distributed Systems: Theory and Practice. ACM Transactions on Computer Systems, on page 6.

[11] Department of Defense trusted computer system evaluation criteria. 1985. DoD 5200.28-STD, In the glossary under entry Trusted Computing Base (TCB).

[12] Gu, J., and Ji, W. 2009. A secure bootstrap based on trusted computing. In International Conference on New Trends in Information and Service Science, IEEE.

[13] Parno, B., McCune, J. M., and Perrig, A. 2011. Bootstrapping Trust in Modern Computers, ISBN 978-1-4614-1459-9, Springer.

[14] Gasser, M., Goldstein, A., Kaufman, C., and Lampson B. 1989. The digital distributed system security architecture. In Proceedings of the National Computer Security Conference.

[15] McCune, J. M., Li, Y., Qu, N., Zhou, Z., Datta, A., Gligor, V., and Perrig, A. 2010. TrustVisor: Efficient TCB Reduction and Attestation. In IEEE Symposium on Security and Privacy, pp. 143-158.

[16] Challener, D. 2011. Programming with TrouSerS. John Hopkins University.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 99 - 108, 2013, ISSN: 2319–8656

On Some New Continuous Mappings in Intuitionistic Fuzzy Topological Spaces

M. Thirumalaiswamy
Department of Mathematics,
NGM College, Pollachi-642001,
Tamil Nadu, India.

K. Ramesh
Department of Mathematics,
NGM College, Pollachi-642001,
Tamil Nadu, India.

Abstract: In this paper we introduce intuitionistic fuzzy almost semipre generalized continuous mappings, intuitionistic fuzzy completely semipre generalized continuous mappings,intuitionistic fuzzy almost semipre generalized closed mappings and intuitionistic fuzzy almost semipre generalized open mappings. Some of their properties are studied.

Keywords: Intuitionistic fuzzy topology, intuitionistic fuzzy point, intuitionistic fuzzy almost semipre generalized continuous mappings, intuitionistic fuzzy completely semipre generalized continuous mappings, intuitionistic fuzzy almost semipre generalized closed mappings and intuitionistic fuzzy almost semipre generalized open mappings.

AMS Subject Classification (2000): 54A40, 03F55.

1. INTRODUCTION

After the introduction of fuzzy sets by Zadeh [15], there have been a number of generalizations of this fundamental concept. Later on, fuzzy topology was introduced by Chang [2] in 1967. The notion of intuitionistic fuzzy sets introduced by Atanassov [1] is one among them. Using the notion of intuitionistic fuzzy sets, Coker [3] introduced the notion of intuitionistic fuzzy topological spaces. Intuitionistic fuzzy semi-pre continuous mappings in intuitionistic fuzzy topological spaces are introduced by Young Bae Jun and SeokZun Song [14]. In this paper we introduce intuitionistic fuzzy almost semi-pre generalized continuous mappings, intuitionistic fuzzy completely semipre generalized continuous mappings, intuitionistic fuzzy almost semipre generalized closed mappings and intuitionistic fuzzy almost semipre generalized open mappings. We investigate some of its properties.

2. PRELIMINARIES

Definition 2.1:[1] Let X be a non-empty fixed set. An intuitionistic fuzzy set (IFS in short) A in X is an object having the form $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$ where the functions $\mu_A: X \to [0,1]$ and $\nu_A : X \to [0,1]$ denote the degree of membership (namely $\mu_A(x)$) and the degree of non-membership (namely $\nu_A(x)$) of each element $x \in X$ to the set A, respectively, and $0 \leq \mu_A(x) + \nu_A(x) \leq 1$ for each $x \in X$. Denote by IFS(X), the set of all intuitionistic fuzzy sets in X.

Definition 2.2: [1] Let A and B be IFSs of the form $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$ and $B = \{\langle x, \mu_B(x), \nu_B(x)\rangle / x \in X\}$. Then

(i) $A \subseteq B$ if and only if $\mu_A(x) \leq \mu_B(x)$ and $\nu_A(x) \geq \nu_B(x)$ for all $x \in X$,
(ii) $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$,
(iii) $A^c = \{\langle x, \nu_A(x), \mu_A(x)\rangle / x \in X\}$,
(iv) $A \cap B = \{\langle x, \mu_A(x) \wedge \mu_B(x), \nu_A(x) \vee \nu_B(x)\rangle / x \in X\}$,
(v) $A \cup B = \{\langle x, \mu_A(x) \vee \mu_B(x), \nu_A(x) \wedge \nu_B(x)\rangle / x \in X\}$.

For the sake of simplicity, we shall use the notation $A = \langle x, \mu_A, \nu_A\rangle$ instead of $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$. Also for the sake of simplicity, we shall use the notation $A = \langle x, (\mu_A, \mu_B), (\nu_A, \nu_B)\rangle$ instead of $A = \langle x, (A/\mu_A, B/\mu_B), (A/\nu_A, B/\nu_B)\rangle$. The intuitionistic fuzzy sets $0_\sim = \{\langle x, 0, 1\rangle / x \in X\}$ and $1_\sim = \{\langle x, 1, 0\rangle / x \in X\}$ are respectively the empty set and the whole set of X.

Definition 2.3: [3] An intuitionistic fuzzy topology (IFT in short) on X is a family τ of IFSs in X satisfying the following axioms:

(i) $0_\sim, 1_\sim \in \tau$,
(ii) $G_1 \cap G_2 \in \tau$, for any $G_1, G_2 \in \tau$,
(iii) $\cup G_i \in \tau$ for any family $\{G_i / i \in J\} \subseteq \tau$.

In this case the pair (X, τ) is called an intuitionistic fuzzy topological space(IFTS in short) and any IFS in τ is known as an intuitionistic fuzzy open set(IFOS in short)in X. The complement A^c of an IFOS A in an IFTS (X, τ) is called an intuitionistic fuzzy closed set (IFCS in short) in X.

Definition 2.4: [3] Let (X, τ) be an IFTS and $A = \langle x, \mu_A, \nu_A\rangle$ be an IFS in X. Then

(i) $int(A) = \cup\{G / G \text{ is an IFOS in X and } G \subseteq A\}$,
(ii) $cl(A) = \cap\{K / K \text{ is an IFCS in X and } A \subseteq K\}$,
(iii) $cl(A^c) = (int(A))^c$,
(iv) $int(A^c) = (cl(A))^c$.

Definition 2.5: [4] An IFS A of an IFTS (X, τ) is an

(i) intuitionistic fuzzy semiclosed set (IFSCS in short) if $int(cl(A)) \subseteq A$,
(ii) intuitionistic fuzzy semiopen set (IFSOS in short) if $A \subseteq cl(int(A))$.

Definition 2.6: [4] An IFS A of an IFTS (X, τ) is an

(i) intuitionistic fuzzy preclosed set (IFPCS in short) if $cl(int(A)) \subseteq A$,
(ii) intuitionistic fuzzy preopen set (IFPOS in short) if $A \subseteq int(cl(A))$.

Note that every IFOS in (X, τ) is an IFPOS in X.

Definition 2.7: [4] An IFS A of an IFTS (X, τ) is an

(i) intuitionistic fuzzy α-closed set (IFαCS in short) if $cl(int(cl(A))) \subseteq A$,
(ii) intuitionistic fuzzy α-open set (IFαOS in short) if $A \subseteq int(cl(int(A)))$,

(iii) intuitionistic fuzzy regular closed set (IFRCS in short) if A = cl(int(A)),
(iv) intuitionistic fuzzy regular open set (IFROS in short) if A = int(cl(A)),
(v) intuitionistic fuzzy β-closed set (IFβCS in short) if int(cl(int(A))) ⊆ A,
(vi) intuitionistic fuzzy β-open set (IFβOS in short) if A ⊆ cl(int(cl(A))).

Definition 2.8: [14] An IFS A of an IFTS (X, τ) is an
(i) intuitionistic fuzzy semipre closed set (IFSPCS for short) if there exists an IFPCS B such that int(B) ⊆ A ⊆ B,
(ii) intuitionistic fuzzy semipre open set (IFSPOS for short) if there exists an IFPOS B such that B ⊆ A ⊆ cl(B).

Definition 2.9: [11] An IFS A is an IFTS (X, τ) is said to be an intuitionistic fuzzysemipre generalized closed set (IFSPGCS) if spcl(A) ⊆ U whenever A ⊆ U and U is an IFSOS in (X, τ). An IFS A of an IFTS (X, τ) is called an intuitionistic fuzzy semipre generalized open set (IFSPGOS in short) if A^c is an IFSPGCS in (X, τ).

Every IFCS, IFSCS, IFαCS, IFRCS, IFPCS, IFSPCS, IFβCS is an IFSPGCS but the converses are not true in general.

Definition 2.10: [9] The complement A^c of an IFSPGCS A in an IFTS (X, τ) is called an intuitionistic fuzzy semipre generalized open set (IFSPGOS for short) in X.

The family of all IFSPGOSs of an IFTS (X, τ) is denoted by IFSPGO(X). Every IFOS, IFSOS, IFαOS, IFROS, IFPOS, IFSPOS, IFβOS is an IFSPGOS but the converses are not true in general.

Definition 2.11: [7] Let α, β ∈ [0, 1] and α+ β ≤ 1. An intuitionistic fuzzy point (IFP for short)$p_{(\alpha,\beta)}$ of X is an IFS of X defined by

$$p_{(\alpha,\beta)}(y) = \begin{cases} (\alpha,\beta) if y = p \\ (0,1) \quad if y \neq p \end{cases}$$

Definition 2.12: [7] Let $p_{(\alpha,\beta)}$ be an IFP of an IFTS (X, τ). An IFS A of X is called an intuitionistic fuzzy neighborhood (IFN for short) of $p_{(\alpha,\beta)}$ if there exists an IFOS B in X such that $p_{(\alpha,\beta)} \in$ B ⊆ A.

Definition 2.13: [8] Let an IFS A of an IFTS (X, τ). Then
(i) αint(A) = ∪{ K / K is an IFαOS in X and K ⊆A}.
(ii) αcl(A) = ∩{ K / K is an IFαCS in X and A ⊆K }.

Definition 2.14: [14] Let A be an IFS in an IFTS (X, τ). Then
(i) sint(A) = ∪{ G / G is an IFSOS in X and G ⊆A },
(ii) scl(A) = ∩{ K / K is an IFSCS in X and A ⊆K }.

Note that for any IFS A in (X, τ), we have $scl(A^c) = (sint(A))^c$ and $sint(A^c) = (scl(A))^c$.

Definition 2.15: [4] Let A be an IFS in an IFTS (X, τ). Then
(i) spint (A) = ∪{G / G is an IFSPOS in X and G ⊆A }.
(ii) spcl (A) = ∩{ K / K is an IFSPCS in X and A ⊆K }.

Note that for any IFS A in (X, τ), we have $spcl(A^c) = (spint(A))^c$ and $spint(A^c) = (spcl(A))^c$.

Definition 2.16: [13] Let A be an IFS in an IFTS (X, τ). Then semipre generalized interior of A (spgint(A) for short) and semipre generalized closure of A (spgcl(A) for short) are defined by
(i) spgint (A) = ∪{ G / G is an IFSPGOS in X and G ⊆A }.
(ii) spgcl(A) = ∩{K / K is an IFSPGCS in X and A⊆K}.

Note that for any IFS A in (X, τ), we have $spgcl(A^c) = (spgint(A))^c$ and $spgint(A^c) = (spgcl(A))^c$.

Definition 2.17: [9] If every IFSPGCS in (X, τ) is an IFSPCS in (X, τ), then the space can be called as an intuitionistic fuzzy semipre $T_{1/2}$ ($IFSPT_{1/2}$ for short) space.

Definition 2.18: [4] Let f be a mapping from an IFTS (X, τ) into an IFTS (Y, σ). Then f is
said to be intuitionistic fuzzy continuous(IF continuous in short) if $f^{-1}(B) \in$ IFO(X) for every B ∈ σ.

Definition 2.19: [4] Let f be a mapping from an IFTS (X, τ) into an IFTS (Y, σ). Then f is said to be
(i) intuitionistic fuzzy semi continuous(IFS continuous in short) if $f^{-1}(B) \in$IFSO(X) for every B ∈ σ,
(ii) intuitionistic fuzzy α- continuous(IFα continuous in short) if $f^{-1}(B) \in$IFαO(X) for every B ∈ σ,
(iii) intuitionistic fuzzy pre continuous(IFP continuous in short) if $f^{-1}(B) \in$IFPO(X) for every B ∈ σ,
(iv) intuitionistic fuzzy β- continuous(IFβ continuous in short) if $f^{-1}(B) \in$IFβO(X) for every B ∈ σ.

Result 2.20:
(i) Every IF continuous mapping is an IFα-continuous mapping and every IFα-continuous mapping is an IFS continuous mapping as well as intuitionistic fuzzy pre continuous mapping. [4]
(ii) Every IF continuous mapping is an IFSG continuous mapping. [5]

Definition 2.21: [14] Let f be a mapping from an IFTS (X, τ) into an IFTS (Y, σ). Then f is said to be an intuitionistic fuzzy semipre continuous (IFSP continuous for short) mapping if $f^{-1}(B) \in$ IFSPO(X) for every B ∈ σ .
Every IFS continuous mapping and IFP continuous mappings are IFSP continuous mapping but the converses may not be true in general.

Definition 2.22: [12]A mapping f : (X, τ) → (Y, σ) is called an intuitionistic fuzzy semipre generalized continuous (IFSPG continuous for short) mappings if $f^{-1}(V)$ is an IFSPGCS in (X, τ) for every IFCS V of (Y, σ).

Definition 2.23: [7] A map f : (X, τ) → (Y, σ) is called an intuitionistic fuzzy closed mapping (IFCM for short) if f(A) is an IFCS in Y for each IFCS A in X.

Definition 2.24: [7] A map f : (X, τ) → (Y, σ) is called an
(i) intuitionistic fuzzy semiopen mapping (IFSOM for short) if f(A) is an IFSOS in Y for each IFOS A in X.
(ii) intuitionistic fuzzy α-open mapping (IFαOM for short) if f(A) is an IFαOS in Y for each IFOS A in X.
(iii) intuitionistic fuzzy preopen mapping (IFPOM for short) if f(A) is an IFPOS in Y for each IFOS A in X.

Definition 2.25: [10]A mapping f : (X, τ) → (Y, σ) is called an intuitionistic fuzzy semipre generalized closed mapping

(IFSPGCM for short) if f(A) is an IFSPGCS in Y for each IFCS A in X.

Definition 2.26: [10] A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy M-semipre generalized closed mapping (IFMSPGCM for short) if f(A) is an IFSPGCS in Y for every IFSPGCS A in X.

Definition 2.27: [6] An IFS A is said to be intuitionistic fuzzy dense (IFD for short) in another IFS B in an IFT (X, τ), if cl(A) = B.

3. INTUITIONISTIC FUZZY ALMOST SEMIPRE GENERALIZED CONTINUOUS MAPPINGS

In this section we have introduced intuitionistic fuzzy almost semipregeneralized continuous mapping and investigated some of its properties.

Definition 3.1: A mapping f : X → Y is said to be an intuitionistic fuzzy almostsemipre generalized continuous mapping (IFaSPG continuous mapping for short) if $f^{-1}(A)$ is an IFSPGCS in X for every IFRCS A in Y.
For the sake of simplicity, we shall use the notation A= ⟨x, (μ, μ), (ν, ν)⟩ instead of A= ⟨x,(a/μ_a, b/μ_b), (a/ν_a, b/ν_b)⟩ in all the examples used in this paper. Similarly we shall use the notation B= ⟨x, (μ, μ), (ν, ν)⟩ instead of B= ⟨x,(u/μ_u, v/μ_v), (u/ν_u, v/ν_v)⟩ in the following examples.

Example 3.2: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.5, 0.4), (0.5, 0.6)⟩,G_2 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping.

Theorem 3.3: Every IF continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IF continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFCS in X, by hypothesis. Since every IFCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.4: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IF continuous mapping.

Theorem 3.5: Every IFS continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFS continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFSCS in X. Since every IFSCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.6: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFS continuous mapping.

Theorem 3.7: EveryIFP continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFP continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFPCS in X. Since every IFPCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.8: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩ andG_2 = ⟨y, (0.5, 0.3), (0.5, 0.7)⟩. Then τ = {0~, G, 1~}andσ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFP continuous mapping.

Theorem 3.9: Every IFβ continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFβ continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFβCS in X. Since every IFβCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.10: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩, G_2 = ⟨x, (0.2, 0.1), (0.8, 0.9)⟩, G_3 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩, G_4 = ⟨x, (0.6, 0.7), (0.4, 0.3)⟩, and G_5 = ⟨y, (0.1, 0.4), (0.9, 0.6)⟩. Then τ = {0~, G_1, G_2, G_3, G_4, 1~}andσ = {0~, G_5, 1~} are IFT on X and Y respectively. Define a mappingf : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFβ continuous mapping.

Theorem 3.11: Every IFSP continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFSP continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFSPCS in X. Since every IFSPCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.12: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩, G_2 = ⟨x, (0.2, 0.1), (0.8, 0.9)⟩, G_3 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩, G_4 = ⟨x, (0.6, 0.7), (0.4, 0.3)⟩, and G_5 = ⟨y, (0.1, 0.4), (0.9, 0.6)⟩. Then τ = {0~, G_1, G_2, G_3, G_4, 1~}andσ = {0~, G_5, 1~} are IFT on X and Y respectively. Define a mapping f: (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFSP continuous mapping.

Theorem 3.13: Every IFα continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFα continuous mapping. Let V be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then f^{-1}(V) is an IFαCS in X. Since every IFαCS is an IFSPGCS, f^{-1}(V) is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.14: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFαcontinuous mapping.

Theorem 3.15: Letf : (X, τ) → (Y, σ) be a mapping where $f^{-1}(V)$ is an IFRCS in X for every IFCS in Y. Then f is an IFaSPG continuous mapping but not conversely.

Proof: Let A be an IFRCS in Y. Since every IFRCS is an IFCS, V is an IFCS in Y. Then $f^{-1}(V)$ is an IFRCS in X. Since every IFRCS is an IFSPGCS, $f^{-1}(V)$ is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.16: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩ and G_2 = ⟨y, (0.5, 0.3), (0.5, 0.7)⟩. Then τ = {$0_{\sim}$, G, $1_{\sim}$}andσ = {$0_{\sim}$, G_2, $1_{\sim}$} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not a mapping as defined in Theorem 3.15.

Theorem 3.17: Every IFSPG continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Assume that f : X → Y be an IFSPG continuous mapping. Let A be an IFRCS in Y. Then A is an IFCS in Y. By hypothesis $f^{-1}(A)$ is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 3.18: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩,G_2 = ⟨x,(0.6, 0.7), (0.4, 0.3)⟩, G_3 = ⟨y, (0.4, 0.2), (0.6, 0.8)⟩ and G_4 =⟨y, (0.4, 0.2), (0.4, 0.8)⟩. Thenτ = {$0_{\sim}$, G_1, G_2, $1_{\sim}$} and σ = {$0_{\sim}$, G_3, G_4, $1_{\sim}$} are IFT on Xand Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFSPG continuous mapping.

Theorem 3.19: Let f : X → Y be a mapping. Then the following are equivalent:
(i) f is an IFaSPG continuous mapping,
(ii) $f^{-1}(A)$ is an IFSPGOS in X for every IFROS A in Y.

Proof: (i) ⇒ (ii) Let A be an IFROS in Y. Then A^c is an IFRCS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGCS in X. That is $f^{-1}(A)^c$ is an IFSPGCS in X. Therefore $f^{-1}(A)$ is an IFSPGOS in X.
(ii) ⇒ (i) Let A be an IFRCS in Y. Then A^c is an IFROS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGOS in X. That is $f^{-1}(A)^c$ is an IFSPGOS in X. Therefore $f^{-1}(A)$ is an IFSPGCS in X. Then f is an IFaSPG continuous mapping.

Theorem3.20: Let $p_{(\alpha, \beta)}$ be an IFP in X. A mapping f : X → Y is an IFaSPGcontinuous mapping if for every IFOS A in Y with $f(p_{(\alpha, \beta)}) \in A$, there exists an IFOS B in X with $p_{(\alpha, \beta)} \in B$ such that $f^{-1}(A)$ is IFD in B.

Proof: Let A be an IFROS in Y. Then A is an IFOS in Y. Let $f(p_{(\alpha, \beta)}) \in A$, then there exists an IFOS B in X such that $p_{(\alpha, \beta)} \in B$ and $cl(f^{-1}(A)) = B$. Since B is an IFOS,$cl(f^{-1}(A))$ is also an IFOS in X. Therefore $int(cl(f^{-1}(A))) = cl(f^{-1}(A))$. Now $f^{-1}(A) \subseteq cl(f^{-1}(A)) = int(cl(f^{-1}(A))) \subseteq cl(int(cl(f^{-1}(A))))$. This implies $f^{-1}(A)$ is an IFβOS in X and hence an IFSPGOS in X. Thus f is an IFaSPG continuous mapping.

Theorem 3.21: Let f : X → Y be a mapping where X is an $IFSPT_{1/2}$ space. Then the following are equivalent:
(i) f is an IFaSPG continuous mapping,
(ii) $spcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$ for every IFSPOS in Y,
(iii) $spcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$ for every IFSOS A in Y,
(iv) $f^{-1}(A) \subseteq spint(f^{-1}(int(cl(A))))$ for every IFPOS A in Y.

Proof: (i) ⇒ (ii) let A be an IFSPOS in Y. Then by Definition 2.8, there exists an IFPOS B such that $B \subseteq A \subseteq cl(B)$ and $B \subseteq int(cl(B))$. Now $cl(int(cl(A))) \supseteq cl(int(cl(B))) \supseteq cl(B) \supseteq A$. Hence $A \subseteq cl(int(cl(A)))$. Therefore $cl(A) \subseteq cl(int(cl(A)))$. But $cl(int(cl(A))) \subseteq cl(A)$. Hence $cl(int(cl(A))) = cl(A)$. This implies cl(A) is an IFRCS in (X, τ). By hypothesis$f^{-1}(cl(A))$ is an IFSPGCS in X and hence $f^{-1}(cl(A))$ is an IFSPCS in X, since X is an $IFSPT_{1/2}$ space. This implies $spcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. Now $spcl(f^{-1}(A)) \subseteq spcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. Thus $spcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$.
(ii) ⇒ (iii) Since every IFSOS is an IFSPOS, proof is similar as in (i) ⇒ (ii).
(iii) ⇒ (i) Let A be an IFRCS in Y. Then A = cl(int(A)). Therefore A is an IFSOS in Y. By hypothesis, $spcl(f^{-1}(A)) \subseteq f^{-1}(cl(A)) = f^{-1}(A) \subseteq spcl(f^{-1}(A))$. Hence $f^{-1}(A)$ is an IFSPCS and hence is an IFSPGCS in X. Thus f is an IFaSPG continuous mapping.
(i) ⇒ (iv) Let A be an IFPOS in Y. Then $A \subseteq int(cl(A))$. Since int(cl(A)) is an IFROSin Y, by hypothesis, $f^{-1}(int(cl(A)))$ is an IFSPGOS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(int(cl(A)))$ is an IFSPOS in X. Therefore $f^{-1}(A) \subseteq f^{-1}(int(cl(A))) = spint(f^{-1}(int(cl(A))))$.
(iv) ⇒ (i) Let A be an IFROS in Y. Then A is an IFPOS in X. By hypothesis, $f^{-1}(A) \subseteq spint(f^{-1}(int(cl(A)))) = spint(f^{-1}(A)) \subseteq f^{-1}(A)$. This implies $f^{-1}(A)$ is an IFSPOS in X and hence is an IFSPGOS in X. Therefore f is an IFaSPG continuous mapping.

Theorem 3.22: Let f : X → Y be a mapping. If f is an IFaSPG continuous mapping, then$spgcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$ for every IFSPOS A in Y.

Proof: Let A be an IFSPOS in Y. Then cl(A) is an IFRCS in Y. By hypothesis$f^{-1}(cl(A))$ is an IFSPGCS in X. Then $spgcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. Now $spgcl(f^{-1}(A)) \subseteq spgcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. That is $spgcl(f^{-1}(A) \subseteq f^{-1}(cl(A))$.

Corollary 3.23: Let f : X → Y be a mapping. If f is an IFaSPGcontinuous mapping, then$spgcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$ for every IFSOS A in Y.

Proof: Since every IFSOS is an IFSPOS, the proof is obvious from the Theorem 3.22.

Corollary 3.24: Let f : X → Y be a mapping. If f is an IFaSPG continuous mapping, then$spgcl(f^{-1}(A)) \subseteq f^{-1}(cl(A))$ for every IFPOS A in Y.

Proof: Since every IFPOS is an IFSPOS, the proof is obvious from the Theorem 3.22.

Theorem 3.25: Let f : X → Y be a mapping. If f is an IFaSPG continuous mapping, then$spgcl(f^{-1}(cl(A))) \subseteq f^{-1}(cl(spint(A)))$ for every IFSPOS A in Y.

Proof: Let A be an IFSPOS in Y. Then cl(A) is an IFRCS in Y and spint(A) = A. By hypothesis,$f^{-1}(cl(A))$ is an IFSPGCS in X. Then $spgcl(f^{-1}(cl(A))) = f^{-1}(cl(A)) \subseteq f^{-1}(cl(spint(A)))$.

Corollary 3.26: Let f : X → Y be a mapping. If f is an IFaSPG continuous mapping, then$spgcl(f^{-1}(cl(A))) \subseteq f^{-1}(cl(spint(A)))$ for every IFSOS A in Y.

Proof: Since every IFSOS is an IFSPOS, the proof is obvious from the Theorem 3.25.

Corollary 3.27: Let f : X → Y be a mapping. If f is an IFaSPG continuous mapping, then $spgcl(f^{-1}(cl(A))) \subseteq f^{-1}(cl(spint(A)))$ for every IFPOS A in Y.

Proof: Since every IFPOS is an IFSPOS, the proof is obvious from the Theorem 3.25.

Theorem 3.28: Let f : X → Y be a mapping. If $f^{-1}(spint(B)) \subseteq spint(f^{-1}(B))$ for every IFS B in Y, then f is an IFaSPG continuous mapping.

Proof: Let B ⊆ Y be an IFROS. By hypothesis, $f^{-1}(spint(B)) \subseteq spint(f^{-1}(B))$. Since B is an IFROS, it is an IFSPOS in Y. Therefore spint(B) = B. Hence $f^{-1}(B) = f^{-1}(spint(B)) \subseteq spint(f^{-1}(B)) \subseteq f^{-1}(B)$. This implies $f^{-1}(B)$ is an IFSPOS and hence an IFSPGOS in X. Thus f is an IFaSPG continuous mapping.

Remark 3.29: The converse of the above theorem is true if B ⊆ Y is an IFROS and X is an $IFSPT_{1/2}$ space.

Proof: Let f be an IFaSPG continuous mapping. Let B be an IFROSin Y. Then $f^{-1}(B)$ is an IFSPGOS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(B)$ is an IFSPOS in X. Therefore $f^{-1}(spint(B)) \subseteq f^{-1}(B) = spint(f^{-1}(B))$. That is $f^{-1}(spint(B)) \subseteq spint(f^{-1}(B))$.

Theorem 3.30: Let f : X → Y be a mapping. If $spcl(f^{-1}(B)) \subseteq f^{-1}(spcl(B))$ for every IFS B in Y, then f is an IFaSPG continuous mapping.

Proof: Let B ⊆ Y be an IFRCS. By hypothesis, $spcl(f^{-1}(B)) \subseteq f^{-1}(spcl(B))$. Since B is an IFRCS, it is an IFSPCS in Y. Therefore spcl(B) = B. Hence $f^{-1}(B) = f^{-1}(spcl(B)) \supseteq spcl(f^{-1}(B)) \supseteq f^{-1}(B)$. This implies $f^{-1}(B)$ is an IFSPCS and hence an IFSPGCS in X. Thus f is an IFaSPG continuous mapping.

Remark 3.31: The converse of the above theorem is true if B ⊆ Y is an IFRCS and X is an $IFSPT_{1/2}$ space.

Proof: Let f be an IFaSPG continuous mapping. Let B be an IFRCS in Y. Then $f^{-1}(B)$ is an IFSPGCS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(B)$ is an IFSPCS in X. Therefore $spcl(f^{-1}(B)) = f^{-1}(B)) \subseteq f^{-1}(spcl(B))$.

Theorem 3.32: The following are equivalent for a mapping f : X → Y where X is an $IFSPT_{1/2}$ space:

(i) f is an IFaSPG continuous mapping,
(ii) $spcl(f^{-1}(A)) \subseteq f^{-1}(\alpha cl(A))$ for every IFSPOS A in Y,
(iii) $spcl(f^{-1}(A)) \subseteq f^{-1}(\alpha cl(A))$ for every IFSOS A in Y,
(iv) $f^{-1}(A) \subseteq spint(f^{-1}(scl(A)))$ for every IFPOS A in Y.

Proof: (i) ⇒ (ii) Let A be an IFSPOS in Y. Then cl(A) is an IFRCS in Y. Hence by hypothesis $f^{-1}(cl(A))$ is an IFSPGCS in X and hence is an IFSPCS in X, since X is an $IFSPT_{1/2}$ space. This implies $spcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. Now $spcl(f^{-1}(A)) \subseteq spcl(f^{-1}(cl(A))) = f^{-1}(cl(A))$. Since cl(A) is an IFRCS, $cl(int(cl(A))) = cl(A)$. Now$spcl(f^{-1}(A)) \subseteq f^{-1}(cl(A)) = f^{-1}(cl(int(cl(A)))) \subseteq f^{-1}(A \cup cl(int(cl(A)))) = f^{-1}(\alpha cl(A))$. Hence $spcl(f^{-1}(A)) \subseteq f^{-1}(\alpha cl(A))$.

(ii) ⇒ (iii) Let A be an IFSOS in Y. Since every IFSOS is an IFSPOS, the proof is obvious.

(iii) ⇒ (i) Let A be an IFRCS in Y. Then A = cl(int(A)). Therefore A is an IFSOS in Y. By hypothesis, $spcl(f^{-1}(A)) \subseteq f^{-1}(\alpha cl(A)) \subseteq f^{-1}(cl(A)) = f^{-1}(A) \subseteq spcl(f^{-1}(A))$. That is $spcl(f^{-1}(A)) = f^{-1}(A)$. Hence$f^{-1}(A)$ is an IFSPCS and hence is an IFSPGCSin X. Thus f is an IFaSPG continuous mapping.

(i) ⇒ (iv) Let A be an IFPOS in Y. Then $A \subseteq int(cl(A))$. Since int(cl(A)) is an IFROS in Y, by hypothesis, $f^{-1}(int(cl(A)))$ is an IFSPGOS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(int(cl(A)))$ is an IFSPOS in X. Therefore $f^{-1}(A) \subseteq f^{-1}(int(cl(A))) = spint(f^{-1}(int(cl(A)))) \subseteq spint(f^{-1}(A \cup int(cl(A)))) = spint(f^{-1}(scl(A)))$. That is $f^{-1}(A) \subseteq spint(f^{-1}(scl(A)))$.

(iv) ⇒ (i) Let A be an IFROS in Y. Then A is an IFPOS in Y. Hence by hypothesis, $f^{-1}(A) \subseteq spint(f^{-1}(scl(A)))$. This implies $f^{-1}(A) \subseteq spint(f^{-1}(A \cup int(cl(A)))) = spint(f^{-1}(A \cup A)) = spint(f^{-1}(A)) \subseteq f^{-1}(A)$. Therefore $f^{-1}(A)$ is an IFSPOS in X and hence it is an IFSPGOS in X. Thus f is an IFaSPG continuous mapping.

Theorem 3.33: Let f : X → Y be a mapping where X is an $IFSPT_{1/2}$ space. If f is an IFaSPG continuous mapping, then $int(cl(int(f^{-1}(B)))) \subseteq f^{-1}(spcl(B))$ for everyB∈ IFRC(Y).

Proof: Let B ⊆ Y be an IFRCS. By hypothesis, $f^{-1}(B)$ is an IFSPGCS in X. Since Xis an $IFSPT_{1/2}$ space, $f^{-1}(B)$ is an IFSPCS in X. Therefore $spcl(f^{-1}(B)) = f^{-1}(B)$. Now $int(cl(int(f^{-1}(B)))) \subseteq f^{-1}(B) \cup int(cl(int(f^{-1}(B)))) \subseteq spcl(f^{-1}(B)) = f^{-1}(B) = f^{-1}(spcl(B))$. Hence $int(cl(int(f^{-1}(B)))) \subseteq f^{-1}(spcl(B))$.

Theorem 3.34: Let f : X → Y be a mapping where X is an $IFSPT_{1/2}$ space. If f is an IFaSPG continuous mapping, then $f^{-1}(spint(B)) \subseteq cl(int(cl(f^{-1}(B))))$ for everyB ∈IFRO(Y).

Proof: This theorem can be easily proved by taking complement in Theorem 3.33.

4. INTUITIONISTIC FUZZY COMPLETELYSEMIPRE GENERALIZED CONTINUOUS MAPPINGS

In this section we have introduced intuitionistic fuzzy completely semipregeneralized continuous mappings and studied some of their properties.

Definition 4.1: A mapping f : X → Y is said to be an intuitionistic fuzzy completelysemipre generalized continuous mapping (IFcSPG continuous mapping for short) iff $f^{-1}(V)$ is an IFRCS in X for every IFSPGCS V in Y.

Theorem 4.2: Every IFcSPG continuous mapping is an IFSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Hence V is an IFSPGCS in Y. Then $f^{-1}(V)$ is an IFRCS in X. Since every IFRCS is an IFSPGCS, $f^{-1}(V)$ is an IFSPGCS in X. Hence f is an IFSPG continuous mapping.

Example 4.3: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y,(0.6, 0.7), (0.4, 0.2)⟩. Then τ = {$0_{\sim}$, G_1, $1_{\sim}$} and σ = {$0_{\sim}$, G_2, $1_{\sim}$} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFSPG continuous mapping but not an IFcSPG continuous mapping.

Theorem 4.4: Every IFcSPG continuous mapping is an IFaSPG continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFRCS in Y. Hence V is an IFSPGCS in Y. Then $f^{-1}(V)$ is an IFRCS in X. Since every IFRCS is an IFSPGCS, $f^{-1}(V)$ is an IFSPGCS in X. Hence f is an IFaSPG continuous mapping.

Example 4.5: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩, G_2 = ⟨x,(0.6, 0.7), (0.4, 0.3)⟩ and G_3 = ⟨y, (0.5, 0.4), (0.5, 0.6)⟩. Then τ = {0~, G_1, G_2, 1~} andσ = {0~, G_3, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPG continuous mapping but not an IFcSPGcontinuous mapping.

Theorem 4.6: Every IFcSPG continuous mapping is an IF continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Hence V is an IFSPGCS in Y. Then f^{-1}(V) is an IFRCS in X and hence an IFCS in X. Hence f is an IF continuous mapping.

Example 4.7: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.6, 0.7), (0.4, 0.2)⟩, G_2 = ⟨y,(0.6, 0.7), (0.4, 0.2)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IF continuous mapping but not an IFcSPG continuous mapping.

Theorem 4.8: Every IFcSPG continuous mapping is an IFS continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Since every IFCS is an IFSPGCS, V is an IFSPGCS in Y. Then f^{-1}(V) is an IFRCS in X. Since every IFRCS is an IFSCS, f^{-1}(V) is an IFSCS in X. Hence f is an IFS continuous mapping.

Example 4.9: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.6, 0.7), (0.4, 0.2)⟩, G_2 = ⟨y,(0.6, 0.7), (0.4, 0.2)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFS continuous mapping but not an IFcSPG continuous mapping.

Theorem 4.10: Every IFcSPG continuous mapping is an IFP continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Hence V is an IFSPGCS in Y. Then f^{-1}(V) is an IFRCS in X, by hypothesis. Since every IFRCS is an IFPCS, f^{-1}(V) is an IFPCS in X. Hence f is an IFP continuous mapping.

Example 4.11: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩, , G_2 = ⟨x,(0.6, 0.7), (0.4, 0.3)⟩ and G_3 = ⟨y, (0.5, 0.4), (0.5, 0.6)⟩. Then τ = {0~, G_1, G_2, 1~} andσ = {0~, G_3, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFP continuous mapping but not an IFcSPG continuous mapping.

Theorem 4.12: Every IFcSPG continuous mapping is an IFSP continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Hence V is an IFSPGCS in Y. Then f^{-1}(V) is an IFRCS in X, by hypothesis. Since every IFRCS is an IFSPCS, f^{-1}(V) is an IFSPCS in X. Hence f is an IFSP continuous mapping.

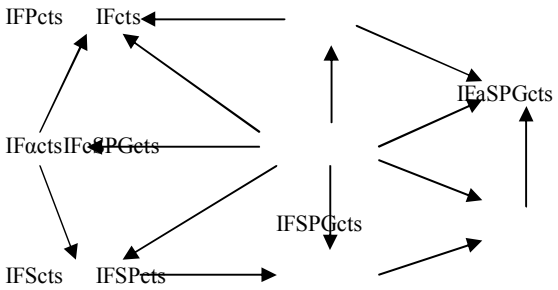
Example 4.13: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.7, 0.8), (0.3, 0.2)⟩, G_2 = ⟨x,(0.6, 0.7), (0.4, 0.3)⟩ and G_3 = ⟨y, (0.5, 0.4), (0.5, 0.6)⟩. Then τ = {0~, G_1, G_2, 1~} andσ = {0~, G_3, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFSP continuous mapping but not an IFcSPGcontinuous mapping.

Theorem 4.14: Every IFcSPG continuous mapping is an IFα continuous mapping but not conversely.

Proof: Letf : (X, τ) → (Y, σ) be an IFcSPG continuous mapping. Let V be an IFCS in Y. Hence V is an IFSPGCS in Y. Then f^{-1}(V) is an IFRCS in X, by hypothesis. Since every IFRCS is an IFαCS, f^{-1}(V) is an IFαCS in X. Hence f is an IFα continuous mapping.

Example 4.15: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.6, 0.7), (0.4, 0.2)⟩, G_2 = ⟨y, (0.6, 0.7), (0.4, 0.2)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFα continuous mapping but not an IFcSPG continuous mapping.

The relation between various types of intuitionistic fuzzy continuity is given in the following diagram. In this diagram cts means continuous mapping.



In the above diagram none of them is reversible.

Theorem 4.16: If f : X → Y is an IFcSPG continuous mapping where X is an $IFSPT_{1/2}$ space, then spcl(f^{-1}(A)) ⊆ f^{-1}(cl(A)) for every IFSPOS A ⊆ Y.

Proof: Let A be an IFSPOS in Y. Then cl(A) is an IFRCS in Y. Hence cl(A) is an IFSPGCS in Y. By hypothesis, f^{-1}(cl(A)) is an IFRCS in X and thus an IFSPCS in X. Therefore spcl(f^{-1}(A)) ⊆spcl(f^{-1}(cl(A))) = f^{-1}(cl(A)).

Corollary 4.17: If f : X → Y is an IFcSPG continuous mapping where X is an $IFSPT_{1/2}$ space, then spcl(f^{-1}(A)) ⊆ f^{-1}(cl(A)) for every IFSOS A ⊆ Y.

Proof: Since every IFSOS is an IFSPOS, the proof is obvious from the Theorem 4.16.

Theorem4.18: A mapping f : X → Y is an IFcSPG continuous mapping if and only if f^{-1}(V) is an IFROS in X for every IFSPGOS V in Y.

Proof: Straightforward.

Theorem 4.19: If a mapping f : X → Y is an IFcSPG continuous mapping, then for every IFP $p_{(\alpha, \beta)}$ ∈ X and for every IFN A of f($p_{(\alpha, \beta)}$), there exists an IFROS B ⊆ X such that $p_{(\alpha, \beta)}$ ∈ B ⊆f^{-1}(A).

Proof: Let $p_{(\alpha, \beta)}$ ∈ X and let A be an IFN of f($p_{(\alpha, \beta)}$). Then there exists an IFOS C in Y such that f($p_{(\alpha, \beta)}$) ∈ C ⊆ A. Since every IFOS is an IFGSPOS, C is an IFSPGOS in Y. Hence by

hypothesis, $f^{-1}(C)$ is an IFROS in X and $p_{(\alpha,\beta)} \in f^{-1}(C)$. Now let $f^{-1}(C) = B$. Therefore $p_{(\alpha,\beta)} \in B = f^{-1}(C) \subseteq f^{-1}(A)$.

Theorem 4.20: If a mapping $f : X \to Y$ is an IFcSPG continuous mapping, then for every IFP $p_{(\alpha,\beta)} \in X$ and for every IFN A of $f(p_{(\alpha,\beta)})$, there exists an IFROS $B \subseteq X$ such that $p_{(\alpha,\beta)} \in B$ and $f(B) \subseteq A$.

Proof: Let $p_{(\alpha,\beta)} \in X$ and let A be an IFN of $f(p_{(\alpha,\beta)})$. Then there exists an IFOS C in Y such that $f(p_{(\alpha,\beta)}) \in C \subseteq A$. Since every IFOS is an IFSPGOS, C is an IFSPGOS in Y. Hence by hypothesis, $f^{-1}(C)$ is an IFROS in X and $p_{(\alpha,\beta)} \in f^{-1}(C)$. Now let $f^{-1}(C) = B$. Therefore $p_{(\alpha,\beta)} \in B \subseteq f^{-1}(A)$. Thus $f(B) \subseteq f(f^{-1}(A)) \subseteq A$. That is $f(B) \subseteq A$.

Theorem 4.21: If a mapping $f : X \to Y$ is an IFcSPG continuous mapping, then $int(cl(f^{-1}(int(B)))) \subseteq f^{-1}(B)$ for every IFS B in Y.

Proof: Let $B \subseteq Y$ be an IFS. Then int(B) is an IFOS in Y and hence an IFSPGOS in Y. By hypothesis, $f^{-1}(int(B))$ is an IFROS in X. Hence $int(cl(f^{-1}(int(B)))) = f^{-1}(int(B)) \subseteq f^{-1}(B)$.

Theorem 4.22: If an injective mapping $f : X \to Y$ is an IFcSPG continuous mapping, then the following are equivalent:

(i) for any IFSPGOS A in Y and for any IFP $p_{(\alpha,\beta)} \in X$, if $f(p_{(\alpha,\beta)})\ q\ A$ then $p_{(\alpha,\beta)} q\, int(f^{-1}(A))$,

(ii) for any IFSPGOS A in Y and for any $p_{(\alpha,\beta)} \in X$, if $f(p_{(\alpha,\beta)})_q A$ then there exists an IFOS B in X such that $p_{(\alpha,\beta)q} B$ and $f(B) \subseteq A$.

Proof: (i) $\Rightarrow$ (ii) Let $A \subseteq Y$ be an IFSPGOS and let $p_{(\alpha,\beta)} \in X$. Let $f(p_{(\alpha,\beta)})\ q\ A$. Then $p_{(\alpha,\beta)q}\ f^{-1}(A)$. By hypothesis, $p_{(\alpha,\beta)\,q} int(f^{-1}(A))$, where $int(f^{-1}(A))$ is an IFOS in X. Let $B = int(f^{-1}(A))$. Since $int(f^{-1}(A)) \subseteq f^{-1}(A)$, $B \subseteq f^{-1}(A)$. Then $f(B) \subseteq f(f^{-1}(A)) \subseteq A$.

(ii) $\Rightarrow$ (i) Let $A \subseteq Y$ be an IFSPGOS and let $p_{(\alpha,\beta)} \in X$. Suppose $f(p_{(\alpha,\beta)})\ q\ A$, then by (ii) there exists an IFOS B in X such that $p_{(\alpha,\beta)q} B$ and $f(B) \subseteq A$. Now $B = f^{-1}(f(B)) \subseteq f^{-1}(A)$. That is $B = int(B) \subseteq int(f^{-1}(A))$. Therefore $p_{(\alpha,\beta)\ q} B$ implies $p_{(\alpha,\beta)\ q}\ int(f^{-1}(A))$.

5. INTUITIONISTIC FUZZY ALMOST SEMIPRE GENERALIZED CLOSED MAPPINGS

In this section we have introduced intuitionistic fuzzy almostsemipregeneralized closed mappings and intuitionistic fuzzy almost semipregeneralized open mappings. We have studied some of their properties.

Definition 5.1: A mapping $f : X \to Y$ is called an intuitionistic fuzzy almost semipregeneralized closed mapping (IFaSPGC mapping for short) if f(A) is an IFSPGCS in Y for each IFRCS A in X.

Example 5.2: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.2, 0.3), (0.8, 0.7) ⟩,G_2 = ⟨y, (0.5, 0.4), (0.5, 0.6)⟩. Then $\tau = \{0_{\sim}, G_{1,}\ 1_{\sim}\}$ and $\sigma = \{0_{\sim}, G_{2,}\ 1_{\sim}\}$ are IFT on X and Y respectively. Define a mapping $f : (X, \tau) \to (Y, \sigma)$ by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping.

Theorem 5.3: Every IFC mapping is an IFaSPGC mapping but not conversely.

Proof: Assume that $f: X \to Y$ is an IFC mapping. Let A be an IFRCS in X. Since every IFRCS is an IFCS, A is an IFCS in X. Then f(A) is an IFCS in Y. Since every IFCS is an IFSPGCS, f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

Example 5.4: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.2, 0.3), (0.8, 0.7) ⟩, G_2 = ⟨y, (0.5, 0.4), (0.5, 0.6)⟩. Then $\tau = \{0_{\sim}, G_{1,}\ 1_{\sim}\}$ and $\sigma = \{0_{\sim}, G_{2,}\ 1_{\sim}\}$ are IFT on X and Y respectively. Define a mapping $f : (X, \tau) \to (Y, \sigma)$ by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFC mapping.

Theorem 5.5: Every IFSC mapping is an IFaSPGC mapping but not conversely.

Proof: Assume that $f : X \to Y$ be an IFSC mapping. Let A be an IFRCS in X. Since every IFRCS is an IFCS, A is an IFCS in X. Then f(A) is an IFSCS in Y. Since every IFSCS is an IFSPGCS, f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

Example 5.6: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.2, 0.3), (0.8, 0.7) ⟩, G_2 = ⟨y, (0.5, 0.4), (0.5, 0.6) ⟩. Then $\tau = \{0_{\sim}, G_{1,}\ 1_{\sim}\}$ and $\sigma = \{0_{\sim}, G_{2,}\ 1_{\sim}\}$ are IFT on X and Y respectively. Define a mapping $f : (X, \tau) \to (Y, \sigma)$ by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFSC mapping.

Theorem 5.7: Every IFαC mapping is an IFaSPGC mapping but not conversely.

Proof: Let $f : X \to Y$ be an IFαC mapping . Let A be an IFRCS in X. Since every IFRCS is an IFCS, A is an IFCS in X. Then f(A) is an IFαCS in Y. Since every IFαCS is an IFSPGCS, f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

Example 5.8: Let X = {a, b}, Y = {u, v} and G_1= ⟨x, (0.2, 0.3), (0.8, 0.7) ⟩,G_2 = ⟨y, (0.5, 0.4), (0.5, 0.6) ⟩. Then $\tau = \{0_{\sim}, G_{1,}\ 1_{\sim}\}$ and $\sigma = \{0_{\sim}, G_{2,}\ 1_{\sim}\}$ are IFT on X and Y respectively. Define a mapping $f : (X, \tau) \to (Y, \sigma)$ by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFαC mapping.

Theorem 5.9: Every IFPC mapping is an IFaSPGC mapping but not conversely.

Proof: Assume that $f : X \to Y$ be an IFPC mapping. Let A be an IFRCS in X. Since every IFRCS is an IFCS, A is an IFCS in X. Then f(A) is an IFPCS in Y. Since every IFPCS is an IFSPGCS, f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

Example 5.10: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.5, 0.3), (0.5, 0.7)⟩ andG_2 = ⟨y, (0.5, 0.6), (0.5, 0.4)⟩. Then $\tau = \{0_{\sim}, G, 1_{\sim}\}$and $\sigma = \{0_{\sim}, G_{2,}\ 1_{\sim}\}$ are IFT on X and Y respectively. Define a mapping $f : (X, \tau) \to (Y, \sigma)$ by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFPC mapping.

Theorem 5.11: Every IFSPGC mapping is an IFaSPGC mapping but not conversely.

Proof: Assume that $f : X \to Y$ be an IFGSPC mapping. Let A be an IFRCS in X. Since every IFRCS is an IFCS, A is an IFCS in X. Then f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

Example 5.12: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.4, 0.2), (0.6, 0.8) ⟩, G_2 = ⟨x,(0.4, 0.2), (0.4, 0.8) ⟩, G_3 = ⟨y, (0.7, 0.8), (0.3, 0.2) ⟩ and G_4 =⟨y, (0.6, 0.7), (0.4, 0.3)⟩. Then $\tau = \{0_{\sim}, G_1, G_2, 1_{\sim}\}$ and $\sigma = \{0_{\sim}, G_3, G_4, 1_{\sim}\}$ are IFT on Xand y respectively.

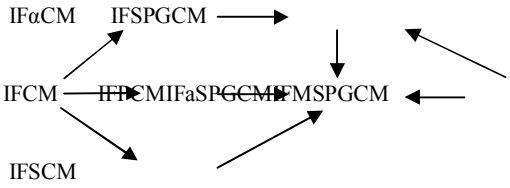
Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFSPGC mapping.

Theorem 5.13: Every IFMSPGC mapping is an IFaSPGC mapping but not conversely.

Proof: Assume that f : X → Y be an IFMSPGC mapping . Let A be an IFRCS in X. Then A is an IFSPGCS in X. By hypothesis f (A) is an IFSPGCS in Y. Therefore f is an IFaSPGC mapping.

Example 5.14: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.4, 0.2), (0.6, 0.8) ⟩, G_2 = ⟨x,(0.4, 0.2), (0.4, 0.8) ⟩, G_3 = ⟨y, (0.7, 0.8), (0.3, 0.2) ⟩ and G_4 =⟨y, (0.6, 0.7), (0.4, 0.3)⟩. Then τ = {$0_{\sim}$, G_1, G_2, $1_{\sim}$} and σ = {$0_{\sim}$, G_3, G_4, $1_{\sim}$} are IFT on Xand y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaSPGC mapping but not an IFMSPGC mapping.

The relation between various types of intuitionistic fuzzy closed mappings is given in the following diagram.



The reverse implications are not true in general in the above diagram.

Definition 5.15: A mapping f : X → Y is called an intuitionistic fuzzy almostsemipre generalized open mapping (IFaSPGO mapping for short) if f(A) is an IFSPGOS in Y for each IFROS A in X.

Theorem 5.16: Let f : X → Y be a bijective mapping. Then the following statements are equivalent:
(i) f is an IFaSPGO mapping,
(ii) f is an IFaSPGC mapping.
Proof: Straightforward.

Theorem 5.17: Let $p_{(\alpha, \beta)}$ be an IFP in X. A mapping f : X → Y is an IFaSPGO mapping if for every IFOS A in X with $f^{-1}(p_{(\alpha, \beta)}) \in A$, then there exists an IFOS B in Y with $p_{(\alpha, \beta)} \in B$ such that f(A) is IFD in B.

Proof: Let A be an IFROS in X. Then A is an IFOS in X. Let $f^{-1}(p_{(\alpha, \beta)}) \in A$, then there exists an IFOS B in Y such that $p_{(\alpha, \beta)} \in B$ and cl(f(A)) = B. Since B is an IFOS, cl(f(A)) = B is also an IFOS in Y. Therefore int(cl(f(A))) = cl(f(A)). Now f(A) ⊆cl(f(A)) = int(cl(f(A))) ⊆ cl(int(cl(f(A)))). This implies f(A) is an IFSPOS in Y and hence an IFSPGOS in Y. Thus f is an IFaSPGO mapping.

Theorem 5.18: Let f : X → Y be a mapping where Y is an $IFSPT_{1/2}$ space. Then the following statements are equivalent:
(i) f is an IFaSPGC mapping,
(ii) spcl(f(A)) ⊆ f(cl(A)) for every IFSPOS A in X,
(iii) spcl(f(A)) ⊆ f(cl(A)) for every IFSOS A in X,
(iv) f(A) ⊆spint(f(int(cl(A)))) for every IFPOS A in X.

Proof: (i) ⇒ (ii) Let A be an IFSPOS in X. Then cl(A) is an IFRCS in X. By hypothesis, f(cl(A)) is an IFSPGCS in Y and hence is an IFSPCS in Y, since Y is an $IFSPT_{1/2}$ space. This implies spcl(f(cl(A))) = f(cl(A)). Now spcl(f(A)) ⊆spcl(f(cl(A))) = f(cl(A)). Thus spcl(f(A)) ⊆ f(cl(A)).
(ii) ⇒ (iii) Since every IFSOS is an IFSPOS, the proof directly follows.
(iii) ⇒ (i) Let A be an IFRCS in X. Then A = cl(int(A)). Therefore A is an IFSOS in X. By hypothesis, spcl(f(A)) ⊆ f(cl(A)) = f(A) ⊆spcl(f(A)). Hence f(A) is an IFSPCS and hence is an IFSPGCS in Y. Thus f is an IFaSPGC mapping.
(i) ⇒ (iv) Let A be an IFPOS in X. Then A ⊆int(cl(A)). Since int(cl(A)) is an IFROS in X, by hypothesis, f(int(cl(A))) is an IFSPGOS in Y. Since Y is an $IFSPT_{1/2}$ space, f(int(cl(A))) is an IFSPOS in Y. Therefore f(A) ⊆ f(int(cl(A))) ⊆spint(f(int(cl(A)))).
(iv) ⇒ (i) Let A be an IFROS in X. Then A is an IFPOS in X. By hypothesis,f(A) ⊆spint(f(int(cl(A)))) = spint(f(A)) ⊆ f(A). This implies f(A) is an IFSPOS in Y and hence is an IFSPGOS in Y. Therefore f is an IFaSPGC mapping.

Theorem 5.19: Let f : X → Y be a mapping. If f is an IFaSPGC mapping, then spgcl(f(A)) ⊆ f(cl(A)) for every IFSPOS A in X.

Proof: Let A be an IFSPOS in X. Then cl(A) is an IFRCS in X. By hypothesis f(cl(A)) is an IFSPGCS in Y. Then spgcl(f(cl(A)) = f(cl(A)). Now spgcl(f(A)) ⊆spgcl(f(cl(A))) = f(cl(A)). That is spgcl(f(A)) ⊆ f(cl(A)).

Corollary 5.20: Let f : X → Y be a mapping. If f is an IFaSPGC mapping, then spgcl(f(A) ⊆ f(cl(A)) for every IFSOS A in X.

Proof: Since every IFSOS is an IFSPOS, the proof is obvious from the Theorem 5.19.

Corollary 5.21: Let f : X → Y be a mapping. If f is an IFaGSPC mapping, then gspcl(f(A) ⊆ f(cl(A)) for every IFPOS A in X.

Proof: Since every IFPOS is an IFSPOS, the proof is obvious from the Theorem 5.19.

Theorem 5.22: Let f : X → Y be a mapping. If f is an IFaSPGC mapping, then spgcl(f(A)) ⊆ f(cl(spint(A))) for every IFSPOS A in X.

Proof: Let A be an IFSPOS in X. Then cl(A) is an IFRCS in X. By hypothesis, f(cl(A)) is an IFSPGCS in Y. Then spgcl(f(A)) ⊆spgcl(f(cl(A))) = f(cl(A)) ⊆ f(cl(spint(A))), since spint(A) = A.

Corollary 5.23: Let f : X → Y be a mapping. If f is an IFaSPGC mapping, then spgcl(f(A)) ⊆ f(cl(spint(A))) for every IFSOS A in X.

Proof: Since every IFSOS is an IFSPOS, the proof is obvious from the Theorem 5.22.

Corollary 5.24: Let f: X → Y be a mapping. If f is an IFaSPGC mapping, then spgcl(f(A)) ⊆ f(cl(spint(A))) for every IFPOS A in X.

Proof: Since every IFPOS is an IFSPOS, the proof is obvious from the Theorem 5.22.

Theorem 5.25: Let f : X → Y be a mapping. If f(spint(B)) ⊆spint(f(B)) for every IFS B in X, then f is an IFaSPGO mapping.

Proof: Let $B \subseteq X$ be an IFROS. By hypothesis, $f(spint(B)) \subseteq spint(f(B))$. Since B is an IFROS, it is an IFSPOS in X. Therefore $spint(B) = B$. Hence $f(B) = f(spint(B)) \subseteq spint(f(B)) \subseteq f(B)$. This implies f(B) is an IFSPOS and hence an IFSPGOS in Y. Thus f is an IFaSPGO mapping.

Theorem 5.26: Let $f : X \to Y$ be a mapping. If $spcl(f(B)) \subseteq f(spcl(B))$ for every IFS B in X, then f is an IFaSPGC mapping.

Proof: Let $B \subseteq X$ be an IFRCS. By hypothesis, $spcl(f(B)) \subseteq f(spcl(B))$. Since B is an IFRCS, it is an IFSPCS in X. Therefore $spcl(B) = B$. Hence $f(B) = f(spcl(B)) \supseteq spcl(f(B)) \supseteq f(B)$. This implies f(B) is an IFSPCS and hence an IFSPGCS in Y. Thus f is an IFaSPGC mapping.

Theorem 5.27: The following statements are equivalent for a mapping $f : X \to Y$, where Y is an $IFSPT_{1/2}$ space:

(i) f is an IFaSPGC mapping,
(ii) $spcl(f(A)) \subseteq f(\alpha cl(A))$ for every IFSPOS A in X,
(iii) $spcl(f(A)) \subseteq f(\alpha cl(A))$ for every IFSOS A in X,
(iv) $f(A) \subseteq spint(f(scl(A)))$ for every IFPOS A in X.

Proof: (i) $\Rightarrow$ (ii) Let A be an IFSPOS in X. Then cl(A) is an IFRCS in X. By hypothesis f(cl(A)) is an IFSPGCS in Y and hence is an IFSPCS in Y, since Y is an $IFSPT_{1/2}$ space. This implies $spcl(f(cl(A))) = f(cl(A))$. Now $spcl(f(A)) \subseteq spcl(f(cl(A))) = f(cl(A))$. Since cl(A) is an IFRCS, $cl(int(cl(A))) = cl(A)$. Therefore $spcl(f(A)) \subseteq f(cl(A)) = f(cl(int(cl(A)))) \subseteq f(A \cup cl(int(cl(A)))) = f(\alpha cl(A))$. Hence $spcl(f(A)) \subseteq f(\alpha cl(A))$.
(ii) $\Rightarrow$ (iii) Since every IFSOS is an IFSPOS, the proof is obvious.
(iii) $\Rightarrow$ (i) Let A be an IFRCS in X. Then $A = cl(int(A))$. Therefore A is an IFSOS in X. By hypothesis, $spcl(f(A)) \subseteq f(\alpha cl(A)) \subseteq f(cl(A)) = f(A) \subseteq spcl(f(A))$. That is $spcl(f(A)) = f(A)$. Hence f(A) is an IFSPCS and hence is an IFSPGCS in Y. Thus f is an IFaSPGC mapping.
(i) $\Rightarrow$ (iv) Let A be an IFPOS in X. Then $A \subseteq int(cl(A))$. Since int(cl(A)) is an IFROS in X, by hypothesis, f(int(cl(A))) is an IFSPGOS in Y. Since Y is an $IFSPT_{1/2}$ space, f(int(cl(A))) is an IFSPOS in Y. Therefore $f(A) \subseteq f(int(cl(A))) \subseteq spint(f(int(cl(A)))) \subseteq spint(f(A \cup int(cl(A)))) = spint(f(scl(A)))$. That is $f(A) \subseteq spint(f(scl(A)))$.
(iv) $\Rightarrow$ (i) Let A be an IFROS in X. Then A is an IFPOS in X. By hypothesis, $f(A) \subseteq spint(f(scl(A)))$. This implies $f(A) \subseteq spint(f(A \cup int(cl(A)))) \subseteq spint(f(A \cup A)) = spint(f(A)) \subseteq f(A)$. Therefore f(A) is an IFSPOS in Y and hence an IFSPGOS in Y. Thus f is an IFaSPGC mapping.

Theorem 5.28: Let $f : X \to Y$ be a mapping where Y is an $IFSPT_{1/2}$ space. If f is an IFaSPGC mapping, then $int(cl(int(f(B)))) \subseteq f(spcl(B))$ for every IFRCS B in X.

Proof: Let $B \subseteq X$ be an IFRCS. By hypothesis, f(B) is an IFSPGCS in Y. Since Y is an $IFSPT_{1/2}$ space, f(B) is an IFSPCS in Y. Therefore $spcl(f(B)) = f(B)$. Now $int(cl(int(f(B)))) \subseteq f(B) = f(spcl(B))$, since $B = spcl(B)$. Hence $int(cl(int(f(B)))) \subseteq f(spcl(B))$.

Theorem 5.29: Let $f : X \to Y$ be a mapping where Y is an $IFSPT_{1/2}$ space. If f is an IFaSPGC mapping, then $f(spint(B)) \subseteq cl(int(cl(f(B))))$ for every IFROS B in X.

Proof: This theorem can be easily proved by taking complement in Theorem 5.28.

Theorem 5.30: Let $f : X \to Y$ be a bijective mapping. Then the following statements are equivalent:

(i) f is an IFaSPGO mapping,
(ii) f is an IFaSPGC mapping,
(iii) f^{-1} is an IFaSPG continuous mapping.

Proof: (i) $\Leftrightarrow$ (ii) is obvious from the Theorem 5.16.
(ii) $\Rightarrow$ (iii) Let $A \subseteq X$ be an IFRCS. Then by hypothesis, f(A) is an IFSPGCS in Y. That is $(f^{-1})^{-1}(A)$ is an IFSPGCS in Y. This implies f^{-1} is an IFaSPG continuous mapping.
(iii) $\Rightarrow$ (ii) Let $A \subseteq X$ be an IFRCS. Then by hypothesis $(f^{-1})^{-1}(A)$ is an IFSPGCSin Y. That is f(A) is an IFSPGCS in Y. Hence f is an IFaSPGC mapping.

6. REFERENCES

[1] K. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems, 20, 1986, 87-96.

[2] C. L. Chang, Fuzzy topological spaces, J.Math.Anal.Appl. 24, 1968, 182-190.

[3] D. Coker, An introduction to intuitionistic fuzzy topological space, Fuzzy Sets and Systems, 88, 1997, 81-89.

[4] H. Gurcay, Es. A. Haydar and D. Coker, On fuzzy continuity in intuitionistic fuzzy topological spaces, J.Fuzzy Math.5 (2) , 1997, 365-378.

[5] R. Santhi and K. ArunPrakash, Intuitionistic Fuzzy Semi-Generalized Irresolute Mapping, Tamkang Journal of Mathematics, Vol. 42, No. 2, 2012.

[6] R. Santhi and D. Jayanthi, Intuitionistic fuzzy almost generalized semi-pre continuous mappings, Tamkang Journal of Mathematics, Vol. 42, 2011, No.2, 175-191.

[7] Seok Jong Lee and EunPyo Lee, The category of intuitionistic fuzzy topological spaces, Bull. Korean Math. Soc. 37, No. 1, 2000, pp. 63-76.

[8] S.S. Thakur and R. Chaturvedi, Regular generalized closed sets in intuitionistic fuzzy topological spaces, Universitatea Din Bacau, Studii Si CercetariStiintifice, Seria:Matematica, 16 (2006), 257-272.

[9] M. Thirumalaiswamy and K. M. Arifmohammed, Semipre Generalized Open Sets and Applications of Semipre Generalized Closed Sets in Intuitionistic Fuzzy Topological Spaces (submitted).

[10] M. Thirumalaiswamy and K. M. Arifmohammed, Semipre Generalized Closed Mappings in Intuitionistic Fuzzy Topological Spaces (submitted).

[11] M. Thirumalaiswamy and K. Ramesh, Intuitionistic fuzzy semi-pre generalized closed sets (submitted).

[12] M. Thirumalaiswamy and K. Ramesh, Semipre Generalized Continuous and Irresolute Mappings in Intuitionistic Fuzzy Topological Space (submitted).

[13] M. Thirumalaiswamy and K. Ramesh, Semipre Generalized Homeomorphisms in Intuitionistic Fuzzy Topological Spaces (submitted)

[14] Young Bae Jun and Seok- Zun Song, Intuitionistic fuzzy semi-pre open sets and Intuitionistic fuzzy semi-pre continuous mappings, Jour. of Appl. Math & computing, 2005, 467-474.

[15] L. A. Zadeh, Fuzzy sets, Information and control, 8, 1965, 338-353.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 109 - 116, 2013, ISSN: 2319–8656

On Some New Contra Continuous and Contra Open Mappings in Intuitionistic Fuzzy Topological Spaces

M. Thirumalaiswamy
Department of Mathematics,
NGM College, Pollachi-642001,
Tamil Nadu, India.

K. M. Arifmohammed
Department of Mathematics,
NGM College, Pollachi-642001,
Tamil Nadu, India.

Abstract: In this paper we introduce intuitionistic fuzzy contrasemipre generalized continuous mappings, intuitionistic fuzzy almost contra semipregeneralized continuous mappings and intuitionistic fuzzy contra semipre generalized open mappings. We study some of their properties.

Keywords: Intuitionistic fuzzy point, intuitionistic fuzzy topology, intuitionistic fuzzy contra semipre generalized continuous mappings, intuitionistic fuzzy almost contra semipre generalized continuous mappings and intuitionistic fuzzy contra semipre generalized open mappings.

AMS Subject Classification (2000): 54A40, 03F55.

1. INTRODUCTION

In 1965, Zadeh [13] introduced fuzzy sets and in 1968, Chang [2] introduced fuzzy topology. After the introduction of fuzzy set and fuzzy topology, several authors were conducted on the generalization of this notion. The notion of intuitionistic fuzzy sets was introduced by Atanassov [1] as a generalization of fuzzy sets. In 1997, Coker [3] introduced the concept of intuitionistic fuzzy topological spaces. In 2005, Young Bae Jun and SeokZun Song [12] introduced Intuitionistic fuzzy semipre continuous mappings in intuitionistic fuzzy topological spaces. In this paper we introduce intuitionistic fuzzy contra semipre generalized continuous mappings, intuitionistic fuzzy almost contra semipre generalized continuous mappings and intuitionistic fuzzy contra semipre generalized open mappings. We investigate some of their properties.

2. PRELIMINARIES

Definition 2.1: [1] Let X be a non-empty fixed set. An intuitionistic fuzzy set (IFS in short) A in X is an object having the form $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$ where the functions $\mu_A : X \to [0, 1]$ and $\nu_A : X \to [0, 1]$ denote the degree of membership (namely $\mu_A(x)$) and the degree of non-membership (namely $\nu_A(x)$) of each element $x \in X$ to the set A, respectively, and $0 \le \mu_A(x) + \nu_A(x) \le 1$ for each $x \in X$. Denote by IFS(X), the set of all intuitionistic fuzzy sets in X.

Definition 2.2: [1] Let A and B be IFSs of the form $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$ and $B = \{\langle x, \mu_B(x), \nu_B(x)\rangle / x \in X\}$. Then

1. $A \subseteq B$ if and only if $\mu_A(x) \le \mu_B(x)$ and $\nu_A(x) \ge \nu_B(x)$ for all $x \in X$
2. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$
3. $A^c = \{\langle x, \nu_A(x), \mu_A(x)\rangle / x \in X\}$
4. $A \cap B = \{\langle x, \mu_A(x) \wedge \mu_B(x), \nu_A(x) \vee \nu_B(x)\rangle / x \in X\}$
5. $A \cup B = \{\langle x, \mu_A(x) \vee \mu_B(x), \nu_A(x) \wedge \nu_B(x)\rangle / x \in X\}$

For the sake of simplicity, we shall use the notation $A = \langle x, \mu_A, \nu_A\rangle$ instead of $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle / x \in X\}$. The intuitionistic fuzzy sets $0_\sim = \{\langle x, 0, 1\rangle / x \in X\}$ and $1_\sim = \{\langle x, 1, 0\rangle / x \in X\}$ are respectively the empty set and the whole set of X.

Definition 2.3: [3] An intuitionistic fuzzy topology (IFT in short) on X is a family τ of IFSs in X satisfying the following axioms:

1. $0_\sim, 1_\sim \in \tau$
2. $G_1 \cap G_2 \in \tau$, for any $G_1, G_2 \in \tau$
3. $\cup G_i \in \tau$ for any family $\{G_i / i \in J\} \subseteq \tau$

In this case the pair (X, τ) is called an intuitionistic fuzzy topological space(IFTS in short) and any IFS in τ is known as an intuitionistic fuzzy open set(IFOS in short)in X. The complement A^c of an IFOS A in an IFTS (X, τ) is called an intuitionistic fuzzy closed set (IFCS in short) in X.

Definition 2.4: [3] Let (X, τ) be an IFTS and $A = \langle x, \mu_A, \nu_A\rangle$ be an IFS in X. Then

1. $int(A) = \cup\{G / G \text{ is an IFOS in X and } G \subseteq A\}$
2. $cl(A) = \cap\{K / K \text{ is an IFCS in X and } A \subseteq K\}$
3. $cl(A^c) = (int(A))^c$
4. $int(A^c) = (cl(A))^c$

Definition 2.5: [5] An IFS A of an IFTS (X, τ) is an

1. intuitionistic fuzzy preclosed set (IFPCS in short) if $cl(int(A)) \subseteq A$
2. intuitionistic fuzzy preopen set (IFPOS in short) if $A \subseteq int(cl(A))$

Note that every IFOS in (X, τ) is an IFPOS in X.

Definition 2.6: [5] An IFS A of an IFTS (X, τ) is an

1. intuitionistic fuzzy α-closed set (IFαCS in short) if $cl(int(cl(A))) \subseteq A$
2. intuitionistic fuzzy α-open set (IFαOS in short) if $A \subseteq int(cl(int(A)))$
3. intuitionistic fuzzy regular closed set (IFRCS in short) if $A = cl(int(A))$
4. intuitionistic fuzzy regular open set (IFROS in short) if $A = int(cl(A))$

Definition 2.7: [12] An IFS A of an IFTS (X, τ) is an

1. intuitionistic fuzzy semipre closed set (IFSPCS in short) if there exists an IFPCS B such that $int(B) \subseteq A \subseteq B$
2. intuitionistic fuzzy semipre open set (IFSPOS in short) if there exists an IFPOS B such that $B \subseteq A \subseteq cl(B)$

Definition 2.8:[9] An IFS A is an IFTS (X, τ) is said to be an intuitionistic fuzzy semipregeneralized closed set (IFSPGCS

in short) if spcl(A) ⊆ U whenever A ⊆ U and U is an IFSOS in (X, τ).
Every IFCS, IFαCS, IFRCS, IFPCS and IFSPCS is an IFSPGCS but the converses are not true in general.

Definition 2.9:[7] The complement A^c of an IFSPGCS A in an IFTS (X, τ) is called an intuitionistic fuzzy semipre generalized open set (IFSPGOS in short) in X.

The family of all IFSPGOSs of an IFTS (X, τ) is denoted by IFSPGO(X). Every IFOS, IFαOS, IFROS, IFPOS and IFSPOS is an IFSPGOS but the converses are not true in general.

Definition 2.10: [6] Let α, β ∈ [0, 1] and α+ β ≤ 1. An intuitionistic fuzzy point (IFP for short) $p_{(\alpha, \beta)}$ of X is an IFS of X defined by

$$p_{(\alpha, \beta)}(y) = \begin{cases} (\alpha, \beta) & if\, y = p \\ (0, 1) & if\, y \neq p \end{cases}$$

Definition 2.11: [5] Let A be an IFS in an IFTS (X, τ). Then
1. spint(A) = ∪{G / G is an IFSPOS in X and G ⊆ A}
2. spcl(A) = ∩{K / K is an IFSPCS in X and A ⊆ K}

Note that for any IFS A in (X, τ), we have $spcl(A^c) = (spint(A))^c$ and $spint(A^c) = (spcl(A))^c$.

Definition 2.12: [11] Let A be an IFS in an IFTS (X, τ). Then semipre generalized interior of A (spgint(A) in short) and semipre generalized closure of A (spgcl(A) for short) are defined by
1. spgint(A) = ∪{G / G is an IFSPGOS in X and G ⊆ A}
2. spgcl(A) = ∩{K / K is an IFSPGCS in X and A ⊆ K}

Note that for any IFS A in (X, τ), we have $spgcl(A^c) = (spgint(A))^c$ and $spgint(A^c) = (spgcl(A))^c$.

Definition 2.13: [7] If every IFSPGCS in (X, τ) is an IFSPCS in (X, τ), then the space can be called as an intuitionistic fuzzy semipre $T_{1/2}$ ($IFSPT_{1/2}$ for short) space.

Definition 2.14:[10] A mapping f : (X, τ) → (Y, σ) is called an intuitionistic fuzzy semipre generalized continuous (IFSPG continuous for short) mappings if $f^{-1}(V)$ is an IFSPGCS in (X, τ) for every IFCS V of (Y, σ).

Definition 2.15: [6] A mappingf : (X, τ) → (Y, σ) is called an intuitionistic fuzzy closed mapping (IFCM for short) if f(A) is an IFCS in Y for each IFCS A in X.

Definition 2.16: [8] A mapping f : (X, τ) → (Y, σ) is called an intuitionistic fuzzy semipre generalized closed mapping (IFSPGCM in short) if f(A) is an IFSPGCS in Y for each IFCS A in X.

Definition 2.17: [8] A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy M-semipre generalized closed mapping (IFMSPGCM in short) if f(A) is an IFSPGCS in Y for every IFSPGCS A in X.

Definition 2.18:[10] A mapping f: (X, τ) → (Y, σ) be an intuitionistic fuzzy semipre generalized irresolute (IFSPG irresolute) mapping if $f^{-1}(V)$ is an IFSPGCS in (X, τ) for every IFSPGCS V of (Y, σ).

Definition 2.19: [5]Two IFSs A and B are said to be q-coincident ($A\ q\ B$ in short) if and only if there exists and element x ∈ X such that $\mu_A(x) > \nu_B(x)$ or $\nu_A(x) < \mu_B(x)$.

Definition 2.19:[4]A mapping f : (X, τ) → (Y, σ) is called an
1. intuitionistic fuzzy contra continuous if $f^{-1}(B)$ is an IFCS in X for everyIFOS B in Y
2. intuitionistic fuzzy contra α continuous if $f^{-1}(B)$ is an IFαCS in X for everyIFOS B in Y
3. intuitionistic fuzzy contra pre continuous if $f^{-1}(B)$ is an IFPCS in X forevery IFOS B in Y

3. INTUITIONISTIC FUZZY CONTRA SEMIPRE GENERALIZED CONTINUOUS MAPPINGS

In this section we have introduced intuitionistic fuzzy contra semipre generalized continuous mappings. We investigated some of its properties.

Definition 3.1: A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy contra semipre generalized continuous mapping (IFCSPG continuous mapping in short) if $f^{-1}(A)$ is an IFSPGCS in X for every IFOS A in Y.

Example 3.2: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.4, 0.2), (0.6, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPG continuous mapping.

Theorem 3.3: Every IFC continuous mapping is an IFCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFOS. Then $f^{-1}(A)$ is an IFCS in Y, by hypothesis. Hencef $^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFCSPG continuous mapping.

Example 3.4: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.4, 0.2), (0.6, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPG continuous mapping but not an IFC continuous mapping.

Theorem 3.5: Every IFCα continuous mapping is an IFCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFOS. Then $f^{-1}(A)$ is an IFαCS in X, by hypothesis. Hence $f^{-1}(A)$ is an IFGSPCS in X. Therefore f is an IFCSPG continuous mapping.

Example 3.6: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.4, 0.2), (0.6, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPG continuous mapping but not an IFCα continuous mapping.

Theorem 3.7: Every IFCP continuous mapping is an IFCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFOS. Then $f^{-1}(A)$ is an IFPCS in X, by hypothesis. Hencef $^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFCSPG continuous mapping.

Example 3.8: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩, G_2 = ⟨x, (0.2, 0.1), (0.8, 0.9)⟩ and G_3 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, G_2,1~} and σ = {0~, G_3,1~} are IFTs on X and Y respectively. Define a mappingf : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPG continuous mapping but not an IFCP continuous mapping.

Theorem 3.9: Let f : (X, τ) → (Y, σ) be a mapping. Then the following statements are equivalent:
(i) f is an IFCSPG continuous mapping
(ii) $f^{-1}(A)$ is an IFSPGOS in X for every IFCS A in Y
Proof: (i) ⇒ (ii) Let A be an IFCS in Y. Then A^c is an IFOS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGCS in X. That is $f^{-1}(A)^c$ is an IFGSPCS in X. Hence $f^{-1}(A)$ is an IFSPGOS in X.
(ii) ⇒ (i) Let A be an IFOS in Y. Then A^c is an IFCS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGOS in X. Hence $f^{-1}(A)$ is an IFSPGCS in X. Thus f is an IFCSPG continuous mapping.

Theorem 3.10: Let f : (X, τ) → (Y, σ) be a bijective mapping. Suppose that one of the following properties hold:
(i) $f^{-1}(cl(B)) \subseteq int(spcl(f^{-1}(B)))$ for each IFS B in Y
(ii) $cl(spint(f^{-1}(B))) \subseteq f^{-1}(int(B))$ for each IFS B in Y
(iii) $f(cl(spint(A))) \subseteq int(f(A))$ for each IFS A in X
(iv) $f(cl(A)) \subseteq int(f(A))$ for each IFSPOS A in X
Then f is an IFCSPG continuous mapping.
Proof: (i) ⇒ (ii) is obvious by taking complement in (i).
(ii) ⇒ (iii) Let A ⊆ X. Put B = f(A) in Y. This implies $A = f^{-1}(f(A)) = f^{-1}(B)$ in X. Now $cl(spint(A)) = cl(spint(f^{-1}(B))) \subseteq f^{-1}(int(B))$ by hypothesis. Therefore $f(cl(spint(A))) \subseteq f(f^{-1}(int(B))) = int(B) = int(f(A))$.
(iii) ⇒ (iv) Let A ⊆ X be an IFSPOS. Then spint(A) = A. By hypothesis, $f(cl(spint(A))) \subseteq int(f(A))$. Therefore $f(cl(A)) = f(cl(spint(A))) \subseteq int(f(A))$.
Suppose (iv) holds: Let A be an IFOS in Y. Then $f^{-1}(A)$ is an IFS in X and $spint(f^{-1}(A))$ is an IFSPOS in X. Hence by hypothesis, $f(cl(spint(f^{-1}(A)))) \subseteq int(f(spint(f^{-1}(A)))) \subseteq int(f(f^{-1}(A))) = int(A) \subseteq A$. Therefore $cl(spint(f^{-1}(A))) = f(f(cl(spint(f^{-1}(A))))) \subseteq f^{-1}(A)$. Now $cl(int(f^{-1}(A))) \subseteq cl(spint(f^{-1}(A))) \subseteq f^{-1}(A)$. This implies $f^{-1}(A)$ is an IFPCS in X and hence an IFSPGCS in X. Thus f is an IFCSPG continuous mapping.

Theorem 3.11: Let f : (X, τ) → (Y, σ) be a map. Suppose that one of the following properties hold:
(i) $f(spcl(A)) \subseteq int(f(A))$ for each IFS A in X
(ii) $spcl(f^{-1}(B)) \subseteq f^{-1}(int(B))$ for each IFS B in Y
(iii) $f^{-1}(cl(B)) \subseteq spint(f^{-1}(B))$ for each IFS B in Y
Then f is an IFCSPG continuous mapping.
Proof: (i) ⇒ (ii) Let B ⊆ Y. Then $f^{-1}(B)$ is an IFS in X. By hypothesis, $f(spcl(f^{-1}(B))) \subseteq int(f(f^{-1}(B))) \subseteq int(B)$. Now $spcl(f^{-1}(B)) \subseteq f^{-1}(f(spcl(f^{-1}(B)))) \subseteq f^{-1}(int(B))$.
(ii) ⇒ (iii) is obvious by taking complement in (ii).
Suppose (iii) holds: Let B be an IFCS in Y. Then cl(B) = B and $f^{-1}(B)$ is an IFS in X. Now $f^{-1}(B) = f^{-1}(cl(B)) \subseteq spint(f^{-1}(B)) \subseteq f^{-1}(B)$, by hypothesis. This implies $f^{-1}(B)$ is an IFSPOS in X and hence an IFGSPOS in X. Thus f is an IFCSPG continuous mapping.

Theorem 3.12: Let f : (X, τ) → (Y, σ) be a bijective mapping. Then f is an IFCSPG continuous mapping if $cl(f(A)) \subseteq f(spint(A))$ for every IFS A in X.
Proof: Let A be an IFCS in Y. Then cl(A) = A and $f^{-1}(A)$ is an IFS in X. By hypothesis $cl(f(f^{-1}(A))) \subseteq f(spint(f^{-1}(A)))$. Since f is onto, $f(f^{-1}(A)) = A$. Therefore $A = cl(A) = cl(f(f^{-1}(A))) \subseteq f(spint(f^{-1}(A)))$. Now $f^{-1}(A) \subseteq f^{-1}(f(spint(f^{-1}(A)))) = spint(f^{-1}(A)) \subseteq f^{-1}(A)$. Hence $f^{-1}(A)$ is an IFSPOS in X and hence an IFSPGOS in X. Thus f is an IFCSPG continuous mapping.

Theorem 3.13: If f : (X, τ) → (Y, σ) is an IFCSPG continuous mapping, where X is an $IFSPT_{1/2}$ space, then the following conditions hold:
(i) $spcl(f^{-1}(B)) \subseteq f^{-1}(int(spcl(B)))$ for every IFOS B in Y
(ii) $f^{-1}(cl(spint(B))) \subseteq spint(f^{-1}(B))$ for every IFCS B in Y
Proof: (i) Let B ⊆ Y be an IFOS. By hypothesis $f^{-1}(B)$ is an IFSPGCS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(B)$ is an IFSPCS in X. This implies $spcl(f^{-1}(B)) = f^{-1}(B) = f^{-1}(int(B)) \subseteq f^{-1}(int(spcl(B)))$.(ii) can be proved easily by taking complement in (i).

Theorem 3.14:(i) If f : (X, τ) → (Y, σ) is an IFCSPG continuous mapping and g : (Y, σ) →(Z, η) is an IF continuous mapping, then
(i) go f: (X, τ)→ (Z, η)is an IFCSPG continuous mapping
(ii) If f : (X, τ) → (Y, σ) is an IFCSPG continuous mapping and g : (Y, σ)→ (Z, η) is an IFC continuous mapping, then g o f : (X, τ) → (Z, η) is an IFSPG continuous mapping
(iii)If f : (X, τ) → (Y, σ) is an IFSPG irresolute mapping and g : (Y, σ)→ (Z, η) is an IFCSPG continuous mapping, then g o f : (X, τ)→(Z, η) is an IFCSPG continuous mapping
Proof: (i) Let A be an IFOS in Z. Then $g^{-1}(A)$ is an IFOS in Y, since g is an IF continuous mapping. As f is an IFCSPG continuous mapping, $f^{-1}(g^{-1}(A))$ is an IFSPGCS in X. Therefore g of is an IFCSPG continuous mapping.
(ii) Let A be an IFOS in Z. Then $g^{-1}(A)$ is an IFCS in Y, since g is an IFC continuous mapping. As f is an IFCSPG continuous mapping, $f^{-1}(g^{-1}(A))$ is an IFSPGOS in X. Therefore g o f is an IFSPG continuous mapping.
(iii) Let A be an IFOS in Z. Then $g^{-1}(A)$ is an IFSPGCS in Y, since g is an IFCSPG continuous mapping. As f is an IFSPG irresolute mapping, $f^{-1}(g^{-1}(A))$ is an IFSPGCS in X. Therefore g of is an IFCSPG continuous mapping.

Theorem 3.15: For a mapping f : (X, τ) → (Y, σ), the following are equivalent, where X is an $IFSPT_{1/2}$ space:
(i) f is an IFCSPG continuous mapping
(ii) for every IFCS A in Y, $f^{-1}(A)$ is an IFSPGOS in X
(iii) for every IFOS B in Y, $f^{-1}(B)$ is an IFSPGCS in X
(iv) for any IFCS A in Y and for any IFP $p_{(\alpha,\beta)} \in X$, if $f(p_{(\alpha,\beta)})\, q\, A$, then $p_{(\alpha,\beta)}\, q\, spint(f^{-1}(A))$
(v) For any IFCS A in Y and for any IFP $p_{(\alpha,\beta)} \in X$, if $f(p_{(\alpha,\beta)})\, q\, A$, then there exists an IFSPGOSB such that $p_{(\alpha,\beta)}\, q\, B$ and $f(B) \subseteq A$
Proof: (i) ⇔ (ii) and (ii) ⇔ (iii) are obvious.
(ii) ⇒ (iv) Let A ⊆ Y be an IFCSand let $p_{(\alpha,\beta)} \in X$. Let$f(p_{(\alpha,\beta)})\, q\, A$. Then$p_{(\alpha,\beta)}\, q\, f^{-1}(A)$. Byhypothesis, $f^{-1}(A)$ is an IFSPGOS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(A)$ is an IFSPOS in X. This implies $spint(f^{-1}(A)) = f^{-1}(A)$. Hence$p_{(\alpha,\beta)}\, q\, spint(f^{-1}(A))$.
(iv) ⇒ (ii) Let A ⊆ Y be an IFCS and let $p_{(\alpha,\beta)} \in X$. Let $f(p_{(\alpha,\beta)})\, q\, A$. Then$p_{(\alpha,\beta)}\, q\, f^{-1}(A)$. By hypothesis $p_{(\alpha,\beta)}\, q\, spint(f^{-1}(A))$. That is $f^{-1}(A) \subseteq spint(f^{-1}(A))$. But we have $spint(f^{-1}(A)) \subseteq f^{-1}(A)$. Therefore $f^{-1}(A) = spint(f^{-1}(A))$. Thus $f^{-1}(A)$ is an IFSPOS in X and hence an IFSPGOS in X.
(iv) ⇒ (v) Let A ⊆ Y be an IFCS and let $p_{(\alpha,\beta)} \in X$. Let $f(p_{(\alpha,\beta)})\, q\, A$. Then$p_{(\alpha,\beta)}\, q\, f^{-1}(A)$. By hypothesis $p_{(\alpha,\beta)}\, q\, spint(f^{-1}(A))$. Thus $f^{-1}(A)$ is an IFSPOS in X and hence an IFSPGOS in X. Let $f^{-1}(A) = B$. Therefore $p_{(\alpha,\beta)}\, q\, B$ and $f(B) = f(f^{-1}(A)) \subseteq A$.
(v) ⇒ (iv) Let A ⊆ Y be an IFCS and let $p_{(\alpha,\beta)} \in X$. Let $f(p_{(\alpha,\beta)})\, q\, A$. Then$p_{(\alpha,\beta)}\, q\, f^{-1}(A)$. By (v) there exists an IFSPGOS B in X such that $p_{(\alpha,\beta)}\, q\, B$ and $f(B) \subseteq A$. Let $B = f^{-1}(A)$. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(A)$ is an IFSPOS in X. Therefore $p_{(\alpha,\beta)}\, q\, spint(f^{-1}(A))$.

Theorem 3.16: A mapping f : (X, τ) → (Y, σ) is an IFCSPG continuous mapping if $f^{-1}(spcl(B)) \subseteq int(f^{-1}(B))$ for every IFS B in Y.

Proof: Let B ⊆ Y be an IFCS. Then cl(B) = B. Since every IFCS is an IFSPCS, spcl(B) = B. Now by hypothesis, $f^{-1}(B) = f^{-1}(spcl(B)) \subseteq int(f^{-1}(B)) \subseteq f^{-1}(B)$. This implies $f^{-1}(B)$ is an IFOS in X.Therefore f is an IFC continuous mapping. Then by Theorem 3.3, f is an IFCSPG continuous mapping.

Theorem 3.17: A mapping f : (X, τ) → (Y, σ) is an IFCSPG continuous mapping, where X is an $IFSPT_{1/2}$ space if and only if $f^{-1}(spcl(B)) \subseteq spint(f^{-1}(cl(B)))$ for every IFS Bin Y.
Proof: Necessity: Let B ⊆ Y be an IFS. Then cl(B) is an IFCS in Y. By hypothesis$f^{-1}(cl(B))$ is an IFSPGOS in X. Since X is an $IFSPT_{1/2}$ space, $f^{-1}(cl(B))$ is an IFSPOS in X. Therefore $f^{-1}(spcl(B)) \subseteq f^{-1}(cl(B)) = spint(f^{-1}(cl(B)))$.
Sufficiency: Let B ⊆ Y be an IFCS. Then cl(B) = B. By hypothesis, $f^{-1}(spcl(B)) \subseteq spint(f^{-1}(cl(B))) = spint(f^{-1}(B))$. But spcl(B) = B. Therefore $f^{-1}(B) = f^{-1}(spcl(B)) \subseteq spint(f^{-1}(B)) \subseteq f^{-1}(B)$. This implies $f^{-1}(B)$ is an IFSPOS in X and hence an IFSPGOS in X. Hence f is an IFCSPG continuous mapping.

Theorem 3.18: An IF continuous mappingf : (X, τ) → (Y, σ) is an IFCSPG continuous mapping if IFSPGO(X) = IFSPGC(X).
Proof: Let A⊆ Y be an IFOS. By hypothesis, $f^{-1}(A)$ is an IFOS in X and hence is an IFSPGOS in X. Since IFSPGO(X) = IFSPGC(X), $f^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFCSPG continuous mapping.

4. INTUITIONISTIC FUZZY ALMOST CONTRA SEMIPRE GENERALIZED CONTINUOUS MAPPINGS

In this section we have introduced intuitionistic fuzzy almost contra semipre generalized continuous mappings and studied some of its properties.

Definition 4.1: A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy almost contra semipre generalized continuous mapping (IFaCSPG continuous mapping for short) if $f^{-1}(A)$ is an IFSPGCS in X for every IFROS A in Y.

Example 4.2: Let X = {a, b}, Y = {u, v} and $G_1 = \langle x, (0.5, 0.4), (0.5, 0.6)\rangle$, $G_2 = \langle y, (0.4, 0.2), (0.6, 0.7)\rangle$. Then $\tau = \{0_\sim, G_1, 1_\sim\}$ and $\sigma = \{0_\sim, G_2, 1_\sim\}$ are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPG continuous mapping.

Theorem 4.3: Every IFC continuous mapping is an IFaCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFROS. Since every IFROS is an IFOS, A is an IFOS in Y. Then $f^{-1}(A)$ is an IFCS in X, by hypothesis. Hence $f^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFaCSPG continuous mapping.

Example 4.4: Let X = {a, b}, Y = {u, v} and $G_1 = \langle x, (0.5, 0.4), (0.5, 0.6)\rangle$, $G_2 = \langle y, (0.4, 0.2), (0.6, 0.7)\rangle$. Then $\tau = \{0_\sim, G_1, 1_\sim\}$ and $\sigma = \{0_\sim, G_2, 1_\sim\}$ are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPG continuous mapping but not an IFC continuous mapping.

Theorem 4.5: Every IFCα continuous mapping is an IFaCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFROS. Since every IFROS is an IFOS, A is an IFOS in Y. Then $f^{-1}(A)$ is an IFαCS in X, by hypothesis. Hence $f^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFaCSPG continuous mapping.

Example 4.6: Let X = {a, b}, Y = {u, v} and $G_1 = \langle x, (0.5, 0.4), (0.5, 0.6)\rangle$, $G_2 = \langle y, (0.4, 0.2), (0.6, 0.7)\rangle$. Then $\tau = \{0_\sim, G_1, 1_\sim\}$ and $\sigma = \{0_\sim, G_2, 1_\sim\}$ are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPG continuous mapping but not an IFCαcontinuos mapping.

Theorem 4.7: Every IFCP continuous mapping is an IFaCSPG continuous mapping but not conversely.
Proof: Let A⊆ Y be an IFROS. Since every IFROS is an IFOS, A is an IFOS in Y. Then $f^{-1}(A)$ is an IFPCS in X, by hypothesis. Hence $f^{-1}(A)$ is an IFSPGCS in X. Therefore f is an IFaCSPG continuous mapping.

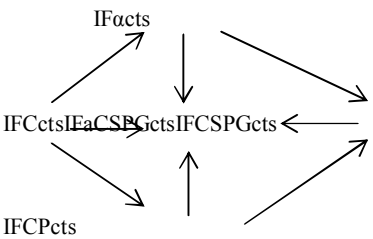
Example 4.8: Let X = {a, b}, Y = {u, v} and $G_1 = \langle x, (0.5, 0.6), (0.5, 0.4)\rangle$, $G_2 = \langle x, (0.2, 0.1), (0.8, 0.9)\rangle$ and $G_3 = \langle y, (0.2, 0.3), (0.8, 0.7)\rangle$,. Then $\tau = \{0_\sim, G_1, G_2, 1_\sim\}$ and $\sigma = \{0_\sim, G_3, 1_\sim\}$ are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPG continuous mapping but not an IFCP continuous mapping.

Theorem 4.9: Every IFCSPG continuous mapping is an IFaCSPG continuous mapping but not conversely.
Proof: Let f : (X, τ) → (Y, σ) be an IFCSPG continuous mapping. Let A⊆ Y be an IFROS. Then A is an IFOS in Y. By hypothesis, $f^{-1}(A)$ is an IFSPGCS in X. Hence f is an IFaCSPG continuous mapping.

Example 4.10: Let X = {a, b}, Y = {u, v} and $G_1 = \langle x, (0.5, 0.6), (0.5, 0.4)\rangle$, $G_2 = \langle y, (0.8, 0.7), (0.2, 0.3)\rangle$ and $G_3 = \langle y, (0.5, 0.5), (0.5, 0.5)\rangle$.Then $\tau = \{0_\sim, G_1, 1_\sim\}$ and $\sigma = \{0_\sim, G_2, G_3, 1_\sim\}$ are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPG continuous mapping but not an IFCSPG continuous mapping.

Theorem 4.11: If f : (X, τ) → (Y, σ) is a mapping, then the following are equivalent:
(i) f is an IFaCSPG continuous mapping,
(ii) $f^{-1}(A) \in IFSPGO(X)$ for every $A \in IFRC(Y)$.
Proof: (i) ⇒ (ii) Let A be an IFRCS in Y. Then A^c is an IFROS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGCS in X. Therefore $f^{-1}(A)$ is an IFSPGOS in X.
(ii) ⇒ (i) Let A be an IFROS in Y. Then A^c is an IFRCS in Y. By hypothesis, $f^{-1}(A^c)$ is an IFSPGOS in X. Therefore $f^{-1}(A)$ is an IFSPGCS in X. Hence f is an IFaCSPG continuous mapping.

The relation between various types of intuitionistic fuzzy contra continuity is given in the following diagram. In this diagram cts means continuous mapping.



The reverse implications are not true in general in the above diagram.

Theorem 4.12: If f : (X, τ) → (Y, σ) is a mapping, where X is an $IFSPT_{1/2}$ space, then the following are equivalent:
(i) f is an IFaCSPG continuous mapping
(ii) $f^{-1}(A) \in IFSPGO(X)$ for every $A \in IFRC(Y)$
(iii) $f^{-1}(int(cl(G))) \in IFSPGC(X)$ for every IFOS $G \subseteq Y$
(iv) $f^{-1}(cl(int(H))) \in IFSPGO(X)$ for every IFCS $H \subseteq Y$
Proof: (i) ⇔ (ii) is obvious from the Theorem 4.12.
(i) ⇒ (iii) Let G be any IFOS in Y. Then int(cl(G)) is an IFROS in Y. By hypothesis, $f^{-1}(int(cl(G)))$ is an IFSPGCS in X. Hencef $^{-1}(int(cl(G))) \in IFSPGC(X)$.
(iii) ⇒ (i) Let A be any IFROS in Y. Then A is an IFOS in Y. By hypothesis, we have $f^{-1}(int(cl(A))) \in IFSPGC(X)$. That is $f^{-1}(A) \in IFSPGC(X)$, since int(cl(A)) = A. Hence f is an IFaCSPG continuous mapping.
(ii) ⇔ (iv) is similar to (i) ⇔ (iii).

5. INTUITIONISTIC FUZZY CONTRA SEMIPRE GENERALIZED OPEN MAPPINGS

In this section we have introduced intuitionistic fuzzy contra semipre generalized openmappings. We have investigated some of its properties.

Definition 5.1: A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy contra semipre generalized open mapping (IFCSPGOM for short) if f(A) is an IFSPGCS in Y for every IFOS A in X.

Example 5.2: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.4, 0.2), (0.6, 0.7) ⟩,G_2 = ⟨y, (0.5, 0.4), (0.5, 0.6) ⟩. Then τ = {$0_{\sim}$, $G_{1,}$ $1_{\sim}$} and σ = {$0_{\sim}$, $G_{2,}$ $1_{\sim}$} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPGOM.

Theorem 5.3: For a bijective mapping f : (X, τ) → (Y, σ), where Y is an $IFSPT_{1/2}$ space, the following statements are equivalent:
(i) f is an IFCSPGOM
(ii) for every IFCS A in X, f(A) is an IFSPGOS in Y
(iii) for every IFOS B in X, f(B) is an IFSPGCS in Y
(iv) for any IFCS A in X and for any IFP $p(\alpha, \beta) \in Y$, if $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$, then$p_{(\alpha, \beta)\, q}$spint(f(A))
(v) For any IFCS A in X and for any $p_{(\alpha, \beta)} \in Y$, if $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$, then there existsan IFSPGOS B such that $p_{(\alpha, \beta)\, q} B$ and $f^{-1}(B) \subseteq A$
Proof: (i) ⇒ (ii) Let A be an IFCS in X. Then A^c is an IFOS in X. By hypothesis, $f(A^c)$ is an IFSPGCS in Y. That is $f(A)^c$ is an IFSPGCS in Y. Hence f(A) is an IFSPGOS in Y.
(ii) ⇒ (i) Let A be an IFOS in X. Then A^c is an IFCS in X. By hypothesis, $f(A^c) = (f(A))^c$ is an IFSPGOS in Y. Hence f(A) is an IFSPGCS in Y. Thus f is an IFCSPGOM.
(ii) ⇔ (iii) is obvious.
(ii) ⇒ (iv) Let A ⊆ X be an IFCSand let $p_{(\alpha, \beta)} \in Y$. Assume that $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$. Then $p_{(\alpha, \beta)\, q} f(A)$. By hypothesis, f(A) is an IFSPGOS in Y. Since Y is an $IFSPT_{1/2}$ space, f(A) is an IFSPOS in Y. This implies spint(f(A)) = f(A). Hence $p_{(\alpha, \beta)\, q}$spint(f(A)).
(iv) ⇒ (ii) Let A ⊆ X be an IFCS and let $p_{(\alpha, \beta)} \in Y$. Assume that $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$. Then $p_{(\alpha, \beta)\, q} f(A)$. By hypothesis $p_{(\alpha, \beta)\, q}$spint(f(A)). That is f(A) ⊆spint(f(A)) ⊆ f(A). Therefore f(A) = spint(f(A)) is an IFSPOS in Y and hence an IFSPGOS in Y.
(iv) ⇒ (v) Let A ⊆ X be an IFCS and let $p_{(\alpha, \beta)} \in Y$. Assume that $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$.Then $p_{(\alpha, \beta)\, q} f(A)$. This implies $p_{(\alpha, \beta)\, q}$spint(f(A)). Thus f(A) is an IFSPOS in Y and hence an IFSPGOS in Y. Let f(A) = B. Therefore $p_{(\alpha, \beta) q} B$ and $f^{-1}(B) = f^{-1}(f(A)) \subseteq A$.
(v) ⇒ (iv) Let A ⊆ X be an IFCS and let $p_{(\alpha, \beta)} \in Y$. Assume that $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$. Thenp$_{(\alpha, \beta)\, q}$ f(A). By hypothesis there exists an IFSPGOS B in Y such that $p_{(\alpha, \beta)\, q} B$ and $f^{-1}(B) \subseteq A$. Let B = f(A). Then $p_{(\alpha, \beta)\, q} f(A)$. Since Y is an $IFSPT_{1/2}$ space, f(A) is an IFSPOS in Y. Therefore $p_{(\alpha, \beta)\, q}$spint(f(A)).

Theorem 5.4: Let f : (X, τ) → (Y, σ) be a bijective mapping. Suppose that one of the following properties hold:
(i) f(cl(B)) ⊆int(spcl(f(B))) for each IFS B in X
(ii) cl(spint(f(B))) ⊆ f(int(B)) for each IFS B in X
(iii) $f^{-1}(cl(spint(A))) \subseteq int(f^{-1}(A))$ for each IFS A in Y
(iv) $f^{-1}(cl(A)) \subseteq int(f^{-1}(A))$ for each IFSPOS A in Y
Then f is an IFCSPGOM.
Proof: (i) ⇒ (ii) is obvious by taking the complement in (i).
(ii) ⇒ (iii) Let A ⊆ Y. Put $B = f^{-1}(A)$ in X. This implies A = f(B) in Y. Now cl(spint(A)) = cl(spint(f(B))) ⊆ f(int(B)) by (ii). Therefore $f^{-1}(cl(spint(A))) \subseteq f^{-1}(f(int(B))) = int(B) = int(f^{-1}(A))$.
(iii) ⇒ (iv) Let A ⊆ Y be an IFSPOS. Then spint(A) = A. By hypothesis, $f^{-1}(cl(spint(A))) \subseteq int(f^{-1}(A))$. Therefore $f^{-1}(cl(A)) \subseteq int(f^{-1}(A))$.
Suppose (iv) holds: Let A be an IFOS in X. Then f(A) is an IFS in Y and spint(f(A)) is an IFSPOS in Y. Hence by hypothesis, we have $f^{-1}(cl(spint(f(A)))) \subseteq int(f^{-1}(spint(f(A)))) \subseteq int(f^{-1}(f(A))) = int(A) \subseteq A$. Therefore $cl(spint(f(A))) = f(f^{-1}(cl(spint(f(A))))) \subseteq f(A)$. Now $cl(int(f(A))) \subseteq cl(spint(f(A))) \subseteq f(A)$. This implies f(A) is an IFPCS in Y and hence an IFSPGCS in Y. Thus f is an IFCSPGOM.

Theorem 5.5: Let f : (X, τ) → (Y, σ) be a bijective mapping. Suppose that one of the following properties hold:
(i) $f^{-1}(spcl(A)) \subseteq int(f^{-1}(A))$ for each IFS A in Y
(ii) spcl(f(B)) ⊆ f(int(B)) for each IFS B in X
(iii) f(cl(B)) ⊆spint(f(B)) for each IFS B in X
Then f is an IFCSPGOM.
Proof: (i) ⇒ (ii) Let B ⊆ X. Then f(B) is an IFS in Y. By hypothesis, $f^{-1}(spcl(f(B))) \subseteq int(f^{-1}(f(B))) = int(B)$. Now $spcl(f(B)) = f(f^{-1}(spcl(f(B)))) \subseteq f(int(B))$.
(ii) ⇒ (iii) is obvious by taking complement in (ii).
Suppose (iii) holds. Let B be an IFCS in X. Then cl(B) = B and f(B) is an IFS in Y. Now f(B) = f(cl(B)) ⊆spint(f(B)) ⊆ f(B), by hypothesis. This implies f(B) is an IFSPOS in Y and hence an IFSPGOS in Y. Thus f is an IFCSPGOM by Theorem 5.3.

Theorem 5.6: Let f : (X, τ) → (Y, σ) be a bijective mapping. Then f is an IFCSPGOM if $cl(f^{-1}(A)) \subseteq f^{-1}(spint(A))$ for every IFS A in Y.
Proof: Let A be an IFCS in X. Then cl(A) = A and f(A) is an IFS in Y. By hypothesis $cl(f^{-1}(f(A))) \subseteq f^{-1}(spint(f(A)))$. Therefore $A = cl(A) = cl(f^{-1}(f(A))) \subseteq f^{-1}(spint(f(A)))$. Now $f(A) \subseteq f(f^{-1}(spint(f(A)))) = spint(f(A)) \subseteq f(A)$. Hence f(A) is an IFSPOS in Y and hence an IFSPGOS in Y. Thus f is an IFCSPGOM by Theorem 5.3.

Theorem 5.7: If f : (X, τ) → (Y, σ) is an IFCSPGOM, where Y is an $IFSPT_{1/2}$ space, then the following conditions are hold:
(i) spcl(f(B)) ⊆ f(int(spcl(B))) for every IFOS B in X
(ii) f(cl(spint(B))) ⊆spint(f(B)) for every IFCS B in X
Proof: (i) Let B ⊆ X be an IFOS. Then int(B) = B. By hypothesis f(B) is an IFSPGCS in Y. Since Y is an $IFSPT_{1/2}$ space, f(B) is an IFSPCS in Y. This implies spcl(f(B)) = f(B) = f(int(B)) ⊆ f(int(spcl(B))).
(ii) can be proved easily by taking complement in (i).
Theorem 5.8: A mapping f : (X, τ) → (Y, σ) is an IFCSPGOM if f(spcl(B)) ⊆int(f(B)) for every IFS B in X.

Proof: Let B ⊆ X be an IFCS. Then cl(B) = B. Since every IFCS is an IFSPCS, spcl(B) = B. Now by hypothesis, f(B) = f(spcl(B)) ⊆int(f(B)) ⊆ f(B). This implies f(B) is an IFOS in Y. Therefore f(B) is an IFSPGOS in Y. Hence f is an IFCSPGOM.

Theorem 5.9: A mapping f : (X, τ) → (Y, σ) is an IFCSPGOM, where Y is an IFSPT$_{1/2}$ space if and only if f(spcl(B)) ⊆spint(f(cl(B))) for every IFS B in X.
Proof: Necessity: Let B ⊆ X be an IFS. Then cl(B) is an IFCS in X. By hypothesis f(cl(B)) is an IFSPGOS in Y. Since Y is an IFSPT$_{1/2}$ space, f(cl(B)) is an IFSPOS in Y. Therefore f(spcl(B)) ⊆ f(cl(B)) = spint(f(cl(B))).
Sufficiency: Let B ⊆ X be an IFCS. Then cl(B) = B. By hypothesis, f(spcl(B)) ⊆ spint(f(cl(B))) = spint(f(B)). But spcl(B) = B. Therefore f(B) = f(spcl(B)) ⊆spint(f(B) ⊆ f(B). This implies f(B) is an IFSPOS in Y and hence an IFSPGOS in Y. Hence f is an IFCSPGOM.

Theorem 5.10: An IFOM f : (X, τ) → (Y, σ) is an IFCSPGOM if IFSPGO(Y) = IFSPGC(Y).
Proof: Let A⊆ X be an IFOS. By hypothesis, f(A) is an IFOS in Y and hence is an IFSPGOS in Y. Thus f(A) is an IFSPGCS in Y, since IFSPGO(Y) = IFSPGC(Y). Therefore f is an IFCSPGOM.

Definition 5.11: A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy almost contra semipre generalized open mapping (IFaCSPGOM for short) if f(A) is an IFSPGCS in Y for every IFROS A in X.

Theorem 5.12: Every IFCSPGOM is an IFaCSPGOM but not conversely.
Proof: Assume that f : (X, τ) → (Y, σ) be an IFCSPGOM. Let A⊆ X be an IFROS. Then A is an IFOS in X. By hypothesis, f(A) is an IFSPGCS in Y. Hence f is an IFaCSPGOM.

Example 5.13: Let X = {a, b}, Y = {u, v}, G_1 = ⟨x, (0.5, 0.7), (0.5, 0.3)⟩, G_2 = ⟨x, (0.4, 0.2), (0.5, 0.4)⟩ and G_3 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩ and G_4 = ⟨y, (0.5, 0.6), (0.5, 0.4)⟩. Then τ = {0~, G_1, G_2,G_3, 1~} and σ = {0~, G_4, 1~} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPGOM but not an IFCSPGOM.

Theorem 5.14: If f : (X, τ) → (Y, σ) is a bijective mapping, where Y is an IFSPT$_{1/2}$ space, then the following conditions are equivalent:
(i) f is an IFaCSPGOM
(ii) f(A) ∈ IFGSPO(Y) for every A ∈ IFRC(X)
(iii) f(int(cl(A))) ∈ IFSPGC(Y) for every IFOS A ⊆ X
(iv) f(cl(int(A))) ∈ IFSPGO(Y) for every IFCS A ⊆ X
Proof: (i) ⇔ (ii) is obvious.
(i) ⇒ (iii) Let A be any IFOS in X. Then int(cl(A)) is an IFROS in X. By hypothesis, f(int(cl(A))) is an IFSPGCS in Y. Hence f(int(cl(A))) ∈ IFSPGC(Y).
(iii) ⇒ (i) Let A be any IFROS in X. Then A is an IFOS in X. By hypothesis, f(int(cl(A))) ∈ IFSPGC(Y). That is f(A) ∈ IFSPGC(Y), since int(cl(A)) = A. Hence f is an IFaCSPGOM.
(ii) ⇔ (iv) is similar as (i) ⇔ (iii).

Definition 5.15: A mapping f : (X, τ) → (Y, σ) is said to be an intuitionistic fuzzy contra Msemipre generalized open mapping (IFCMSPGOM) if f(A) is an IFSPGCS in Y for every IFSPGOS A in X.

Example 5.16: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.6), (0.5, 0.4)⟩, G_2 = ⟨y, (0.2, 0.3), (0.8, 0.7)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, 1~} are IFTs on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCMSPGOM.

Theorem 5.17: Let f : (X, τ) → (Y, σ) be a bijective mapping. Then the following statements are equivalent:
(i) f is an IFCMSPGOM,
(ii) f(A) is an IFSPGOS in Y for every IFSPGCS A in X.
Proof: (i) ⇒ (ii) Let A be an IFSPGCS in X. Then A^c is an IFSPGOS in X. By hypothesis, f(A^c) is an IFSPGCS in Y. That is f(A)^c is an IFSPGCS in Y. Hence f(A) is an IFSPGOS in Y.
(ii) ⇒ (i) Let A be an IFSPGOS in X. Then A^c is an IFGSPCS in X. By hypothesis, f(A^c) is an IFSPGOS in Y. Hence f(A) is an IFSPGCS in Y. Thus f is an IFCMSPGOM.

Theorem 5.18: Every IFCMSPGOM is an IFCSPGOM but not conversely.
Proof: Assume that f : (X, τ) → (Y, σ) be an IFCMSPGOM. Let A⊆ X be an IFOS. Then A is an IFSPGOS in X. By hypothesis, f(A) is an IFSPGCS in Y. Hence f is an IFCSPGOM.

Example 5.19: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.6, 0.7), (0.4, 0.3)⟩ and G_3 = ⟨y, (0.4, 0.7), (0.6, 0.3)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, G_3, 1~} are IFTs on X and Y respectively. Define a mappingf : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFCSPGO mapping but not an IFCMSPGOM.

Theorem 5.20: Every IFCMSPGOM is an IFaCSPGO mapping but not conversely.
Proof: Assume that f : X → Y be an IFCMSPGOM. Let A⊆X be an IFROS. Then A is an IFSPGOS in X. By hypothesis, f(A) is an IFSPGCS in Y. Hence f is an IFaCSPGOM.

Example 5.21: Let X = {a, b}, Y = {u, v} and G_1 = ⟨x, (0.5, 0.4), (0.5, 0.6)⟩, G_2 = ⟨y, (0.6, 0.7), (0.4, 0.3)⟩ and G_3 = ⟨y, (0.4, 0.7), (0.6, 0.3)⟩. Then τ = {0~, G_1, 1~} and σ = {0~, G_2, G_3, 1~} are IFT on X and Y respectively. Define a mapping f : (X, τ) → (Y, σ) by f(a) = u and f(b) = v. Then f is an IFaCSPGO mapping but not an IFCMSPGO mapping

The relation between various types of intuitionistic fuzzy contra open maps is given in the following diagram.

IFCSPGOmapIF~~aCSPGOmap~~

IFCMSPGO map

The reverse implications are not true in general in the above diagram.

Theorem 5.22: (i) If f : (X, τ) → (Y, σ) is an IFOM and g : (Y, σ) → (Z, η) be an IFCSPGOM, then g of is an IFCSPGOM.
(ii) If f : (X, τ) → (Y, σ) is an IFCSPGOM and g : (Y, σ) → (Z, η)is an IFMSPGCM, then g of is an IFCSPGOM.
(iii) If f : (X, τ) → (Y, σ) is an IFSPGOM and g : (Y, σ) → (Z, η)is an IFCMSPGOM, then g of is an IFCSPGOM.

(iv) If $f : (X, \tau) \to (Y, \sigma)$ is an IFCSPGOM and $g : (Y, \sigma) \to (Z, \eta)$is an IFCMSPGOM, then $g \circ f : (X, \tau) \to (Z, \eta)$ is an IFSPGOM.

Proof: (i) Let A be an IFOS in X. Then f(A) is an IFOS in Y. Therefore g(f(A)) is an IFSPGCS in Z. Hence g of is an IFCSPGOM.

(ii) Let A be an IFOS in X. Then f(A) is an IFSPGCS in Y. Therefore g(f(A)) is an IFSPGCS in Z. Hence g of is an IFCSPGOM.

(iii) Let A be an IFOS in X. Then f(A) is an IFSPGOS in Y. Therefore g(f(A)) is an IFSPGCS in Z. Hence g of is an IFCSPGOM.

(iv) Let A be an IFOS in X. Then f(A) is an IFSPGCS in Y, since f is an IFCSPGOM. Since g is an IFCMSPGOM, g(f(A)) is an IFSPGOS in Z. Therefore g of is an IFSPGOM.

Theorem 5.23: If $f : (X, \tau) \to (Y, \sigma)$ is an IFCMSPGOM, then for any IFSPGCS A in X and for any IFP $p_{(\alpha, \beta)} \in Y$, if $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$, then $p_{(\alpha, \beta)} \, q \, spgint(f(A))$.

Proof: Let $A \subseteq X$ be an IFSPGCSand let $p_{(\alpha, \beta)} \in Y$. Assume that $f^{-1}(p_{(\alpha, \beta)}) \, q \, A$. Then$p_{(\alpha, \beta)} \, q \, f(A)$. By hypothesis, f(A) is an IFSPGOS in Y. This implies spgint(f(A)) = f(A). Hence $p_{(\alpha, \beta)} \, q \, spgint(f(A))$.

REFERENCES

[1] K. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems, 20, 1986, 87-96.

[2] C. L. Chang, Fuzzy topological spaces, J.Math.Anal.Appl. 24, 1968, 182-190.

[3] D. Coker, An introduction to intuitionistic fuzzy topological space, Fuzzy Sets and Systems, 88, 1997, 81-89.

[4] E.Ekici and B.Krsteska, Intuitionistic fuzzy contra strong pre-continuity, Facta Univ. Ser.Math. Inform., 2007, 273-284.

[5] H. Gurcay, Es. A. Haydar and D. Coker, On fuzzy continuity in intuitionistic fuzzy topological spaces, J.Fuzzy Math.5 (2) , 1997, 365-378.

[6] Seok Jong Lee and EunPyo Lee, The category of intuitionistic fuzzy topological spaces, Bull. Korean Math. Soc. 37, No. 1, 2000, pp. 63-76.

[7] M. Thirumalaiswamy and K. M. Arifmohammed, Semipre Generalized Open Sets and Applications of Semipre Generalized Closed Sets in Intuitionistic Fuzzy Topological Spaces (submitted).

[8] M. Thirumalaiswamy and K. M. Arifmohammed, Semipre Generalized Closed Mappings in Intuitionistic Fuzzy Topological Spaces (submitted).

[9] M. Thirumalaiswamy and K. Ramesh, Intuitionistic fuzzy Semipre Generalized Closed Sets (submitted).

[10] M. Thirumalaiswamy and K. Ramesh, Semipre Generalized Continuous and Irresolute Mappings in Intuitionistic Fuzzy Topological Space (submitted).

[11] M. Thirumalaiswamy and K. Ramesh, Semipre Generalized Homeomorphisms in Intuitionistic Fuzzy Topological Spaces (submitted)

[12] Young Bae Jun and Seok- Zun Song, Intuitionistic fuzzy semi-pre open sets and Intuitionistic fuzzy semi-pre continuous mappings, Jour. of Appl. Math & computing, 2005, 467-474.

[13] L. A. Zadeh, Fuzzy sets, Information and control, 8, 1965, 338-353.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 117 - 120, 2013, ISSN: 2319–8656

DESIGN OF AN INTELLIGENT AND EFFICIENT LIGHT CONTROL SYSTEM

Arun Radhakrishnan,
Department of ECE,
Jimma Institute of Technology,
Jimma University,
Ethiopia

Vuttaradi Anand,
Department of ECE,
Jimma Institute of Technology,
Jimma University,
Ethiopia

Abstract: Recently, many researches has been carried out to save the energy in many aspects such as producing a device which consumes very less energy or designing a system which helps to reduce the power consumption using the existing devices. In this paper, a room light control system is proposed which is named as light control system (LCS). This proposed system will able to provide the needed light which provides the satisfaction of users and will provide energy saving and management.

In this paper the Lighting Control System and the decision making algorithm, are discussed. As per the algorithm the system will first check any occupant is there in the room. If so then the system will check the intensity of light in the room and if it is low then it will switch on the light.

Our proposed system can able to minimize the energy consumed for lighting in a room and can able to provide it efficiently.

Keywords: Lighting Control system, Energy saving, LDR, PIR sensor

1. INTRODUCTION:

Power saving have became a necessary thing in our day to day life. Many conventional power saving methods such as using electrical devices which consumes very less energy or cutting off the entire power supply for a scheduled time for a particular area are not efficient and there will be a lot discomforts to the users and cost may also increase to use a low power electrical device.

Buildings are responsible for up to 40% of energy usage. Most part of this energy is used mainly for maintaining good lighting such that the workers feel comfortable. Nowadays the newly constructed modernised or automated buildings may have lighting system to improve the comfort of occupants and to save the energy. But there are large number of old buildings which contains the traditional lighting system. To reduce the energy consumption in those types of buildings and to help the owners of that building in terms of saving electricity bill an intelligent and an effective method is discussed in this paper.

Because of advancement in Sensor technology a very cheap and portable methods to measure our surroundings are available.

The amounts of light required to for a good environment to work comfortably in various areas are shown in table 1 which is recommended by CIBSE lighting guides.'

Table 1 Required intensity of light for various environments

Type of place and work	Intensity required
Filing – Office work	300 lux
General office (Typing and Writing)	500lux
Painting	750 lux
Classrooms	300 lux
Classrooms for evening class	500 lux
Auditorium	500 lux
Assembly (Industry)	1000 lux

2. EXISTING SYSTEM:

This section describes about the most commonly used lighting control system used in buildings. Since this method is going to use wireless sensor network it is mandatory to know the operation of existing lighting control system. It can be decided that energy loss is occurred with a lighting system when the lighting system illuminates a light which is an area which is not being used currently at that particular time or when it illuminates a light even though sufficient lighting is available to work.

The most commonly used lighting systems are explained below.

2.1 A Switch operated manually:

In this method a user has to switch ON and OFF the required lights. Since the user can switch on and off the lights as per their preferences there is a chance of keeping the lights in on state even though it was not need during that time. This may occur because of carelessness of user and a large amount of power is wasted.

2.2 By Detecting Occupants:

This approach first checks whether any occupants are there in the room or not. If anybody is there in that room then it checks the intensity of light, if it is enough then it won't switch on the light otherwise it switch on the light.

The lighting system with occupant detection uses passive infrared sensor (PIR). This PIR sensor detects any movement is present in that particular area. If any movement is there means then this system automatically switches ON the lights. If timers are not used in this type of system means then the lights will be kept in ON state even after the user left the place. Because of this fault also a large amount of energy can be wasted.

Then another drawback about this type of system is, it will switch ON the lights when there is an occupant is present in that area. But there is a possibility of enough lighting will be there at that particular time. This system is not going to check the intensity of light before switching on the lights. Because of this also a large amount of energy can be lost.

3. PROPOSED SYSTEM:

The proposed system overcomes all the drawbacks of existing system. This system takes two things into account before taking any action, namely (1) human presence and (2) intensity of light. The system consists of a PIR sensor (Parallax 555- 28027) and an LDR (NORP 12). The PIR sensor is used to detect whether any occupants are there in that room and LDR is used to detect the intensity of light in that room. Apart from this an algorithm can be implemented in our system which uses both the LDR and PIR sensor to decide whether to switch on the light or not.

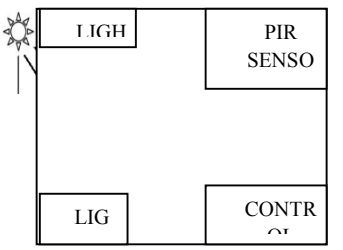


Figure 1 Setup of proposed system

4. SYSTEM DESIGN:

4.1 Block diagram:

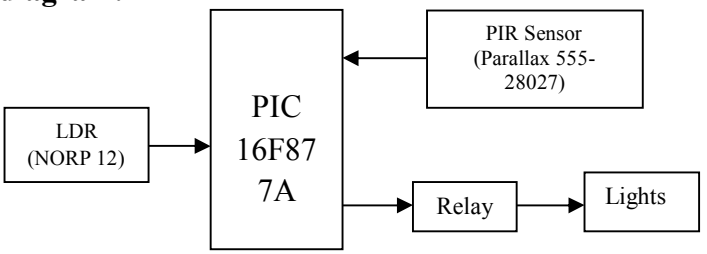


Figure 2 Block Diagram for the proposed system.

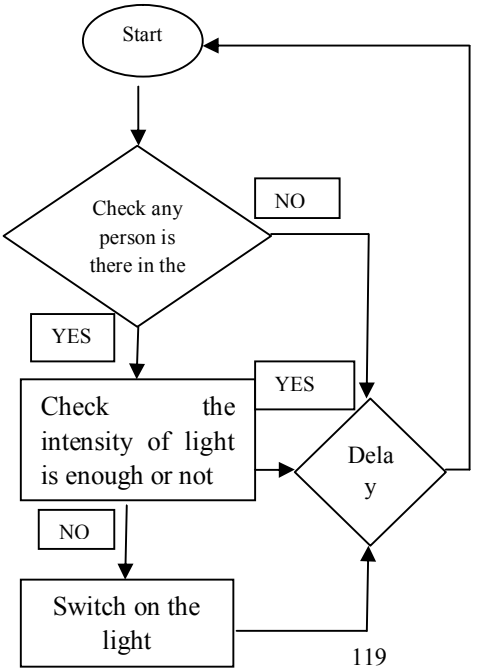
This system can be implemented using a PIC 16F877A, a LDR, A PIR sensor and the lights can be controlled by relays. The LDR sensor will keep on sensing the intensity of light and sends it to the microcontroller. The PIR sensor will send a signal to the microcontroller if there is any occupant in the room. If anybody is present in the room then the microcontroller compares the sensed value of intensity in the room with the value already stored in the microcontroller. If the sensed value is less than the value stored in the microcontroller then the light will be switched on by connecting the relay.

5. ALGORITHM:

Step 1: Start
Step 2: Check whether any occupant is there in the room using PIR sensor.
Step 3: If any Occupants is there means then compare the intensity of light in the room which was sensed by LDR. If nobody was there means then after some time delay again go to step 1.
Step 4: If the sensed intensity is less than the required level, then switch on the light or if it was enough means then after some time delay proceed to step 1.
As per the algorithm our system will first check whether any occupants are there in the room with the help of PIR sensor where the system has been installed. If any occupants are there then it will check the value of light luminance which is sensed through LDR and then the sensed value will be compared with the value stored in the microcontroller, if the value is less than the lights will be switched on or if the sensed value is greater than the stored value then it will wait for some time and again it will from the first.

While checking for occupants if no one is there in the room then the system will wait for some time (delay), which can be programmed in the microcontroller then it will start from the first step.

6. FLOWCHART:



7. RESULTS:

The proposed system has been implemented in a room with four lights each of 40 watts. Since it is normal classroom where evening classes are also conducted the intensity required has been set to 500 lux which was set as the reference level in microcontroller. Before implementing this system, around 800 watts of energy was consumed per day. After implementing this system in that room it has been considerably reduced to 480 Watts. Thus on using this system a large amount of energy can be saved.

8. CONCLUSION AND FUTURE WORK:

The proposed system can able to reduce the power consumption to the maximum limit and also this system will help us to keep the working environment in a pleasant and comfortable manner.

In this system the number of persons present in the room (Person counter) can be included and also the data transmission from PIR sensor to microcontroller can be implemented through wireless such that the system will become a scalable one in the sense a single system can able to control a large number of rooms. Apart from these things the system can be upgraded to allow the users to configure the intensity of light in real time.

9. REFERENCES:

[1] CIBSE. Reasoning about naming systems. The Chartered Institution of Building Services Engineers, 2002.

[2] Intelligent Energy Conservation System Design Based on Hybrid Wireless Sensor Network Hung-Cheng Chen Department of Electrical Engineering, National Chin-Yi University of Technology, Taiwan, Teng-Fa Tsao Department of Electrical Engineering, Nan Kai University of Technology, Taiwan , Chun-Liang Hsu Department of Electrical Engineering, St. John's University, Taiwan IPCSIT vol. 23 (2012).

[3] Evaluation of Energy-Efficiency in Lighting Systems using Sensor Networks Declan T. Delaney, Gregory M.P. O'Hare, and Antonio G. Ruzzelli CLARITY: Centre for Sensor Web Technologies University College Dublin

[4] Intelligent Lighting System Using Wireless Sensor Networks A.A.Nippun Kumaar , Kiran.G ,Sudarshan TSB Department of Computer Science & Engineering, Amrita Vishwa Vidyapeetham, School Of Engineering, Bangalore Campus, India IJASUC Vol.1, No.4, December 2010

[5] Microchip Technology Inc. PIC16F877A Datasheet, RevisionC, 2003.

[6]http://www.parallax.com/detail.asp?productid=555-28027

[7] Datasheet of NORP 12 LDR

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 121 - 125, 2013, ISSN: 2319–8656

Bragged Regression Tree Algorithm for Dynamic Distribution and Scheduling of Jobs

Navneet Randhawa
Department of Information Technology
Adesh Institute of Engineering and Technology
Faridkot, India

Davinder Singh Gill
Department of Information Technology
Adesh Institute of Engineering and Technology
Faridkot, India

Parneet Kaur
Department of Information Technology
Guru Nanak Dev University
Jalandhar, India

Abstract: In the past few years, Grid computing came up as next generation computing platform which is a combination of heterogeneous computing resources combined by a network across dynamic and geographically separated organizations. So, it provides the perfect computing environment to solve large-scale computational demands. As the Grid computing demands are still increasing from day to day due to rise in large number of complex jobs worldwide. So, the jobs may take much longer time to complete due to poor distribution of batches or groups of jobs to inappropriate CPU's. Therefore there is need to develop an efficient dynamic job scheduling algorithm that would assign jobs to appropriate CPU's dynamically. The main problem which dealt in the paper is, how to distribute the jobs when the payload, importance, urgency, flow time etc. dynamically keeps on changing as the grid expands or is flooded with number of job requests from different machines within the grid.

In this paper, we present a scheduling strategy which takes the advantage of decision tree algorithm to take dynamic decision based on the current scenarios and which automatically incorporates factor analysis for considering the distribution of jobs.

Keywords: Grid Computing; Job Scheduling; Regression Tree; factorization; Scheduler

1. INTRODUCTION

Grid computing is a high performance computing environment to solve large-scale computational demands. It emerged as a next generation computing platform which is a collection of heterogeneous computing resources connected by a network across dynamic and geographically dispersed organizations, to form a distributed high performance computing infrastructure. Job scheduling is a fundamental issue in achieving high performance in grid computing systems, as it is very difficult to tackle the new features of Grid systems such as its dynamic nature and the high degree of heterogeneity of jobs and resources. Grid computing demands are still increasing from day to day due to rise in large number of complex jobs worldwide. So the jobs may take much longer time to complete due to poor distribution of batches or groups of jobs to inappropriate CPU's. The main goal of scheduling in grid computing is to minimize the job completion time and wastage of CPU cycles but scheduling jobs in a heterogeneous grid environment is different compared to parallel architectures. Before scheduling the tasks in the grid environment one must keep in mind the new features of Grid systems such as its dynamic nature and the high degree of heterogeneity of jobs and resources.

The main problem which dealt in the dissertation is how to distributing the jobs when the payload, importance, urgency, flow time, dynamically keeps on changing as the grid expands or is flooded with number of job requests. So in this research work, we proposed a scheduling algorithm "Bragged regression tree algorithm for dynamic distribution and scheduling of jobs" that takes into consideration the heterogeneity of jobs.

This paper is organized as follows: Section 2 describes the present work. Authors Section 3 presents a proposed methodology. Section 4 provides implementation details. Section 5 presents results and discussion. Section 6 presents the conclusion and future scope of this paper. Thus at last the acknowledgement and references are presented.

2. RELATED WORK

In the present work we will discuss the papers related to my work. In [1], N. Muthuvelu, et. al. presents a dynamic job grouping-based scheduling algorithm that groups the jobs according to processing power of the available resource. In this he evaluated a dynamic scheduling strategy that maximizes the utilization of Grid resource processing capabilities, and reduces the overhead time and cost taken to execute the jobs on the Grid. The algorithm reduces the total processing time and cost of the jobs, it also maximizes the resource utilization. However, the algorithm does not take the dynamic resource characteristics into account and it does not pay attention to the network bandwidth of the resources.

In [2] Ng Wai Keat, et. al. proposed a bandwidth-aware job-grouping based scheduling algorithm that schedules jobs in grid systems by taking into consideration of computational capabilities and the communication capabilities of the resources. It uses network bandwidth of the resources to determine the priority of each resource. These jobs are grouped in such a way that, it maximizes the utilization of resources. This algorithm minimizes the network latency, but the scheduling strategy is not ensuring that the resource having a sufficient bandwidth to send the group jobs within required time.

Moreover some of the scheduling algorithms do not consider the dynamic behavior of Grid resources and there characteristics such as [3]. Thus further going through various other papers such as in [6] author found there were some limitations such as the algorithm build in this paper is efficient in all ways except when user changes the priority at dynamic time. In paper [4] author found there were some drawbacks

such as in this algorithm resource are selected in FCFS order, there is no priority for selecting resources.

Therefore there is need to develop an efficient dynamic job scheduling algorithm that would take best decision about assigning of jobs to appropriate CPU's dynamically.

In this paper, we present a scheduling strategy which takes the advantage of decision tree algorithm to take dynamic decision based on the current scenarios and which automatically incorporates factor analysis for considering the distribution of jobs.

2.1 Research Objectives

The following are the objectives of the dissertation:-

i. To develop a framework for scheduling batches (jobs) in grid computing.
ii. To develop parameter models for taking scheduling decisions.
iii. Apply factorization for scheduling algorithm "Bragged Regression Tree Algorithm for Dynamic Distribution and Scheduling of Jobs".
iv. Run task scheduler and get the result verified.

3. Proposed methodology

The methodology used in this proposed work clearly explains what to be done to achieve the objectives defined above. This is done by designing the basic model of job scheduling and work flow model.

3.1 Job scheduling model

The Job scheduling model shown in Figure 1 explains the overall methodology we proposed to obtain our objectives or goals. In this scheduling model, first of all various metrics are calculated which are required for decision making of job scheduling which includes user preferences such as Importance and Urgency, Grid resource such as task payload, time parameters and CPU states and many more. Then our algorithm conducts a factor analysis to find out factors which are urgent and important for decision making analysis and then pass on these extracted factors to the regression tree algorithm. Then this algorithm basically develops multiple linear discriminate functions as per regression tree algorithm. Thus finally the algorithm will help us in taking the dynamic decision based on the current scenarios for scheduling the jobs to appropriate CPU's.

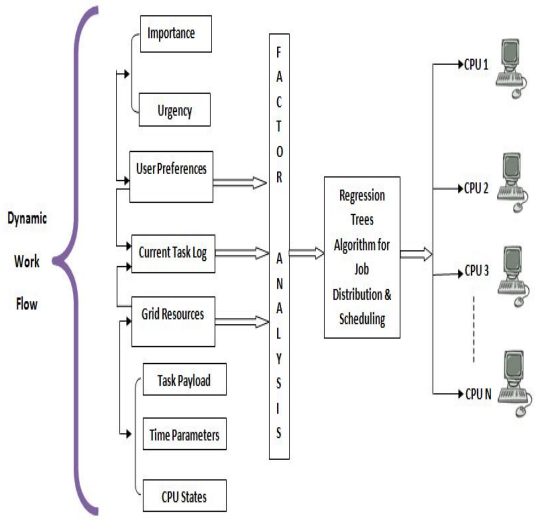


Figure 1 Shows the Job scheduling model

3.2 Work Flow Architecture

The work flow diagram shows the flow of research work to be done to obtain our objectives. In this flow diagram we first, set up Grid environment in which we will calculate batch task matrices such as user preference matrices. Then the log sheet is prepared which includes data set based on matrices and user preferences. Then do the factor analysis which will help in finding the important and useful factors on which variables are dependent. Then take the decisions based on factor analysis done in previous step. The decisions can be, to which CPU what kind of work is to be allotted. Then run the task scheduler and get the results. So this is basically shown in the work flow diagram below in Figure 2

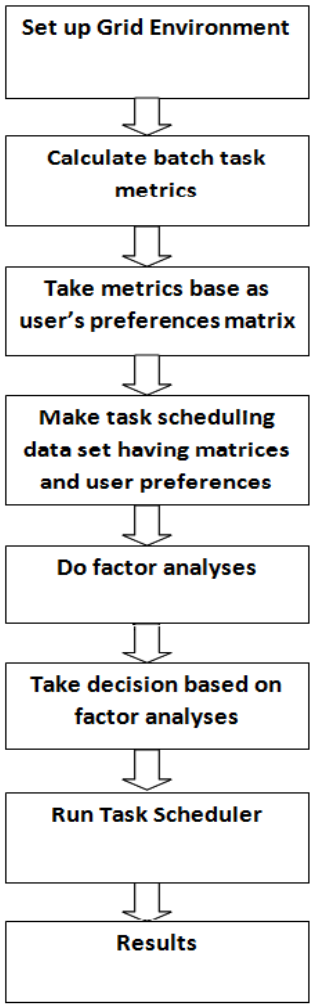


Figure 2 Shows Work Flow Architecture

4. IMPLEMENTATION OF PROPOSED METHODOLOGY

We need to consider some polynomial form of the equation, when we cannot represent in a linear form of equation that is Y= M(x) +C. In a function, whenever a trend line is made, there is no possibility of Y intercept having two values. But if an intercept will have two intercepts or more than that, then it is no longer a function as a definition. By plotting X or Y we only come to know that how X is behaving against Y. But we are unable to find some associative, casual, trivial, scientific facts between the two variables or simply we are unable to understand the nature of two variables. The two variables are

differentiated on the basis of who is dependent on whom and which is independent. So in that case we need to find the regression between two variables. This will help us to know the nature of the variables. The term nature here means, regression basically tries to develop the concept of discriminate function.

The biggest challenge is to design the discriminate function. In simple terms what should we do that, we are able to differentiate from large group of data points, from large domain of variables. If the relationship between X and Y is linear we call it linear discriminate function (LDA). So there are statistical tests like F-test, T-test, Chi-square test or R-square test which help us to determine the overall quality of our model (data points which are being discriminated. But when the relationship between X and Y is non linear and it is even difficult to represent in a polynomial from which may implies that, it has multiple Y intercepts and highly erratic, slow gradient. The best way to find the gradient /slope of polynomial data points which may even be spiral in nature is to run multiple linear discriminate functions. Based on which the multiple Y (predictor) intercepts.

Now here comes another problem. The problem is that, "on but basis multiple linear discriminate function must be run and for each discriminate function, how it must be designed or how it must be validated or tested to test the coefficient of determinant or goodness of the model".

Therefore there arises the need for developing classification trees which are non parametric and non linear in nature following certain if-then-else rules and there is no need for implicit assumptions that the underlined relationship between the predictor value and the dependent are continuous outcome. This model is particularly suited for doing decision making tasks where there is little prior knowledge nor any coherent set of theories or predictions regarding which variables are related and how.

The aim of doing classification and regression tree analysis is to run the algorithm in such a manner that it produces best possible predictive accuracy. Operationally, the most accurate prediction is defined as the prediction with minimum cost, for example if we have a job scheduling task, the classification tree tries to find based on its prediction, which is further based on minimum cost to the resources to which it wants to schedule the job. The notion of cost is basically a generalized way to represent best prediction having lowest misclassification rate which is the performance parameter for its run.

So, we have a choice of either minimizing the cost or minimizing the misclassification rate or both. This process is called designing the tree classifier. In this one of the important task is to select a right size tree as unreasonable big tree may consumes more computational resources and decisions hard to interpret due to enormous size of tree. Typically one should grow the tree size to find the optimal size of the tree. So the four steps involved in this computation are as follows:

1. Specifying the criteria for predictive accuracy,
2. Selecting splits
3. Determining when to stop splitting
4. Selecting the "right-sized" tree

4.1 Algorithm Description

In this research work we have proposed the job scheduling algorithm named "Bragged Regression Tree Algorithm for Dynamic Distribution and Scheduling of Jobs" as shown in Figure 3 below. This algorithm will include the factor analysis and regression analysis for scheduling the jobs to appropriate CPU's. The input to this algorithm is log sheet prepared by simulator, based on the factors taken into account such as make span, flow time, computational time and cost, user preference, number of resources, number of users etc. Thus the algorithm does factor analysis of the given input and gives the important and urgent list of factors as variables to regression analysis which further develops a decision tree. So therefore, this decision tree will tell us which job is to send to what CPU.
Calculation of classification decision tree is as follows:

Data points calculated before uses if –Then – Else rules which will help in sending the job to the appropriate CPU. Thus these rules play vital role in job scheduling algorithm. These can be explained as follows:

If DP >= Threshold Value 1 <=Threshold value 2 then send the job to CPU 1
End
If DP >= Threshold value 3 <= Threshold value 4 then send the job to CPU 2
End
If DP >= Threshold value 4 <= Threshold value 5 then send the job to CPU 3
End
If DP >= Threshold value 5 <= Threshold value 6 then send the job to CPU 4
End

Before we approach the test set, we'll see how well the model has classified the training set. This is not a good estimate of the accuracy the model would have on a test set; it is biased because the classification is being done on the same samples used for training. However, it is an indicator of whether a successful classification of test data may be possible.

Algorithm of Proposed Methodology

```
For each Feature,
        Do factor analysis
            For each top ranked Feature
                Develop a Feature Row.
                Develop a Resource Matrix.

        For each Resource Matrix
            Label each Feature Row with CPU number
        End

    For each Feature Row and label
        Find upper and lower thresholds.

        If there are more sets of lower and upper thresholds

            Develop decision tree

            Else

            Develop decision based on upper and lower
                thresholds for each label and row.
        End
    End
End
```

Figure 3 Shows the Algorithm of Proposed Methodology

5. RESULTS AND DISCUSSION

The results of our proposed algorithm are evaluated according to which the dynamic distribution of jobs to the CPU's is decided. That is decision tree will clearly define which job is to be send to what CPU based on if then else rules applied in classification tree.

The Figure 4 below depicts how each CPU is getting which job or in simple terms, what is the probability against the predicted class or CPU's. It is found that when probability lies between 0.1 and 0.8 the jobs are scheduled to CPU 1. If the probability lies between 0.1 and 0.9 then the jobs are scheduled to CPU 3. But if the probability lies between 0.0 and 0.1 then jobs are scheduled to CPU 4. So at last when probability is found between 0.7 and 1 then jobs are scheduled to CPU 2. This result clearly shows us how the group of jobs is scheduled to different CPU's.

As well as the predicted classes, the predict function outputs a second result, the scores. The score of an observation on a class is the probability that it comes from that class, as indicated by the model. These probabilities are used by the model when making classifications; the class with the highest probability is the one predicted. The scores can be used to give a measure of the confidence the model has in a particular prediction; if a sample has a much higher probability of being one class than all the others, than the prediction will be fairly solid. But if the predicted class is only a little more probable than all the others, the prediction is more shakier.

The scores can be conveniently displayed in a parallel coordinates plot. The four values on the x-axis are the four classes into which samples can be classified. Each sample is represented by a line, and the height of that line at each x-axis value gives the probability that the sample comes from that class. It is clear that all the samples are being predicted with high confidence.

The Figure 5 below shows the structure of decision tree applied to the data points given as inputs, which are the log entries to the grid. Based on If then else rules the figure also shows, the decision making points for identifying the various CPU's based on the feature given to it, which includes the input parameters. So this figure plays very important role in taking the decisions that which job is to be sent to what CPU.

The Figure 6 below shows the decision tree for classification. Moreover, it displays a confusion matrix, which contains a count of the samples, broken down by their actual and predicted classes. The rows represent the samples' actual class and the columns the predicted class. Numbers on the diagonal indicate a correct prediction; off-diagonal entries indicate a misclassification. The model is successfully classifying all samples in the training set, which is good but not unexpected.

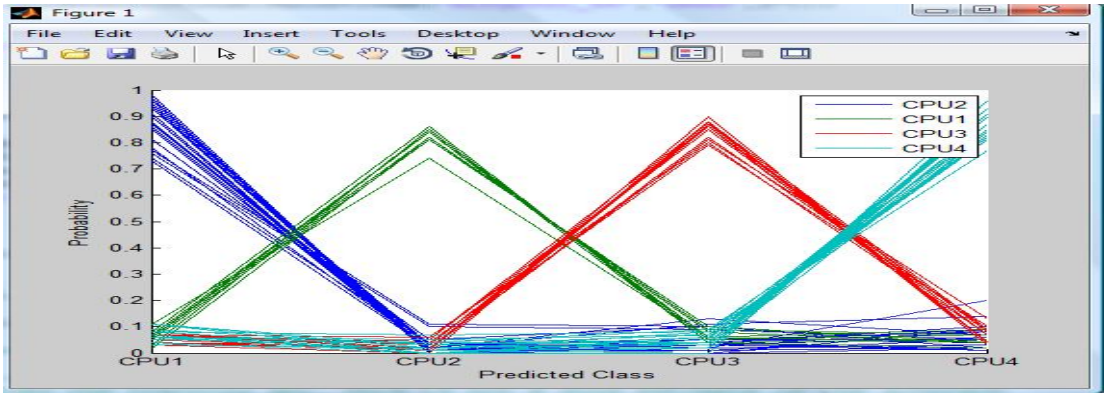


Figure 4 Shows the Probability against the predicted class.

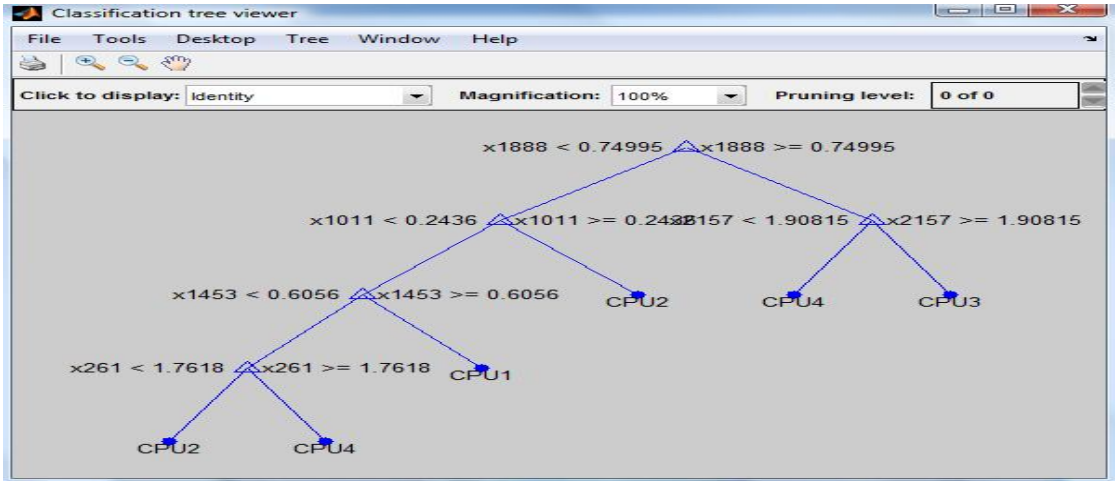


Figure 5 shows the structure of decision tree applied to the data points given as inputs.

```
Decision tree for classification
 1  if x1888<0.74995 then node 2 elseif x1888>=0.74995 then node 3 else CPU2
 2  if x1011<0.2436 then node 4 elseif x1011>=0.2436 then node 5 else CPU2
 3  if x2157<1.90815 then node 6 elseif x2157>=1.90815 then node 7 else CPU4
 4  if x1453<0.6056 then node 8 elseif x1453>=0.6056 then node 9 else CPU1
 5  class = CPU2
 6  class = CPU4
 7  class = CPU3
 8  if x261<1.7618 then node 10 elseif x261>=1.7618 then node 11 else CPU2
 9  class = CPU1
10  class = CPU2
11  class = CPU4
```

	CPU2	CPU1	CPU3	CPU4
CPU2	23	0	0	0
CPU1	0	8	0	0
CPU3	0	0	12	0
CPU4	0	0	0	20

Figure 6 Shows the Decision tree for classification

6. CONCLUSION AND FUTURE SCOPE

In this thesis we have discussed about the problem of job scheduling in heterogeneous grid where basic issue was how to distribute the jobs when the payload, importance, urgency, flow time etc. dynamically keeps on changing as the grid expands or is flooded with number of job requests. So we have proposed a scheduling algorithm named "Bragged Regression Tree Algorithm for Dynamic Distribution and Scheduling of Jobs" which takes the advantage of decision tree algorithm to take dynamic decisions based on current scenario and which automatically incorporates factor analysis for considering the distribution of job. In this research we have taken 4 CPU's and close to 20 parameters from wide choice of 34 parameters. So finally we came to conclusion that, decision tree should be taken into account which will dynamically decide which jobs are to be sending to what CPU's based on nature of job. Moreover by using this algorithm we are able to handle the dynamic job distribution task in heterogeneous environment very effectively with proper utilization of resources and reduction of total computational cost. .

6.1 Future Scope

The proposed approach has been analyzed and can be refined further as a more improved job scheduling algorithm can be considered in which some more factors could be included such as, energy parameters etc. Moreover some QOS requirements can also be taken into account. Furthermore it can't reflect the real computational grid environment that promotes further research in proposed work

7. ACKNOWLEDGMENT

I would like to thank my guide Er. Navneet S. Randhawa, Asstt. Professor and Head, Department of Information Technology, Adesh Institute of Engg. And Technology, Fridkot, India for his valuable assistant in the research work. I am highly grateful to Dr. Vikas Chawla**,** Director-Principal, Adesh Institute of Engineering & Technology, Faridkot, for providing this opportunity to carry out the present thesis work. I would also like to express gratitude to Er. Amit Makkar**,** Asstt. Professor & Head, Department of Computer Science & Engg., Dr. Urvinder Singh**,** Asstt. Professor, Department of Electronics and Communication Engg. and to other faculty members of CSE/IT Deptt., for their intellectual support throughout the course of this work and for providing valuable support in this research work.

8. REFERENCES

[1] Nithiapidary, M., Junyang, L.,Na L. S., Srikumar, V., Anthony, S., and Rajkumar, B. 2005. A dynamic job grouping-based scheduling for deploying applications with fine-grained tasks on global grids. In Proceedings of the 2005 Australasian workshop on Grid computing and e-research.

[2] Ng W. K., Ang T. F., Ling T. C., and Liew C. S. 2006. Scheduling framework for bandwidth-aware job grouping-based scheduling in grid computing. Malaysian Journal of Computer Science.

[3] T.F. Ang and W.K. Ng. 2009. A bandwidth-aware job scheduling-based scheduling on grid computing. Asian Network for Scientific Information.

[4] Quan L., Yeqing L. 2009. Grouping based fine-grained job scheduling in grid computing. In Proceedings of the 2009 First International Workshop on Education Technology and Computer Science.

[5] Raksha S., Vishnu K. S., Manoj K. M., Prachet B. 2010. A Survey of Job Scheduling and Resource Management in Grid Computing. World Academy of Science, Engineering and Technology.

[6] Saeed F. 2009. Efficient Job Scheduling in Grid Computing with Modified Artificial Fish Swarm Algorithm. International Journal of Computer Theory and Engineering.

[7] Jia Y., Rajkumar B., Kotagiri R. 2008. Workflow Scheduling Algorithms for Grid Computing. In Metaheuristics for Schdeuling in Distributed Computing Environments.

[8] Fangpeng D., Selim G. A. 2006. Scheduling Algorithm for Grid Computing: State of the Art and Open Problems.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 126 - 130, 2013, ISSN: 2319–8656

Performance Comparison of Digital Image Watermarking Techniques: A Survey

Namita Chandrakar
Department of Electronics and Telecommunication
Shri Shankaracharya Technical Campus
Bhilai, India

Jaspal Bagga
Department of Information and Technology
Shri Shankaracharya Technical Campus
Bhilai, India

Abstract: Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. In order to provide high quality watermarked image, the watermarked image should be imperceptible. This paper presents different techniques of digital image watermarking based on spatial & frequency domain, which shows that spatial domain technique provides security & successful recovery of watermark image and higher PSNR value compared to frequency domain.

Keywords: Image watermarking, Spatial domain, Frequency domain, Least Significant Bit (LSB), PSNR (Peak Signal to Noise ratio), MSE (Mean Square Error).

1. INTRODUCTION

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the internet & other computer networks. So the growth of e-commerce applications in the world wide web requires the need to increase the security of data communications over the internet. To provide security to these applications data encryption and information hiding techniques were introduced & developed.

There are many approaches like Cryptography, Watermarking and Steganography to transfer the data/image to the intended user at destination without any modifications [1]. A watermark is a secondary image, which is overlaid on the primary image, and provides a means of protecting the image [2].

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Cryptography only provides security by encryption and decryption. There is no protection after decryption & only protected content of the messages but watermarks can protect content even after they are decoded.

Watermarking is a pattern of bits inserted into digital image, audio, video or text file that identifies the file's copyright information such as author and rights [3]. Thus, watermarking is an approach to make sure the data are protected. Watermarking is designed to be completely invisible. Once the watermarking is done, user can send the watermarked image to other computer so that other user is able to read the watermark or the hidden message in the image only if the same algorithm is used. Thus, the watermark can be protected without being revealed.

It may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography literally means, "covered writing". An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. Steganographic methods are in general not robust, that is the hidden information cannot be recovered after data manipulation. Watermarking is robust against attacks. If the existence of the hidden information is known it is difficult, ideally impossible for an attacker to destroy the embedded watermark.

Imperceptibility, robustness, inseparability, security, are the features of digital watermarking.

2. TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be divided into various categories in various ways.

1) According to the type of document to be watermarked, watermarking techniques can be divided into four categories as follows:
   i. Text Watermarking
   ii. Image Watermarking
   iii. Audio Watermarking
   iv. Video Watermarking
2) In other way, the digital watermarks can be divided into three different types as follows:
   i. Visible watermark: Visible watermark is a secondary translucent overlaid into the primary image.

   ii. Invisible-Robust watermark: The invisible-robust watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

   iii. Invisible-Fragile watermark: The invisible-fragile watermark is embedded in such a way that any modification of the image would alter or destroy the watermark.

A robust watermark should survive a wide variety of attacks both incidental and malicious [4, 5]. These watermark attacks can be Simple, Detection-disabling, Ambiguity and Removal attacks. Incidental attacks are those which is applied with a purpose other than to destroy the watermark. Malicious attacks are those which is designed to remove or weaken the watermark.

3. DIGITAL IMAGE WATERMARKING

Figure 1 shows the gereral block diagram of digital image watermarking. Digital Image Watermarking can protect image, video, audio from unauthorized person, noise, copyright etc. The best known image watermarking method that works in the spatial domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information.

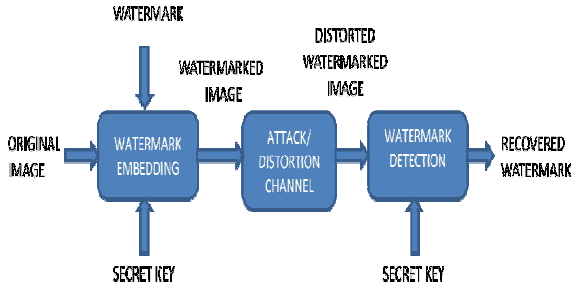


Figure 1. Block Diagram of Digital Image Watermarking

4. PREVIOUS WORKS

The image watermarking techniques can be classified into two categories:

4.1 Spatial-domain techniques (spatial watermarks) :

The spatial-domain techniques directly modify the intensities or color values of some selected pixels. No transforms are applied to the host signal during watermark embedding. Spatial techniques are not very robust against attacks. The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. spatial domain technique, is less time consuming as compare to wavelet or frequency domain techniques.

4.1.1 Least Significant Bit (LSB) Technique

The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels of the cover image. Example of least significant bit watermarking

Image:
10001010 01110100 00011011 01000001 ...
Watermark:
0 1 1 0 ...
Watermarked Image:
1000101**0** 0111010**1** 0001101**1** 0100000**0** ...

Schyndel *et al.* [6] proposed a technique in which a watermark is generated using a m-sequence generator. The watermark was embedded to the least significant bit(LSBs) of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. They showed that the resulting image contained an invisible watermark with simple extraction procedures. But the watermark, was not robust to additive noise. Mohamed Ali HAJJAJI *et al.* [7] proposed watermarking of medical image, in which a set of data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For 10% compression rate, the watermark is successfully recovered. Disadvantage of these technique is that, all the substituted data cannot properly extract when a Gaussian noise is applied in the watermarked image. Puneet Kr Sharma and Rajni, [1] proposed image watermarking & different security issues. To hide logo (secret image) into the cover image they used LSB algorithm. LSB of each of the pixel of the cover image is replaced by the bits of the secret image. Then 2nd LSB of each pixel of the cover image is replaced by the bits of the secret image and so on. Then PSNR and MSE are calculated for different bit substitution from LSB to MSB in image. The PSNR and MSE found for 1st LSB bit substitution was 55.8784 and 0.1680 respectively. Deepshikha Chopra *et al.* [8] proposed invisible watermarking technique and a visible watermarking technique using Least Significant Bit (LSB) algorithm, which replaces the least significant bits of pixels selected to hide the information. They applied various attacks on the watermarked image and their impact on quality of images are measured using MSE and PSNR. Koushik Pal *et al.* [9] proposed biomedical image watermarking technique, modified bit replacement algorithm in spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack , they still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm. Some author name which works on spatial domain with their features and results is shown in Table 1.

Table 1. SPATIAL DOMAIN TECHNIQUE

AUTHOR NAME	FEATURES	RESULT
Mohamed Ali HAJJAJI *et al.* [7]	Data insertion: i) SHA-1 (Secure Hash Algorithme) ii) Error Correcting Code (ECC): Turbo Code Data detection: Harris Corner Detector	For 10% compression rate, the watermark is successfully recovered (for the IRM and Echographic medical images).
Puneet Kr Sharma and Rajni [1]	i) Pseudo-random number generator ii) LSB embedding algorithm	LSB or 1st Bit Substitution PSNR = 55.8784 & MSE = 0.1680 8th Bit Substitution PSNR = 14.3467 & MSE = 2.3900e+003
Chopra *et al.* [8]	Least Significant Bit (LSB) algorithm	LSB or 1st Bit Substitution PSNR = 54.87 & MSE = 0.21 MSB or 8th Bit Substitution PSNR = 14.3467 &

		MSE = 2.3900e+003
Sharma *et al.* [16]	i)A pseudo random number generator ii)The information hiding and extraction system iii)Visual Cryptography iv)Two different cover images are used for covering the secret share	Watermarked image for baboons PSNR(with one LSB) (db) = 54.45 PSNR(with three LSB) (db)= 44.15 Watermarked image for leena PSNR(with one LSB) (db) = 51.15 PSNR(with three LSB) (db)= 44.17

4.2 Frequency-domain techniques (spectral watermarks):

The frequency-domain techniques modify the values of some transformed coefficients. The frequency-domain technique first transforms an image into a set of frequency domain coefficients. The watermark is then embedded in the transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations. Finally, the coefficients are inverse transformed to obtain the watermarked image. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. This technique is complex and watermark cannot be easily recovered at the receiver end as compared to the spatial domain technique.

Xiang-Gen Xia *et al*. [10] proposed a watermarking technique based on the Discrete Wavelet Transform (DWT). They performs two–level decomposition using the Haar wavelet filters. The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. Maha Sharkas *et al*. [11] Senior Members IEEE, proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the watermarked image. They applied compression, low pass filtering, salt and pepper noise and luminance change attack into the watermarked image to increase the robustness of the technique. In all four attacks secondary watermark was detectable. Cheng *et al*. [12] proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter. P.Ramana Reddy *et al*. [13] proposed an algorithm that embeds and extracts the watermark in frequency domain and it is checked for salt and pepper & Gaussian noise attacks. They applied watermark in the DWT coefficients of the original image.

$$I_w(x,y)= I(x,y) +k.w(x,y) \quad (1)$$

Where $I_w(x,y)$ represents watermarked image, k denotes the gain factor. Robustnest of the watermarked image increases with the increase in gain k but the quality of the final watermarked image is reduced. Preeti Gupta, [14], proposed cryptography based blind image watermarking technique that embed more number of watermark bits in the gray scale cover image. They applied blind watermarking technique that uses watermark nesting and encryption. An extra watermark is embedded into the main watermark then main watermark is embedded into the DWT domain of the cover image. This technique embeds more number of bits in the cover image. Mistry, [15], proposed digital image watermarking and compared different digital watermarking methods. Image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. This paper introduced Spatial domain (like LSB) and transform domain (like DCT, DWT) methods. Authors found that DCT and DWT watermarking is comparatively much better but complex than the spatial domain encoding. Some author name which works on frequency domain with their features and results is shown in Table 2.

Table 2:FREQUENCY DOMAIN TECHNIQUE

AUTHOR NAME	FEATURES	RESULT
Harpuneet Kaur [3]	i) Watermark nesting (at level 2), Means embed one watermark in other and encryption. ii) Used DWT based technique	PSNR of main watermark after embedding watermark1 in it = 17.3239 dB PSNR of gray scale cover image after embedding watermarked watermark = 37.1587dB
Xia-mu Niu *et al.* [17]	i)Gray level digital watermark ii) Stack filter's threshold decomposition technique iii) DCT	PSNR = 30.7 dB Disadv- due to the multiple watermarks, the PSNR of the watermarked image isnot very high compared with traditional method.
Xiang-Gen Xia *et al.* [10]	i)Multiresolution watermarking method,	They test algorithm with common image

	ii)DWT, iii)Pseudo-random codes, iv) Haar DWT	distortions. Signature can be detected using DWT compared to DCT approach.
Maha Sharkas *et al.* [11]	i)Dual watermarking technique ii) DWT domain	PSNR = 44.1065dB Disadv-Secondary watermark was still detectable when multi threshold DWT tech was applied on the watermarked image.

Table 1 and Table 2 shows comparision of two digital image watermarking techniques, which is based on PSNR values and their results. From table it is clear that we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly. And also complexity of embedding and extracting watermark in frequency domain is increases and more difficult compared to spatial domain. Spatial domain provides successful recovery of watermark at receiver end.

Here different watermarking methods have been presented . Most watermarking methods are based on small, pseudorandom changes are applied to selected Coefficients in the spatial or transform domain. Spatial domain watermarking schemes are in general less robust toward noise like attacks [5]. But the big advantage of using Spatial domain watermarking schemes is that the watermark may easily be recovered if the image has been cropped or translated. This is less obvious if the frequency domain is used. Cropping in the spatial domain results in a substantially large distortion in the frequency domain, which usually destroys the embedded watermark. In the case of DCT domain, if DCT blocks are watermarked, it is important to know the block position for successful watermark decoding. The similar drawbacks in the case of wavelet domain, because the wavelet transform is neither shift nor rotation invariant. Due to the simplicity and efficiency of the spatial domain, watermark in the spatial domain is most used.

5. CONCLUSION

Different techniques of digital image watermarking, based on spatial and frequency domain techniques have been discussed. On the basis of above survey it is clear that spatial domain is most widely used technique because the watermark can successfully & easily be recovered if the image has been cropped or translated. as compared to frequency domain.

On the other hand frequency domain provides more security but at the same time recovery of watermark at the receiver end is more difficult because the complexity increases. Successful recovery of watermark cannot be provided by the frequency domain techniques.

6. RESULT

Literature survey shows that the watermark may be of visible or invisible type and each method has its own strengths and weaknesses.The quality of watermarked images is measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case the value of PSNR & MSE should be infinite and zero respectively . But it is not possible for watermarked image. So, large PSNR and small MSE is desirable.

7. REFERENCES

[1] Puneet Kr Sharma and Rajni, "*Analysis of Image Watermarking using Least Significant Bit Algorithm*" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp. 95-101.

[2] Manpreet Kaur , Sonika Jindal , Sunny Behal "*A Study of Digital Image Watermarking*" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905, pp. 126-136.

[3] Harpuneet Kaur, "*Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data*" Computer Science & Engineering Department, Thapar Institute of Engineering & Technology. May 2006, pp. 1-69.

[4] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi (Oct. 2001), "*A survey on watermarking application scenarios and related attacks*", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993.

[5] Frank Hartung, Martin Kutter, "*Multimedia Watermarking Techniques*", Proceedings of
The IEEE, July 1999, Vol. 87, No. 7, pp. 1085 – 1103.

[6] R. Schyndel, A. Tirkel, and C. Osborne, "*A Digital Watermark*," *Proc. IEEE Int. Conf. on Image Processing*, Nov. 1994, vol. II, pp. 86-90.

[7] Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE, "*A Watermarking of Medical Image: Method Based "LSB"*", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12, December 2011, ISSN 2079-8407, pp. 714-721.

[8] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "*Lsb Based Digital Image Watermarking For Gray Scale Image*" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), pp. 36-41.

[9] Koushik Pal, Goutam Ghosh, Mahua Bhattacharya, *" A Comparative Study between LSB and Modified Bit Replacement (MBR) Watermarking Technique in Spatial Domain for Biomedical Image Security"* International Journal of Computer Applications and Technology (2278 - 8298) Volume 1 – Issue 1, 2012, pp. 30-39

[10] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce, "*A Multiresolution Watermark for Digital Images*" Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[11] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, Senior Member IEEE, "*A Dual Digital-Image Watermarking*

Technique" World Academy of Science, Engineering and Technology 5 2005, pp. 136-139.

[12] Lu, W., Lu, H. and Chung, F.L. (2006) "*Robust digital image watermarking based on subsampling*" Applied Mathematics and Computation, vol. 181, pp. 886-893.

[13] P.Ramana Reddy, Munaga. V.N.K. Prasad, D. Sreenivasa Rao, "*Robust Digital Watermarking of Color Images under Noise attacks*" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009, pp. 334-338.

[14] Preeti Gupta, "*Cryptography based digital image watermarking algorithm to increase security of watermark data*" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 1 ISSN 2229-5518, pp. 1-4.

[15] Darshana Mistry, "*Comparison of Digital Water Marking methods*," 21st Computer Science Seminar SA1-T1-7. IJCSE, Vol. 02, No. 09, ISSN : 0975-3397 , 2010, pp. 2905-2909.

[16] Mr. Abhay Sharma, Mrs. Rekha Chaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, *" New Improved and Robust Watermarking Technique based on 3rdLSB substitution method*" International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 ISSN 2250-3153, pp. 1-4.

[17] Xia-mu Niu, Zhe-ming Lu and Sheng-ho Sun, "*Digital Watermarking of Still Images with Gray-Level Digital Watermarks*" Department of Automatic Test and Control Harbin lnstitute of Technology Harbin, P. R. China, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, February 2000, pp. 137-145.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 131 - 136, 2013, ISSN: 2319–8656

Challenges, Issues and Research directions in Optical Burst Switching

Terrance Frederick Fernandez
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India

Megala.T
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India

Sreenath.N
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India

Abstract: Optical Burst Switching architecture (OBS) is based on buffer-less WDM network that provides unbelievably huge bandwidth for communication. A brief review on OBS architecture along with its supporting protocols is studied here. This architecture suffers from various issues and these complications along with the future research directions are reviewed here.

Keywords: Optical Burst Switching, Contention resolution, AON, Routing and Wavelength Assignment, OBS research issues.

1. INTRODUCTION TO OBS

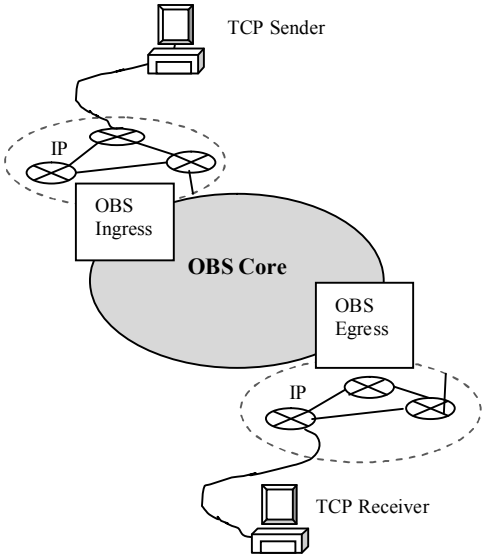


Figure 1. OBS Network Architecture

Optical Switching architecture has become the research focus [1], [2] in recent years due to the heavy demand in huge bandwidth and efficient network resource allocation. Three Optical switching architectures are available and they are Optical Circuit Switching (OCS), Optical Packet Switching (OPS) and Optical Burst Switching (OBS). Among these schemes, OBS [3] combines the merits of mature electronic process capability and the high-capacity optical transport capability. Multiple packets that belong to the same egress node are packed into a single Data Burst (DB) at the ingress nodes. Control information for this DB is sent ahead on separate wavelength and is called Burst Header Packet (BHP). BHPs are processed electronically at each intermediate core nodes to reserve network resources before the arrival of the DBs.

1.1 OBS Assembly

The Burst assembly happens at the input node ingress, where the packets belonging to the same destination are grouped into a single Burst in order to switch all-optically into the core nodes.

- Timer based Burst Assembly Mechanism.
- Burst Length (threshold) based Burst Assembly Mechanism.
- Hybrid/Mixed Burst Assembly Mechanism.
- Composite Burst Assembly Mechanism.
- Optimized/Adaptive Burst Assembly Mechanism.

An assembled burst is sent into the core at periodic/fixed time intervals while the Data Bursts are of variable lengths for Timer based Burst Assembly Mechanism [4]. On the contrary, the burst lengths are fixed and are generated at non-periodic/variable time intervals for Burst; length-threshold based Burst Assembly Mechanism [4]. In some special cases, packets of different classes but belonging to same bursts are combined. Here, these are placed from head of the burst to the tail of the bursts in order of decreasing classes and this is called as composite burst assembly algorithm [4]. In hybrid/mixed burst assembly mechanism, the bursts are assembled and sent either if the timer expires or the burst length is reached [5]. Dynamic adaptive threshold on burst length is set in order to optimize the overall performance in OBS for QoS sensitive traffic [5].

1.2 OBS Routing

Types of routing Strategies include

- Proactive/Static routing
- Dynamic congestion-based routing

The Proactive approach is based on adaptive use of multiple paths between edge nodes. In dynamic congestion based routing the core nodes in the network gather the load information on their output links and send feedback to all the edge nodes, so as to enable the edge nodes to balance the load and thus routing is done.

There are two subtypes in dynamic congestion-based routing:

- Fixed alternate shortest path dynamic congestion-based routing
- Least congested dynamic route calculation

The other routing strategies are [6]:

- Distributed routing
- Isolated routing approach

Distributed routing algorithm [7] introduces the problem of inaccuracy in network state information. The routing decisions performed by this algorithm are optimal as long as this information perfectly represents the actual network state, what is impossible to achieve in real network. Moreover, distributed routing involves additional signalization complexity so as to exchange the state information inside the network. The isolated routing approach [7] which performs the path selection based only on local node/link state information minimizes problems encountered in isolated routing algorithm. However, its suboptimal nature since it only considers the congestion of the current node and its links may result in worse performance results.

In [8], three different routing algorithms have been implemented, namely:

- Shortest Path (SP).
- Multi-Path (MP) and
- Bypass (BP).

The SP algorithm is used here as a reference for the later two algorithms could be classified as isolated adaptive routing algorithms. SP assigns a route of the shortest distance between source and destination nodes for each burst. If more than one such path exists, the first computed is selected. In this case, only one route is available for a burst. Therefore, if there is a contention between burst reservations that cannot be resolved in the frequency and time domains the burst is lost.

In MP algorithms number of paths are pre-established between each pair of source and destination nodes. The algorithm makes a routing decision for each individual burst selecting the shortest path available, i.e. the path that has free output channel available for resources reservation procedure. Therefore, the first route that is analyzed is the SP and in case the burst cannot be transmitted on it the next one of a length equal or higher is checked. After path selection in source node the burst follows this path towards the destination node. If the congestion occurs inside the network the routing algorithm can reroute the burst to the other path under condition that this path is originated and terminated in the same pair of nodes as the burst source and destination nodes. In the evaluation study we consider that there are 4 paths available between each pair of source-destination nodes.

BP algorithm assumes that a burst can by-pass congested link by transmitting it through another node. In particular, if there are no resources available for burst transmission on specific output port, the burst is allowed to make one additional hop through other node with the objective to return to its default path in the next hop. Regarding the isolated adaptive routing, the isolated term means that the routing decision is made on base of local node state information. Likewise, the adaptive routing term expresses capability to dynamic changes in route selection in order to perform the best decision. Both considered isolated adaptive routing takes into account availability of transmission resources for a given burst on its default output port. In case, there are not free resources the algorithm tries to reroute a burst on other path (if it is available) with other output port according to the routing strategy, by selecting either one of multiple paths in MP or bypassing congested link in BP.

Therefore, the goal of the study is to investigate the capability of pure isolated adaptive routing algorithms to distribute the traffic and reduce data losses in connection-oriented OBS networks.

1.3 Traffic Distribution in OBS

Traffic distribution in OBS can be done at the Burst Level (BL) by making a path selection for each newly incoming burst at ingress node according to a calculated distribution probability within a time period. It can also be made at the Flow Level (FL) by making a path selection for each newly incoming flow at ingress node according to a calculated distribution probability within a time period and all bursts within a particular flow will follow the same path. Balance the traffic load by shifting incoming bursts along the primary and secondary paths. Probe the sent packets periodically and sent through the least congested path. Always aim to minimize Burst loss and average transfer delay [8].

- Equal Proportion Multipath Routing (EPMR).
- Hop Length Multipath Routing (HLMR).
- Adaptive Alternative Routing Algorithm (AARA).
- Gradient Projection Multipath Routing (GPMR).

GPMR-BL (Burst level) outperforms all. Burst Loss for GPMR-BL is 20% less than AARA-BL for low traffic loads and also improves with medium/ high loads. GPMR-BL converges quickly (with sudden traffic increase). Burst level probability first decreases and then increases as measurement time window increases. For small Window size, GPMR-BL cannot work with inaccurate traffic information. For large Window size, GPMR cannot adapt to changing traffic load in networks [15].

1.4 Scheduling in OBS

- Horizon Scheduling.
- Latest Available Unused Channel with Void Filling (LAUC-VF).
- Minimum Starting Void (MSV).
- Constant Time Burst Resequencing (CTBR)

The latest time at which a channel is currently scheduled to use is called as a “horizon”. In the horizon scheduling algorithm, the horizon scheduler selects the channel with latest horizon from the set of channels whose horizons are less than burst arrival times. LAUC-VF keeps track of all voids in a channel and schedule bursts in one of the voids. If more than one void can fit a burst then the one with latest beginning time is assigned.MSV uses a geometric approach (binary search tree) that minimizes the distance between the starting time of the void and starting time of the burst. CTBR is the “Optimum Wavelength Scheduler”. Instead to process burst as soon as the BHP arrive, we delay scheduling of the bursts and process in order of expected Burst arrival time. BHP is processed not in its arrival times but at the arrival times of Data bursts. The link utilization of LAUC-VF is higher than horizon scheduling but gets slower with huge number of voids.

Table 1. Time Complexity for Scheduling Algorithms

Complexity	Scheduling Algorithm
O (log h)	Horizon Scheduling
O (log m)	Latest available unused channel - Void filling
O (log m)	Minimum Starting Void
O (1)	Constant Time Burst Resequencing

1.5 Signaling in OBS

The wavelength reservation algorithm for OBS network was adopted from “ATM Block Transfer (ABT)”. There are two versions of ABT and they are [7].ABT with immediate reservation and ABT with delayed reservation. In the former, the wavelength is immediately reserved and Data Bursts are sent on receiving Burst Header. If wavelength cannot be reserved then the DB is dropped. In the latter, the header and

Bursts are separated by a period called "Offset Time (OT)".Based on the above two versions of ABT, there are three Burst Reservation schemes in OBS

- Tell And Go (TAG) protocol.
- Just in Time (JIT) protocol.
- Just Enough Time (JET) protocol.
- Horizon.

TAG does immediate reservation with Zero/ minimum offset. DB is delayed by FDL while CP is processed. Negative Acknowledgement (NACK) is sent if DB is dropped.JIT does immediate reservation with Zero/ minimum offset. DBs and CPs are separated by time slot. In-band Terminator (IBT) at the end of each DBs to release wavelength.JET does delayed reservation. CPs and DBs are separated by an "Offset Time (OT)". OT corresponds to the number of hops between source and destination. Delayed reservation is required for OBS networks, because the travelling speed of the DB is usually slower than that of the CP. It is because the DB can cut through the switches without buffering/processing delay unlike the CP which has that. So, this reservation would deny the catching up of the DB with its CP. Horizon [12] based on the knowledge of the latest time at which the channel is currently scheduled to be in use.

1.6 Contention Resolution in OBS

"Contention" occurs in OBS if two or more incoming bursts contend for the same output wavelength at the same link [11]. This contention is to be resolved and is done by

- Optical Buffering.
- Wavelength Conversion.
- Burst Deflection Routing (Alternate Routing).
- Burst Segmentation.
- Burst re-transmission.
- Burst TCP (BTCP) [12].

If a contention occurs at any OBS core node without any of the above contention schemes or if the degree of contention is so high and it is not able to tackle the contentions then the network would opt for a policy called "Dropping Policy (DP)". There is an extension of the DP with retransmission [13], where we may retransmit and drop DBs that have experienced fewer retransmissions. Buffering in OBS is done in time domain by the use of the Fiber Delay Lines that limit the amount of time a burst could reside unlike electronic buffers, where a packet can stay in the buffer for an undefined time. Electronic buffers are present at the electronic edge nodes. Optical technology is immature and buffers are not invented for optical core nodes. It is impossible to delay the burst for infinite period of time using Fiber Delay Lines (FDLs). It is done in "Space domain". Wavelength Conversion is the capability of the optical network to convert an input wavelength to a desired output wavelength. It is done in spectral/Wavelength domain. It is immature, costly and produces linear effects such as noise.

Break the assembled data-burst into a number of segments and the process is called "Segmentation" [14]. "Segments" are basic transport units [8] and are electronic transport units invisible in optical domain [15]. There are two segmentation policies and they are: Head dropping policy and tail dropping policy. In the former, the head of the contending burst is dropped. In the latter, the tail of the contending burst is dropped. In [11], 'The modified-tail dropping policy' was proposed, where the tail of the contending burst is dropped only if the number of segments in the tail is less than the total number of segments in the contending burst . On the other case, the entire contending burst is dropped. This reduces the probability of a short burst preempting a longer burst and minimizes the number of packets lost during contention. Deflection Routing is done in a "Space domain". If there is a contention at the preferred link then the burst is forwarded at any available output. This is also called as "Hot Potato Routing" [11]. In [8], two different algorithms for contention resolution are described in frequency and time domains, namely

- *MINLEN* that is a Horizon type and
- *VF-MM* that is a Void-Filling type.

The Horizon algorithms base on the knowledge of the latest time at which the channel (wavelength) is currently scheduled to be in use. The MINLEN allocation algorithm looks for a free channel with a minimum queue, i.e. with the earliest possible allocation. The Void Filling scheduling algorithm can make a reservation of free resources even if they are located between two reservations already done. Basing on this approach the VF-MM algorithm tries to place a new reservation in a space of a minimum gap.

2. OBS CHALLENGES

2.1 Burst Segmentation in Practical System

Challenges when implementing burst segmentation in practical systems were:

- **Switching time:** Since the system does not implement buffering or any other delay mechanism, the switching time is the number of packets lost during reconfiguring the switch due to contention. Hence, a slower switching time results in higher packet loss. While deciding which burst to segment, we consider the remaining length of the original burst, taking the switching time into account. By including switching time in burst length comparisons, we can achieve the optimal output burst lengths for a given switching time.
- **Segment boundary detection:** In the optical network, segment boundaries of the burst are transparent to the intermediate nodes that switch the burst segments all-optically. At the network edge nodes, the burst is received and processed electronically. Since the burst is made up of many segments, the receiving node must be able to detect the start of each segment and identify whether or not the segment is intact. If each segment consists of an Ethernet frame, detection and synchronization can be performed using the preamble field in the Ethernet frame header, while errors and incomplete frames can be detected by using the CRC field in the Ethernet frame.
- **Trailer creation:** The trailer has to be created electronically at the switch where the contention is being resolved. The time to create the trailer can be included in the header processing time, at each node.

2.2 Challenges in Contention Resolution Strategies

- A burst can reside in an optical buffer only for a specified amount of time unlike electronic buffers.
- Wavelength conversion produces linear effects like 'noise' and it is costly.
- In tail dropping segmentation scheme, the header contains the total burst length even if the tail is dropped

[15], and thus downstream nodes are unaware of truncation. This is called "*Shadow Contention*".

- In head dropping segmentation scheme, there will be more out-of-order delivery [15] in contrast to the tail dropping policy where the sequence is maintained.
- Long bursts passing through different switches experience contention at many switches [15].
- Bursts of bigger lengths cannot be stored at the "Fiber Delay Lines" [7].
- Burst deflection routing dynamically deflects the Bursts in an alternate path due to contention in the primary path and is usually longer than the primary path. Thus it increases the propagation delay [5].
- The deflected bursts might also loop multiple times wasting network bandwidth [14].

2.3 TCP over OBS Challenges

It is quite normal to employ OBS as core architecture under TCP as it constitutes almost 90% of the current internet traffic and thus when an optical core network, i.e.., Optical Burst Switching is considered there would be number of challenges namely:

- OBS experiences Bandwidth Delay Product (BDP) , thus suffers from speed mismatch with TCP. Even if the TCP Scaling option is employed to reach congestion window to 4MB from 64KB longer time would be consumed.
- The Delayed ACK must be used in TCP over OBS as in reality all TCP segments cannot be included in a single burst which causes further delay. .
- High Speed TCP (HSTCP) was proposed for high BDP networks that offers bad throughput for Burst losses.

3. OBS ISSUES

In [13], a TCP over OBS network is considered. The throughput of various implementations of TCP namely TCP Tahoe, Reno and New Reno are done. An experimental study represented results of throughput of TCP source variants, Tahoe, Reno and New Reno. The network parameters such as, bandwidth, packet size, congestion window size and queue-limit were considered for this experiment. The vital issue in this paper is TCP variants like TCP Vegas, TCP SACK, and TCP FACK etc.., were not considered. Most cases consider TCP Westwood over OBS networks.

In [17], a performance evaluation of an OBS router was done. It was said that OBS with LPI can reduce energy consumption up to 60% at low loads. A desired scheduler buffer size to minimize the overall packet blocking probability of OBS was considered in [18]. A novel label Switched path design for Generalized MPLS over OBS was modeled in [19].

The Control plane in IP and optical domains are usually separated. But in [20], a "unified control plane" is made for end-end service provision. Another contention resolution technique by proposing new CRT based on control packet buffering was done in [21]. Mathematical model also been proved to analyze the performance of OBS network core node with JIT, buffering is done on electronic node. The Control Packet that fails reserving required amount of resource were not dropped immediately, rather electronically buffered for some threshold time, the time is decided at ingress node depend on each burst duration. Offset time must be increased so that to avoid the burst to reach the core node are still not ready. New quality theory impatience concept was mathematically driven .JIT is used; slight modification is done at MAC layer performance enhancing technique.

LPI was proposed by IEEE 802.3az task Force to reduce energy consumption in network devices. In [22] a Wake Transition Decision algorithm was proposed to maximize sleep time thus improving performance. A hybrid Wavelength Division Multiplexing and Optical Code Division Multiplexing (WDM/OCDM) scheme is used to mitigate the blocking probability of OBS networks in [23]. Fiber Delay Lines are Optical buffers that can tap/delay an optical data for a finite amount of time and they are costly. An aim to minimize this issue, OBS Tune and Select (TAS) node architecture was proposed in [24], where a dedicated input/output port of the switch is assigned to an FDL shared between the output ports in a feedback configuration (TAS-shFDL).

In [25], several alternative TCP protocols were reviewed and their performance in terms of throughput and fairness were compared to select the most suitable TCP protocol for end-to-end Grid data transmission all the proposed methodologies are demonstrated and evaluated on an actual OBS/WSON testbed with both control and data planes, allowing the verification of their feasibility and effectiveness, and obtaining valuable insights for deploying the proposed solutions into real consumer Grid networks. However, even though state-of-the-art techniques are being considered, there are three major limitations namely Limitation of network infrastructures, limitation of resource discovery and management Schemes an limitation of end-to-end transmission control protocols (TCP) that prevent the wide deployment of the consumer Grid. In order to address these above 3 issues, an integrated OBS/wavelength switched optical network (WSON) was proposed with the assistance of a self-organized resource discovery and management scheme to support consumer Grid applications. These proposed solutions are experimentally demonstrated and evaluated on an actual OBS/WSON testbed. An experimental demonstration and evaluation of dynamic provisioning of consumer Grid services by using the integrated OBS/WSON as a network infrastructure, SRDM for resource discovery and management, and High-speed TCP were done.

4. OBS RESEARCH DIRECTIONS

OBS has attracted lot of researchers due to its ability to achieve dynamic and on-demand bandwidth allocation that offers improved network economics and enables control and management integration. Optical Burst Switching is currently one of the biggest research topics under study and the research issues in it can be broadly classified into two namely: Security issues in OBS and QoS issues in OBS. The QoS issues were discussed in (SECTION 3) and can be sub-categorized based on two kinds of blocking either QoS issues due to contention or QoS issues due to Bit Error Rates.

At the industrial level, commercial products were very rarely made based on OBS and the only company that offers this product is "Matisse networks" as the technology is still immature [10]. To model or design an OBS node, there is a requirement of test beds or simulators. Few of the OBS simulations were implemented on test beds. These OBS network test-beds would not be imported to most Asian countries like India, Sri Lanka, and Pakistan etc. So, these researchers are forced to a single option namely, implementing on a simulator. On the other hand, simulators that are available for Optical Burst Switching do not cater the entire requirements that are needed to simulate the entirety of a particular OBS protocol. The survey of various simulators was done in [26], [27], and [28]. It was inferred that

simulators like NCTUns could satisfy all the specs for simulation but are not freely available. Some others like JAVOBS, DESMO-J, OBSIM etc use Java as its building programming language, thus much time is consumed for the temporary compilation of user code to byte code. This code does not become executable code until the program is actually run.

5. CONCLUSION

Optical Burst Switching is an efficient architecture to utilize the enormous bandwidth provided by the optical fiber and cater communication at the network cores with minimal Burst losses. OBS suffers from a phenomenon called as contention as it cuts-through switches unlike other architectures where the data is stored and forwarded. Various contention resolution mechanisms available were thus discussed highlighting their merits. Challenges thus faced when these resolution policies are used are also discussed and hence concluded that every contention policy carries one issue or another. Finally, it was discussed that research directions on OBS can be reviewed either based on QoS constraints or security constraints.

6. REFERENCES

[1] B. Mukherjee, *"Optical WDM Networks"*, New York: Springer, 2006, ch. 17–18.

[2] M. J. O'Mahony, C. Politi, D. Klonidis, R. Nejabati, and D. Simeonidou, "Future optical networks," *Journal of Lightwave Technology*, vol. 24, pp. 4684–4696, 2006.

[3] C. Qiao and M.Yoo, "Optical burst switching (OBS) A new paradigm for an optical internet," *Journal of High Speed Networking*, vol. 8, no. 1, pp. 69–84, 1999, Special Issue on Optical Networking.

[4] Farid Farahmand, Jason Jue , Vinod Vokkarane,"A Layered Architecture for Supporting Optical Burst Switching" , Proceedings of the Advanced Industrial Conference on Telecommunications, 2005 IEEE.

[5] Basem Shihada and Pin-Han Ho, University of Waterloo, "Transport Control Protocol in optical Burst Switched Networks: Issues, solutions, and Challenges", IEEE Communications Surveys & Tutorials 2nd Quarter 2008.

[6] M. Klinkowski, D. Careglio, Elias Horta and J. Solé-Pareta, "Performance Analysis of Isolated Adaptive Routing Algorithms in OBS networks".

[7] Andrew S Tanenbaum, "Computer Networks", Prentice Hall 1988.

[8] Yong Liu, Gurusamy Mohan, Senior Member, IEEE, Kee Chaing Chua, and Jia Lu, " Multipath Traffic Engineering in WDM Optical Burst Switching Networks" , IEEE Transactions on Communications, Vol. 57, No. 4, April 2009.

[9] Pushpendra Kumar Chandra, Ashok Kumar Turuk, Bibhudatta Sahoo , "Survey on Optical Burst Switching in WDM Networks", ©2009 IEEE.

[10] Samrat Ganguly, Sudeept Bhatnagar, Rauf Izmailov, Chunming Qiao , "Multi-path Adaptive Optical Burst Forwarding", ©2004 IEEE.

[11] Onur Ozturk, Ezhan Karasan, Member, IEEE, and Nail Akar, Member, IEEE, "Performance Evaluation of Slotted Optical Burst Switching Systems with Quality of Service Differentiation", Journal of lightwave technology, vol. 27, no. 14, July 15, 2009.

[12] Jiangtao Luo , Jun Huang, Hao Chang, Shaofeng Qiu, Xiaojin Guo and Zhizhong Zhang Chongqing, " ROBS: A novel architecture of Reliable Optical Burst Switching with congestion control" ,University of Post & Telecom, Chongqing 400065, P.R. China , Journal of High Speed Networks 16 (2007) 123–131, IOS Press.

[13] L. Kim, S. Lee, and J. Song, "Dropping Policy for Improving the Throughput of TCP over Optical Burst-Switched Networks," ICOIN, 2006, pp. 409–18.

[14] T. Venkatesh, A. Jayaraj, and C. Siva Ram Murthy, Senior Member, IEEE, "Analysis of Burst Segmentation in Optical Burst Switching Networks Considering Path Correlation", Journal of Lightwave technology, Vol. 27, No. 24, December 15, 2009.

[15] Vinod M. Vokkarane, Jason P. Jue, and Sriranjani Sitaraman, "Burst Segmentation: An Approach For Reducing Packet Loss In Optical Burst Switched Networks", 2002 IEEE.

[16] Sodhatar, S.H.; Patel, R.B.; Dave, J.V, "Throughput Based Comparison of Different Variants of TCP in Optical Burst Switching (OBS) Network", 2012 International Conference on Communication Systems and Network Technologies (CSNT).

[17] Wonhyuk Yang; Jin-Hyo Jung; Young-Chon Kim, "Performance evaluation of energy saving in core router architecture with Low Power Idle for OBS networks", 2012 International Conference on Information Networking (ICOIN).

[18] Ichikawa, H.; Kamakura, K., "Dimensioning an scheduler buffer in OBS networks using forward resource reservation", 2012 International Conference on Computing, Networking and Communications (ICNC).

[19] Pedroso, P.; Perelló, J.; Careglio, D.; Klinkowski, M.; Spadaro, S,"Optimized Burst LSP Design for Absolute QoS Guarantees in GMPLS-Controlled OBS Networks",IEEE/OSA Journal of Optical Communications and Networking.

[20] Dongxu Zhang; Lei Liu; Linfeng Hong; Hongxiang Guo; Tsuritani, T.; Jian Wu; Morita, I, "Experimental demonstration of OBS/WSON multi-layer optical switched networks with an Open Flow-based unified control plane", 16th International Conference on Optical Network Design and Modeling (ONDM), 2012.

[21] Abd El-Rahman, A.I.; Rabia, S.I.; Shalaby, H.M.H, "MAC-Layer Performance Enhancement Using Control Packet Buffering in Optical Burst-Switched Networks", Journal of Lightwave Technology.

[22] Dong-Ki Kang; Won-Hyuk Yang; Jin-Hyo Jung; Young-Chon Kim, "Wake Transition Decision algorithm for energy saving in OBS network with LPI", International Conference on Computing, Networking and Communications (ICNC), 2012.

[23] Beyranvand, H.; Salehi, J.A., "Efficient Optical Resource Allocation and QoS Differentiation in Optical Burst Switching Networks Utilizing Hybrid WDM/OCDM" , Journal of Lightwave Technology.

[24] Tafani D, McArdle C, Barry, L.P, "Cost Minimization for Optical Burst Switched Networks with Share-per-Node Fibre Delay Lines", IEEE Communications Letters.

[25] Lei Liu, Hongxiang Guo, Tsuritani, T et. al., "Dynamic Provisioning of Self-Organized Consumer Grid Services Over Integrated OBS/WSON Networks ", Journal of Lightwave Technology.

[26] Vasco N. G. J. Soares, Iúri D. C. Veiga and Joel J. P. C. Rodrigues "OBS Simulation Tools: A Comparative Study", 2009.

[27] Oscar Pedrola, Sébastien Rumley and Miroslaw Klinkowski, "Flexible Simulators for OBS Network Architectures", International Conference on Transparent Optical Networks (ICTON), pp. 117-122, 2008.

[28] Joel J. P. C. Rodrigues, Nuno M. Garcia and Pascal Lorenz, "Object-oriented modelling and simulation of Optical Burst Switching Networks", IEEE Communication Society, GLOBECOM, pp 288-292, 2004, Portugal.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 137 - 140, 2013, ISSN: 2319–8656

Deep Packet Inspection with Regular Expression Matching

T. Nalini
Dept of Computer Science and Engineering
Bharath University
Chennai

M. Padmavathy
Dept of Computer Science and Engineering
Bharath University
Chennai

Abstract: Deep packet inspection directs, persists, filters and logs IP-based applications and Web services traffic based on content encapsulated in a packet's header or payload, regardless of the protocol or application type. In content scanning, the packet payload is compared against a set of patterns specified as regular expressions. With deep packet inspection in place through a single intelligent network device, companies can boost performance without buying expensive servers or additional security products. They are typically matched through deterministic finite automata (DFAs), but large rule sets need a memory amount that turns out to be too large for practical implementation. Many recent works have proposed improvements to address this issue, but they increase the number of transitions (and then of memory accesses) per character. This paper presents a new representation for DFAs, orthogonal to most of the previous solutions, called delta finite automata (δFA), which considerably reduces states and transitions while preserving a transition per character only, thus allowing fast matching. A further optimization exploits Nth order relationships within the DFA by adopting the concept of temporary transitions.

Keywords: Regular Expressions, Deep Packet Inspection, Differential Encoding, Finite Automata (FA), Pattern Matching

1. INTRODUCTION

Nowadays, deep packet inspection is required in an increasing number of network devices (intrusion prevention systems, traffic monitors, application recognition systems). Traditionally, the inspection was done with common multiple-string matching algorithms, but state-of-the-art systems use regular expressions (regexes) [1] to describe signature sets. They are adopted by well-known tools, such as Snort [2] and Bro [3], and in devices by different vendors such as Cisco [4].

Typically, finite automata (FAs) are employed to implement regexes matching. In particular, deterministic FAs (DFAs) allow for fast matching by requiring one state transition per character, while nondeterministic FAs (NFAs) need more transitions per character. The drawback of DFAs is that for the current regex sets they require an excessive amount of memory. Therefore, many works have been recently presented with the goal of memory reduction for DFAs, by exploiting the intrinsic redundancy in regex sets. However, most of these solutions can require more than one memory reference, thus lowering search speed.

This paper introduces a novel compact representation scheme (named δFA), which is based on the observation that since most adjacent states share several common transitions, it is possible to delete most of them by taking into account the different ones only (the δ in δFA just emphasizes that it focuses on the differences between adjacent states). Reducing the redundancy of transitions appears to be very appealing since the recent general trend in the proposals for compact and fast DFAs construction suggests that the information should be moved toward edges rather than states. In particular, our idea comes from D^2FA [5], which introduce default transitions.

We add the concept of "temporary transition," to improve the δFA. Instead of specifying the transition set of a state with respect to its direct parents (also defined 1-step ancestors), relaxing this requirement to the adoption of *N*-step "ancestors" increases the chances of compression. As we will show in the following, the best approach to exploit this *N*th-order dependence is to define the transitions of the states between ancestors and child as "temporary." This, however, introduces a new problem during the construction process. The optimal construction (in terms of memory or transition reduction) appears to be an *NP*-complete problem. Therefore, a direct and oblivious approach is chosen for simplicity. Results on real rule-sets show that our simple approach does not differ significantly from the optimal construction. Since this optimized technique is an extension to δFA that exploits *N*th-order dependence, we name it $\delta^N FA$. While many other proposed algorithms for DFA compression require more transitions per character, δFA and $\delta^N FA$ examine one state per character only, thus reducing the number of memory accesses and speeding up the overall lookup process. This improvement comes at the cost of wider memory accesses (with respect to previous schemes).

The rest of this paper is organized as follows. Section II explains the background of the work. Section III describes the algorithms for the creation of transition and lookup table. Section IV describes the experiments and results. Section V concludes this paper.

2. BACKGROUND WORK

Deep packet inspection has recently gained popularity as it provides the capability to accurately classify and control traffic in terms of content, applications, and individual subscribers. Cisco and others today see deep packet inspection happening in the network and they argue that "Deep packet inspection will happen in the ASICs, and that ASICs need to be modified" [6]. Some applications requiring deep packet inspection are listed below:

- Network intrusion detection and prevention systems (NIDS/NIPS) generally scan the packet header and payload in order to identify a given set of signatures of well known security threats.
- Layer 7 switches and firewalls provide content-based filtering, load-balancing, authentication and monitoring. Application-aware web switches, for example, provide scalable and transparent load balancing in data centers.

Deep packet inspection often involves scanning every byte of the packet payload and identifying a set of matching predefined patterns. Traditionally, rules have been represented as exact match strings consisting of known patterns of interest. Naturally, due to their wide adoption and importance, several high speed and efficient string matching algorithms have been proposed recently. Some of the standard string matching algorithms such as Aho-Corasick [7] Commentz-Walter [8], and Wu-Manber [9], use a preprocessed data-structure to perform high-performance matching. A large body of research literature has concentrated on enhancing these algorithms for use in networking. Tuck et.al presents techniques to enhance the worst-case performance of Aho-Corasick algorithm. Their algorithm was guided by the analogy between IP lookup and string matching and applies bitmap and path compression to Aho-Corasick. Their scheme has been shown to reduce the memory required for the string sets used in NIDS by up to a factor of 50 while improving performance by more than 30%.

3. PROPOSED SYSTEM

As discussed, several works in the recent years have focused on memory reduction of DFAs by trading size for number of memory accesses. The most important and cited example of such a technique is D2FA [6], where an input character (hereafter simply "char") can require a (configurable) number of additional steps through the automaton before reaching the right state.

3.1 Motivating Example

In this section, we introduce δFA, a D^2FA-inspired automaton that preserves the advantages of D^2FA while requiring a single memory access per input char. In order to make clearer the rationale behind δFA construction and the differences with D^2FA, we start by analyzing the example of [6] given below.

Fig. 1(a) represents a DFA on the alphabet {a,b,c,d} that recognizes the regular expressions (a^+), (b^+c), and (c^*d^+). In Fig. 1(b), the D^2FA for the same set of regexes is shown. The main idea is to reduce the memory footprint of states by storing only a limited number of transitions for each state and by taking a default transition for all input chars for which a transition is not defined. When, for example, in Fig. 1(b) the state machine is in state 3 and the input is *d*, the default transition to state 1 is taken. State 1 has a specified transition for char *d*, therefore we jump to state 4 (as in the standard DFA).

In this example, taking a default transition costs one more hop (one more memory access) for a single input char. However, it may happen that also after taking a default transition, the destination state for the input char is not specified and another default transition must be taken, and so on. In the example, the number of transitions was reduced to nine in the D^2FA (while the DFA has 20 edges), thus achieving a remarkable compression.

However, observing the graph in Fig. 1(a), it is evident that most transitions for a given input lead to the same state, regardless of the starting state. In particular, adjacent states share the majority of the next-hop states associated with the same input chars. Then, if we jump from state 1 to state 2 and we "remember" (in a local memory) the entire transition set of 1, we will already know all the transitions defined in 2 (which has the same set of 1). This means that state 2 can be described with a very small amount of bits. Instead, if we jump from state 1 to 3, and the next input char is c, the transition will not be the same as the one that c produces starting from 1. Then, state 3 will have to specify its transition for c.

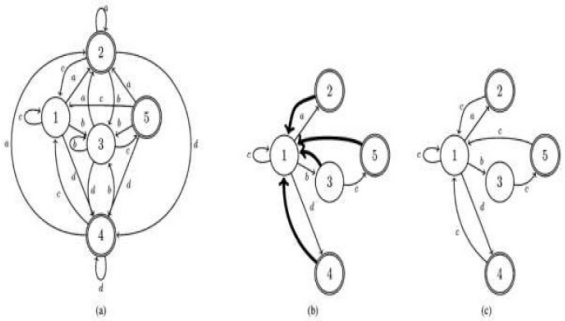


Fig-1: Automata Recognizing (a+), (b+c), and (c*d+) (a) DFA, (b) D2FA and (c) δFA

The result of what we have just described is shown in Fig. 1(c) (except for the local transition set), which is the δFA equivalent to the DFA in Fig. 1(a). We have eight edges only in the graph, and every input char requires a *single state traversal*.

3.2 Main Idea of δFA

The target of δFA is to obtain a similar compression as D^2FA without giving up the *single state traversal per character* of DFA. The idea of δFA comes from the following observations on D^2FAs and DFAs.

- Most default transitions are directed to states closer to the initial state.
- In a DFA, most transitions for a given input char are directed to the same state. Therefore, it becomes evident that most adjacent states share a large part of the same transitions. Thus, we can store only the differences between adjacent states. This requires, however, the introduction of a supplementary structure that locally stores the transition set of the current state. The main idea is to let this local transition set evolve as a new state is reached. If there is no difference with the previous state for a given character, then the corresponding transition defined in the local memory is taken. Otherwise, the transition stored in the state is chosen. In all cases, as a new state is read, the local transition set is updated with all the stored transitions of the state. The δFA in Fig. 1(c) only stores the transitions that *must* be defined for each state in the original DFA.

3.3 Construction

In Algorithm 1, the process for creating a δFA from an *N*-states DFA (for a char set of C elements) is shown. The algorithm works with the *transition tablet[s, c]* of the input DFA (i.e., an $N \times N$ matrix that has a row per state and where the *i*th item in a given row stores the state number to reach upon the reading of input char *i*). The final result is a "compressible" transition table $t_c[s, c]$ that stores the transitions required by the δFA only. All the other cells of the $t_c[s, c]$ matrix are filled with the special LOCAL_TX symbol and can be simply eliminated through a bitmap.

Algorithm 1: Creation of the Transition Table t_c of a δFA

1: for c ← 1, C do

```
2:          t_c[1, c] ← t[1, c]
3:    for s ← 2, N do
4:          for c ← 1, C  do
5:                t_c[s, c] ← EMPTY
6:    for S_parent  ← 1, N do
7:          for c ← 1, C  do
8:             Schild ← t[Sparent, c]
9:            for y ← 1, C do
10:         if t[S_parent, y] ≠ t[S_child, y] then
11:               t_c[S_child, y] ← t[S_child, y]
12.               else
12:          if t_c[S_child, y] == EMPTY then
14:               t_c[S_child, y] ←
LOCAL_TX
```

The construction requires a step for each transition (C) of each pair of adjacent states ($N \times C$) in the input DFA, thus it costs $O(N \times C^2)$ in terms of time complexity. The space complexity is $O(N \times C)$ because the structure upon which the algorithm works is another $N \times C$ matrix. In detail, the construction algorithm first initializes the t_c matrix with EMPTY symbols and copies the first (root) state of the original DFA in the t_c (it will act as base for subsequently storing the differences). Then, the algorithm observes the states in the original DFA one at a time. It refers to the observed state as *parent*. Then, it checks the *children* states (i.e., the states reached in one transition from parent state).

If, for an input char c, the child state stores a different transition than the one associated with any of its parent nodes, we cannot exploit the knowledge we have from the previous state, and this transition must be stored in the t_c table. On the other hand, when all of the states that lead to the child state for a given character share the same transition, then we can omit to store that transition. In Algorithm 1, this is done by using the special symbol LOCAL_ TX.

After the construction, since the number of transitions per state is significantly reduced, it may happen that some of the states have the same identical transition set. If we find j identical states, we can simply store one of them, delete the other j-1, and substitute all the references to those with the single state we left. Notice that this operation again creates the opportunity for a new state-number reduction because the substitution of state references makes it more probable for two or more states to share the same transition set. Hence, we iterate the process until the duplicate states end.

3.4 Lookup

The lookup in a δFA is shown in Algorithm 2. First, the current state must be read with its whole transition set. Then, it is used to update the local transition set t_{loc}: For each transition defined in the set read from the state, we update the corresponding entry in the local storage. This procedure comes at virtually no cost since it requires a number of operations on a fast local memory and its execution is easily masked in threaded systems or hardware implementations. Finally, the next state s_{next} is computed by simply observing the proper entry in the local storage t_{loc} .

Algorithm 2: Pseudocode for the lookup in a δFA. The current state is s and the input char is c

```
1.  read(s)
2.  for i ← 1, C do
3.    if t_c[s,i] ≠ LOCAL_TX then
4.          t_loc[i] ← t_c[s,i]
5.  s_next←t_loc[c]
return s_next
```

4. EXPERIMENTS AND RESULTS

The language used is java sdk2.0. Java is related to C++, which is a direct descendant of C. The trouble with C and C++ is that they are designed to be compiled for a specific target. But Java is a portable, platform-independent language that could be used to produce code that would run on a variety of CPUs under differing environments. Java can be used to create two types of programs: applications and applets. An application is a program that runs on our computer, under the operating system of that computer. Java is Simple, Secure, Portable, Object-oriented, Robust, Multithreaded, Architectural-neutral, Interpreted, High Performance, Distributed, and Dynamic.

As the number of network security threats rises, the NIDS has become one of the most important applications of packet inspection. Therefore, this study demonstrates the feasibility of integrating the proposed as the matching regular expression sets, introduces a novel compact representation scheme (named FA), which is based on the observation that since most adjacent states share several common transitions, it is possible to delete most of them by taking into account the different ones only (the in FA just emphasizes that it focuses on the differences between adjacent states). Reducing the redundancy of transitions appears to be very appealing since the recent general trend in the proposals for compact and fast DFAs construction suggests that the information should be moved toward edges rather than states.

Fig-2: Packet construction

Fig-3 Transmission

Packet Construction:

Fig-2 shows the packet construction, we are constructing the packets with a regular expression. The header information of a data packet is added in this phase. A packet consists of two kinds of data: control information and user data (also known as *payload*). The control information provides data the network needs to deliver the user data, for example: source and destination addresses, error detection codes like checksums, and sequencing information. Typically, control information is found in packet headers and trailers, with user data in between. The algorithms shown in Section II C.1 and D.1 are used to construct the transition table, lookup table respectively. It initializes the number of transitions in the DFA construction.

Transmission:

Fig-3 shows the transmission, the sender transmits the data to the receiver through the intermediate nodes.To find which source data is send into particular destination in the network. Here the data is received in all the intermediate

nodes and it must be checked for the illegitimate packets. The GUI provides the facility to send the packets to be inspected. Here the transitions will be checked and default transition will be added. The result of this will sent to look up table.

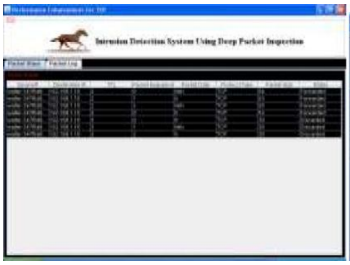


Fig-4: Packet Inspection

Fig-5: Evaluation

Packet Inspection:

Fig-4 shows the packet inspection. This is the phase of classifying intruder packet from the transmission. In the high-layer intrusion detection, expression may appear anywhere in the packet payload and making the attacking packets difficult to recognize. It may not only examine the header information but also the contents of the packet in order to determine more about the packet than just information about its source and destination. If the packets are matched with our expression and the packet is alive then it will be forwarded to the client else that will be discarded.

5. CONCLUSION

In this paper, we considered the implementation of fast regular expression matching for packet payload scanning applications. While NFA based approaches are usually adopted for implementation because naïve DFA implementations can have exponentially growing memory costs, we showed that with our rewriting techniques, memory-efficient DFA-based approaches are possible. While we do not claim to handle all possible cases of dramatic DFA growth (in fact the worse case cannot be improved), rewrite rules do over those patterns present in common payload scanning rule sets thus making fast DFA-based pattern matching feasible for today's payload scanning applications. It is possible that a new type of attack also generates signatures of large DFAs. For those cases, unfortunately, we need to study the signature structures before we can rewrite them.

6. REFERENCES

[1] R. Sommer and V. Paxson, "Enhancing byte level network intrusion detection signatures with context,''in Proc. ACM CCS, 2003, pp. 262 – 271.

[2] "Snort: Lightweight intrusion detection for networks," Sourcefire, Inc., Columbia, MD[Online]. Available: http://www.snort.org/.

[3] "Bro: A system for detecting network intruders in real time," Lawrence Berkeley National Laboratory, Berkeley, CA [Online]. Available: http://www.bro-ids.org

[4] J. William and W. Eatherton, "An encoded version of reg-ex database from Cisco Systems provided for research purposes," 2005.

[5] S. Kumar, S. Dharmapurikar, F. Yu, P. Crowley, and J. Turner, "Algorithms to accelerate multiple regular expressions matching for deep packet inspection," in Proc. ACM SIGCOMM, 2006, pp. 339–350.

[6] Scott Tyler Shafer, Mark Jones, "Network edge courts apps,"http://infoworld.com/article/02/05/27/020527newebdev_1.html

[7] A. V. Aho and M. J. Corasick, "Efficient string matching: An aid to bibliographic search," Comm. of the ACM, 18(6):333–340, 1975.

[8] B. Commentz-Walter, "A string matching algorithm fast on the average," Proc. of ICALP, pages 118–132, July 1979.

[9] S. Wu, U. Manber, "A fast algorithm for multi-pattern searching," Tech. R. TR-94-17, Dept. of Comp. Science, Univ of Arizona, 1994.

[10] D.R. Sidhu and V. K. Prasanna, "Fast regular expression matching using FPGAs," In IEEE Symposium on Field- Programmable Custom Computing Machines, Rohnert Park, CA, USA, April 2001.

[11] Antichi, G. Di Pietro, A. Ficara, D. Giordano, S. Procissi, G. Vitucci, "Second-Order Differential Encoding of Deterministic Finite Automata," Dept. of Inf. Eng., Univ. of Pisa, Pisa, Italy Nov. 30 2009-Dec. 4 2009.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 141 - 146, 2013, ISSN: 2319–8656

A Review on Wireless Sensor Network Protocol for Disaster Management

M. Sheik Dawood
Sethu Institute of Technology
Pulloor, India

J. Suganya
Sethu institute of Technology
Pulloor, India

R. Karthika Devi
Sethu institute of Technology
Pulloor, India

G. Athisha
PSNA College of Engg. & Technology
Dindigul, India

Abstract: Disasters management and emergency services used to protect a person or society from the cost of disasters such as tsunami warning , landslide monitoring, earthquake rescue operation , volcano monitoring, and fire protection. Timely report and responses are especially important for reducing the number of sufferers and damages from incidents. In such cases, the communication structure that may not function well. This makes it hard to gain information about the incident, and then to respond to the incident rapidly and properly. Sensor networks can provide a good solution to these problems through actively monitoring and well-timed reporting emergency incidents to base station. Our objective on this topic aim to study different sensor network protocols to resolve some key technical problems in this area, thus identify the energy efficient wireless sensor network architecture for significant improvement of disaster management . We also analyze the WSN protocol based on metrics such as Energy efficiency, location awareness, network lifetime. It furthermore focuses the advantages and performance for disaster management.

Keywords: —Disaster management, Sensor network, Energy Efficiency, Lifetime

1. INTRODUCTION

Disaster Management is a colossal task. They could hardly enclose to any particular location that neither do they disappear as quickly they appear. It is important about proper management to optimize efficiency of planning and response. Due to limited resources collective efforts occurred. The level of association requires a coordinated and organized effort to militate against, prepare for, respond to, and recover from emergencies and their effects in the shortest possible time [18].

A disaster is an event of natural or man-made causes that lead to sudden disruption of normalcy within society, causing damage to life and property, to reduce this damage effective management of information is important in the disaster management sector. The sectors from emergency response planning to short-range early warning to long-range mitigation and prevention planning are applied [19].

2. SENSOR NETWORK FOR LANDSLIDE MONITORING

Alberto Rosi et al. Proposing their research in "Landslide Monitoring with sensor network". This paper report on the implementation and deployment of a system for Landslide Monitoring in the Northern Italy Apennines and analyze the positive results and achieved it. Here efficient 'data collection algorithm' is used to receive the data correctly when disaster is occurring. [14]

Distributed detection strategy for landslide prediction using WSN". Propose by Prakshep Mehta (2007) et al. The researchers furthermore explained the use of various distributed algorithms for landslide prediction using WSN. The distributed vector based detection with independent cluster (DVBD-IC) algorithm stated that each CH sends the calculated likelihood ratio (LR) to the base station through multihop. They assumed that the data from the nodes within the cluster correlated but the data from different clusters are independent. The result of this paper shows that high Energy consumption of WSN protocol. [12].

Rehana Raj T et al, described their current research in Fault Tolerant energy saving Clustering scheme in WSN for Landslide Area Monitoring to reduce communication and processing overhead. The proposed approach, which organizes the whole network into smaller cluster and sub cluster groups as shown in figure -1 for enabling a considerable reduction of Communication and processing overhead. Sub clusters formation also gives the possibility to deal skillfully with sensor nodes, node leader, and cluster head failures.

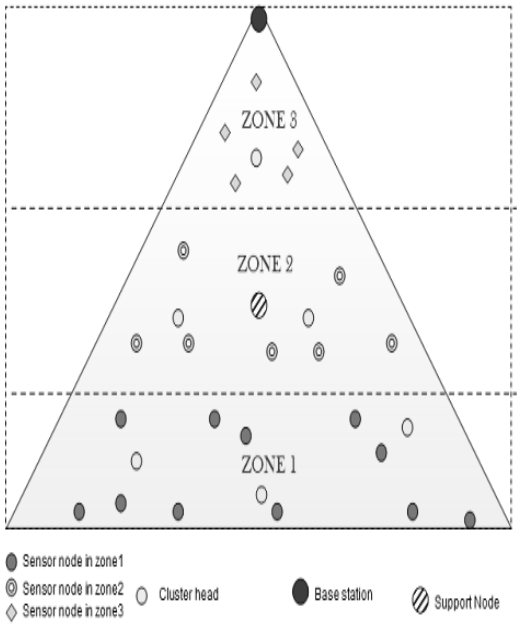


Figure- 1

On this approach failed data prediction is being achieved by a fuzzy control system [6]. Dominating Set based Algorithm used for fixing Cluster heads to improve the energy efficiency of network.

Siti Khairunniza-Bejo (2011) et al, proposed that "Historical Analysis of the Land Movement in Landslide Area Using Elastic Image Registration and Conditional Statement Approach". An elastic image registration and change-unchanged conditional statements procedure appropriate for historical analysis of the land movement in a landslide area presented herein. Landslide areas detected using the number of pixel movements during the registration process. It shows that the size of pixel movement used to detect changes in landslide areas. The more sequences of changed images were used, and the more information about the history of the area can be gathered [15].

G. P. Ganapathy (2010) et al reported their current research in "Need and Urgency of Landslide Risk Planning for Nilgiri District, Tamil Nadu State, India". The landslide is one of the major natural hazards that are commonly experienced in hilly terrains all over the world. In this, paper Landslide Vulnerability Index Risk analysis involves assessing the threat and these affected the people and property. It furthermore, provided an overview of risk management processes on Landslide Monitoring and relief operation. [16].

Kohei Arai (2012) analyzed their current research in "Sensor Network for Landslide Monitoring with Laser Ranging System, Avoiding Rainfall Influence on Laser Ranging by Means of Time Diversity and Satellite Imagery Data Based Landslide disaster relief". Sensor networks for Landslide Monitoring with a laser ranging system developed together with landslide disaster relief with remote sensing satellite imagery data. Experimental results show that the proposed protocol does work for the situation like rainfall influence and for landslide disaster relief [17].

Energy efficient sensor network protocol for landslide area monitoring proposed by sheik Dawood et.al (2012). The work furthers explained the Energy efficient modulation with two tier clustering Architecture for the fault tolerant sensor network. The improved lifetime of this protocol can be useful for the disastrous condition like Landslide Monitoring and management. [20].

3. WSN FOR AIR POLLUTION MONITORING

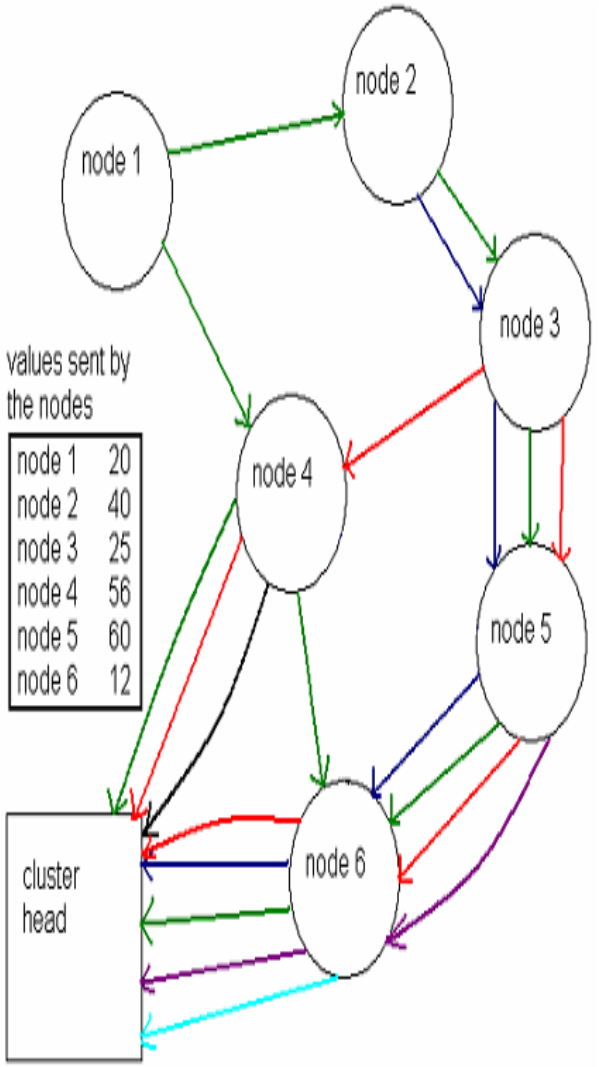
Kavi k.Khedo (2010) et al. Report on a "WSN air pollution monitoring system (WAPMS)".Indeed with the increasing number of vehicles on our roads and rapid urbanization air pollution has considerably increased in last decades. To reduce this problem they use 'Recursive Converging algorithm' and duplicate elimination technique.both the techniques are represented by authors shown in figure-2

The algorithm is used to merge data to eliminate duplicates, filter out invalid readings and summarize to simple form which significantly reduce the quantity of data to be transmitted to the sink and thus saving Energy [1].

4. WSN FOR EMERGENCY RESPONSE

A Location aware WSN protocol for emergency response task when disaster happens is described by Ashok Kumar (2009). In this paper localization, Communication is the main aspects of disaster-aided network (DAN).In localization aspects, a 'ranging and position estimation methodology' for patient localization at disaster site is proposed. As the result shows that DAN system supports efficient resource planning, quick evacuating of the patient and increase of situation awareness during disaster management [13]

G.Ragunath (2012) et al. Analyze "Deployment of the WSN for real time monitoring and disaster management". It is very essential to have a robot during disaster conditions like an earthquake or Bomb blast, where we have to identify living human beings as quickly as possible to save life; the authors explained the use of two mobile Robots for Surveillance (Target robot) and Rescue operation. The Target robot could easily navigate through rough terrain without being stuck and it can detect obstacles , fire, poisonous gases, Enemy remote vehicles. The Rescuer robot uses to detect a human, using the IR radiation emerging from the live humans and contactless sensor microwave Impulse radar (MIR) for detecting the heartbeat of human. The robot has a scissor Lift for Lifting heavier debris or Metal Rods and rescues the human. This paper is considered as very effective and life saving protocol for earthquake, landslides and other natural disasters [2]



Multihop routing of data during a collection instance and illustration of duplicate elimination technique

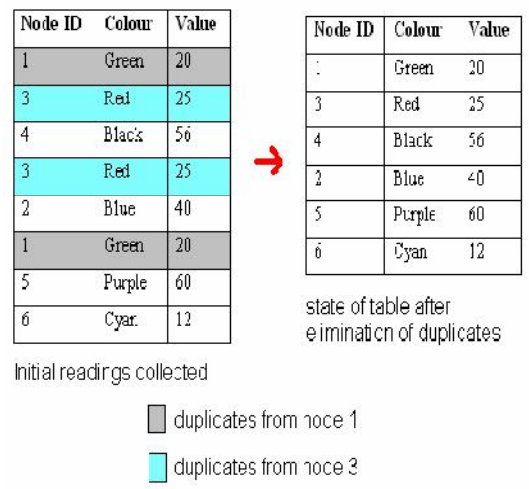


Figure -2

5. WSN FOR EARTHQUAKE DETECTION

Rui tan (2010) et al. Describing in their current research in "Quality driven Volcanic Earthquake Detection using WSN". In this paper, they described novel qualities driven approach to achieve real time, long-lived volcanic detection. These approaches based on 'collaborative signal processing algorithm'. The result of this is minimizing sensor's Energy consumption subject to sense quality requirement [11].

Makoto Suzuki (2007) et al. Proposing "A high density earthquake monitoring system using WSNs". For high precision monitoring, they developed Pavenet OS, which is hard real time operating system for sensor nodes, and accelerate the sensor board. In this model work in wireless mode and acceleration sensor board for necessary earthquake monitoring. As a result, they have easily preliminary evaluation of high precision and high density earthquake monitoring system [10].

Naveed Ahmad (2011) et al, propsed a architecture for Ad-hoc wirelesses Sensor Network for Disaster Survivor Detection as shown in figure-3 .Wireless Ad hoc sensor nodes are playing a vital role in wireless data transmission infrastructure.

The proposed model for the disaster survivor detection based on extremely critical disaster situations where this Energy efficient Architecture can successfully trace and locate thousands of people in critical circumstances. The emphasis of this paper focuses on earthquake based disasters. [7].

6. WSN FOR FORECASTING

Victor seal (2012) et al. Describing "A simple flood forecasting scheme using wireless sensor network" This work presents a forecasting model designed using WSNs to predict flood in rivers using a simple and fast calculations to provide real time results and, save the lives of people who may be affected by the flood. The novel algorithm is used to predict from the flood forecasting and use the independent number of guidelines. Figure-4 depicts the WSN deployment scheme in a flood prone river basin. The result is to give awareness to the people and, save their life [5].

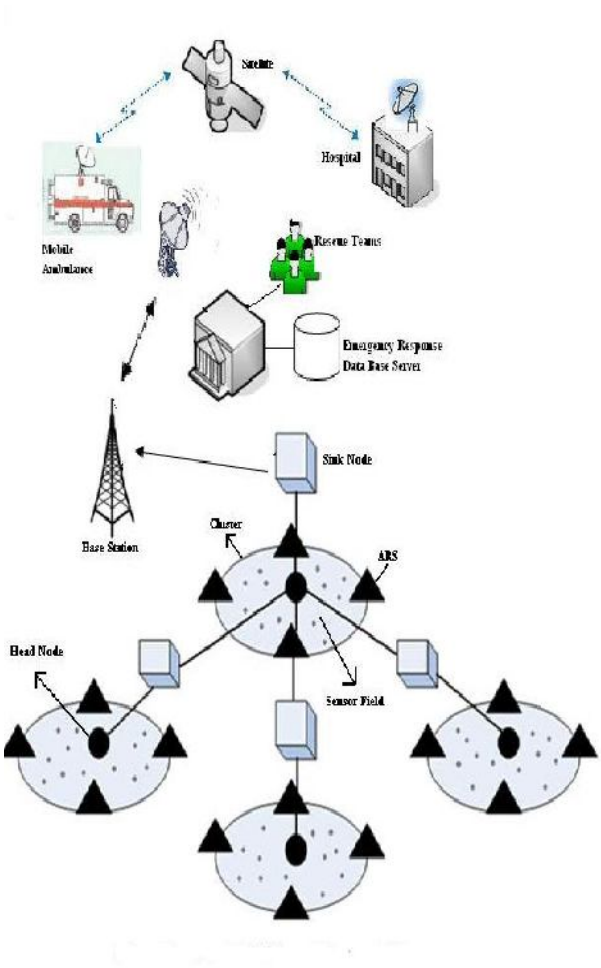


Figure-3

Cholatip Yawut (2011) et al proposed that **"**A WSN for Weather and disaster Alarm Systems" In this paper, presented a system used to avoid massive damage from natural disasters. In this system, a WSN based on ZIGBEE used as a weather station network sending information and disasters' alerts. This proposed system takes advantage of WSNs that can send signals over far distances by using a mesh topology; this transfer the data and consumes low power. Therefore, this system installed in locations has no access to electricity [4].

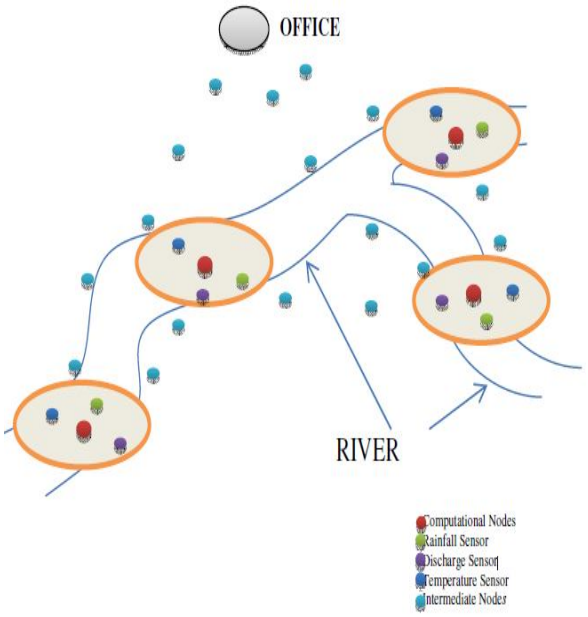


Figure-4

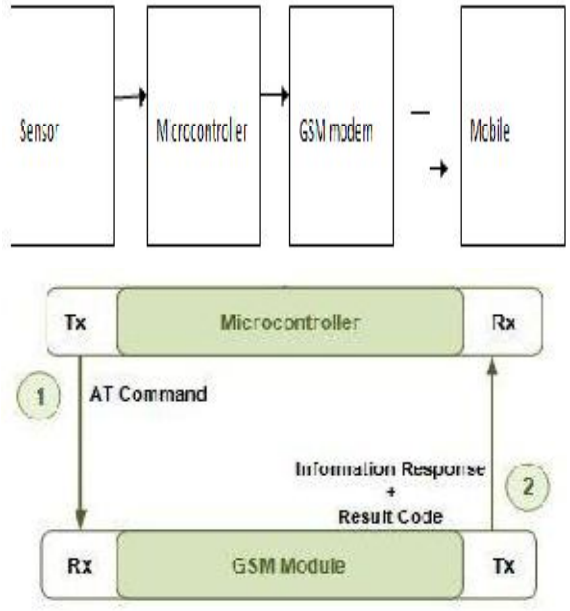


Figure-5

7. PERFORMANCE ANALYSIS OF DISASTER MANAGEMENT PROTOCOLS

Mohamed youis (2004) et al, analyzed that "On Handling QOS Traffic in WSN" Many new routing and MAC layer protocols have been proposed for WSNs tackling the issues raised by the resource constrained unattended sensor nodes in large-scale deployments. Transmission of data in such cases requires the Energy and QOS aware network management to ensure efficient usage of the sensor resources and effective access to the gathered measurements. They highlight the architectural and operational challenges of handling of QOS traffic in sensor networks [8].

Sanjay Patel (2011) report On an "Interfacing of Sensor Network to Communication Network for Disaster Management".This work with the sensor network and Communication network for disaster management using GSM modem which the concerned authorities dealing with disaster management get the message on their mobile phones about disaster information. Figure-5 given a general block diagram for Interfacing of Sensor Network to Communication Network for Disaster Management.

The GSM modem sends and receives data through radio waves. Now a day's number of small disasters like fire, chemical leakage, pollution etc, happens frequently and need immediate relief action. The result of this paper release the immediate information for quick action to such events [3].

WSNDM is a wireless sensor network protocol for disaster management is proposed by Saha, S. Matsumoto, M. The authors have proposed this protocol with an updated hybrid network framework. In this paper, the performance of WSNDM protocol compared with LEACH.it furthermore gave a solution to collapsed base station problem. In sensor networks, average Energy dissipation measured performance, system lifetime, successful data delivery and the number of live nodes. Their simulation, considered those performance factors. Simulation results prove that WSNDM outperforms LEACH protocol . [22]

A natural disaster management system based on location aware distributed sensor networks is presented by Kumar (2005) to achieve maximum lifetime in WSNs in disaster management applications. The authors propose a system based on hierarchical transmission of packets from sensor nodes to the base station by identifying a path from one head to a subsequent head along the route. The algorithm divides the entire sensor network into logical concentric zones based on Energy of transmission of the packet is transmitted from a head node to one of the head nodes in the next zone with lesser distance. The implementation profoundly uses the location awareness of sensor nodes for better routing and, hence is applicable only to those situations where such data can be made available at the time of installation. They further provide the concept of multiple memberships of sensor nodes to different heads within its area of reach thereby handling disaster conditions where a head fails without notification to its primary members [21].

8. WSN FOR ENVIRONMENTAL MONITORING

Al-Sakib Khan Pathan (2006) et al. Analyzing "Smartening the Environment is using WSNs in a developing country". In this paper, they explore the prospects of wireless sensor networks and propose a design level framework for developing the smart environment using WSNs. Here update the information about flood, water level, traffic and controlling, environmental frequently. If any changes mean, they used two phases. First phase used to collect the data and send to the local base station. The second phase involves data distribution network, where the processed data sent to different factors involved in network [9].

9. CONCLUSION

This survey studies the role of sensor network in disaster management. It furthermore studied the different types of disaster management protocols and their application in extremely disastrous conditions. The performance such protocols are studied based on Energy efficiency, location awareness and network lifetime.

10. REFERENCES

[1] Kavi k khedo, Rajiv perseedoss.2010. Avinash Mungar, "A wireless sensor network air pollution monitoring system", International Journal of wireless &Mobile Networks(IJWMN),Vol.2,No.2.

[2] G. Ragunath & Dinesh Kumar.2012. "Deployment of the WSN for real time monitoring and disaster management", Indian Journal of Innovation & developments, Vol.1.

[3] Sanjay Patel, O.P, Vyas.2012. "Interfacing of Sensor Network to Communication Network for Disaster Management" International Journal of Soft computing & Engineering (IJSCE), Vol.2.

[4] Cholatip yawut & Sathapath kilaso.2011. "A Wireless Sensor Network for Weather and disaster Alarm Systems" in proceedings of International conference on Information & Electronics Engineering.

[5] Victor Seal, Arnab Raha, Shovan Maity.2012. "A simple flood forecasting scheme using wireless sensor network", International Journal of Adhoc Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.1.

[6] Rehna Raj, Maneesha Ramesh, V. and Sangeeth Kumar.2008. "Fault Tolerant Clustering Approaches in Wireless Sensor Network for Landslide Area Monitoring"in Proceedings of the International Conference on Wireless Networks (ICWN'08), Vol. 1, pp. 107–113

[17] Naveed Ahmad, Naveed Riaz, Mureed Hussain.2011. "Ad hoc wirelesses Sensor Network Architecture for Disaster Survivor Detection", International journal of advance science and technology, vol 34, September 2011.

[8] Mohamed youis.2004."On Handling QoS Traffic in Wireless Sensor Network", in proceedings of the International conference, January 2004.

[9] Al-Sakib Khan Pathan, Choong Seon Hong, Hyung-Woo Lee.2006. "Smartening the Environment using wireless sensor networks in a developing country", IEEE ICACT, Volume I.

[10] Makoto Suzuki, Narito Kurata, Hiroyuki Morikawa, Shunsuke Saruwatari.2007. "A high density earthquake monitoring system using wireless sensor networks", International conference on Embedded network sensor system

[11] Rui Tan, Guoliang Xing, Jinzhu Chen, Wen-Zhan Song, Renjie Huang. 2010. in inproceedings on "Quality driven Volcanic Earthquake Detection using wireless sensor network", Real time system symposium.

[12] Prakshep Mehta, Bhushan Jagyasi, Kalyana Tejaswi, Rajat Bansal, Chandresh Parekh, Anmol Sheth, S. N. Merchant, T. 2007.'Distributed detection strategies for landslide prediction using Wireless sensor networks, in proceedings of first international global information infrastructure Symposium, Morocco. Pp 195-198

[13]Ashok Kumar.2009. "A Location aware wireless sensor network for assisting emergency response to disaster" International journal of computer science and information security, Vol 2, June 2009.

[14] Alberto Rosi, Nicola Bicocchi, Gabriella Castelli, Marco Mamei, Franco Zambonelli..2011. "Landslide Monitoring with sensor network" published in the International journal of signal and imaging systems engineering. Vol. 10 No.3.

[15] Siti Khairunniza-Bejo, Abdul Rashid Mohamed Shariff.2011. "Historical Analysis of the Land Movement in Landslide Area Using Elastic Image Registration and Conditional Statement Approach" International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 3.

[16] G. P. Ganapathy, K. Mahendran, S.K Sekar.2010. "Need and Urgency of Landslide Risk Planning for Nilgiri District, Tamil Nadu State, India" International journal of genetics and Geosciences volume 1, no 1.

[17] Kohei Arai.2012."Sensor Network for Landslide Monitoring With Laser Ranging System Avoiding Rainfall Influence on Laser Ranging by Means of Time Diversity and Satellite Imagery Data Based Landslide Disaster Relief" International Journal of Applied Sciences (IJAS), Vol 3,No.1 .

[18] "Disaster management".2008 an article published online in the Virtual University for Small States of the Commonwealth (VUSSC) .

[19] Aloysius J. Rego.2001. "National Disaster Management Information Systems & Networks" June 2001.

[20] M. Sheik Dawood, Sajin Salim, S. Sadasivam, G. Athisha.2012."Energy Efficient Modulation Techniques for Fault Tolerant Two-Tiered Wireless Sensor Networks,Journal of Asian scientific research. Vol.2, No.3, pp.124-131.

[21] Ranjan, G. , Kumar, A. 2005. A natural disaster management system based on location aware distributed sensor networks, in proceeding of IEEE International Conference on Mobile Adhoc and Sensor Systems, 7 Nov. 2005 pp. - 182

[22] Saha, S. , Matsumoto, M.2006. Performance Analysis of WSNDM (Wireless Sensor Network Protocol for Disaster Management) , International Conference on Communication Technology, ICCT '06.2006 , pp 1 - 4

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 147 - 151, 2013, ISSN: 2319–8656

A New Architecture for Group Replication in Data Grid

Leila Azari
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Khouzestan, Iran

Mashalla Abbasi Dezfouli
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Khouzestan, Iran

Abstract: Nowadays, grid systems are vital technology for programs running with high performance and problems solving with large-scale in scientific, engineering and business. In grid systems, heterogeneous computational resources and data should be shared between independent organizations that are scatter geographically. A data grid is a kind of grid types that make relations computational and storage resources. Data replication is an efficient way in data grid to obtain high performance and high availability by saving numerous replicas in different locations e.g. grid sites. In this research, we propose a new architecture for dynamic Group data replication. In our architecture, we added two components to OptorSim architecture: Group Replication Management component (GRM) and Management of Popular Files Group component (MPFG). OptorSim developed by European Data Grid projects for evaluate replication algorithm. By using this architecture, popular files group will be replicated in grid sites at the end of each predefined time interval.

Keywords: data Grid; data replication; group replication; architecture; replica.

1. INTRODUCTION

In grid systems, heterogeneous computational resources and data should be shared between independent organizations that are scatter geographically [1]. On the other hand, the data Grid is a kind of grid services that provides services and infrastructure for distributed data applications with large volumes of data. These basic services which are provided by the data grid architecture are: storage systems, data access and meta-data services [2]. Data replication is one of the main services to manage volume data in data grid. This service save replica in different locations. Therefore, when each user needs those files, it will be available locally and causes reducing access latency time, response time and bandwidth consumption. So far various strategies have been presented in this field. Grid architecture has an efficient factor in replication technique. There are different architectures for data grid that all of them are based on hierarchal data model [3]. Data grids can be classified into two types [4]: multi-tier data grids that first introduced by the MONARC project [5], and cluster data grids that initially proposed by Chang et al. [6]. Multi-tier data grid architecture contains two models, tree model and graph (peer to peer) model. In tree model, Each node can communicate only to the parent node and there is only one path from a leaf to the root. Because of architecture failure we can not simply add nodes to the grid. For example, at GriPhyN project has been used tree model. There are five tiers in this model. In this multi-tier data grid architecture, the root site holds all files that are produced initially in the data grid. Next tiers are national center, regional center, work groups and leafs node represents desktop. In graph model, grid sites connect to each others as a peer to peer architecture. In this model, some of the limitations of the tree type are improved. In 2001, six replication techniques were presented by Ranganathan and foster [7] for a multi-tier data grid. In 2002 Ranganathan [8] presented a replication technique based on peer to peer communities. A cluster represents an organization unit which is a group of sites that are geographically close to each others. A cluster data grid consists of n clusters connected by the Internet [9]. Recent researchers have used hierarchal models as a basis and proposed other architectures for replication techniques. The most above mentioned techniques are the based on a single replication. If a replica does not exist locally in a requester grid site replication techniques will replicate it to that grid site. In this paper, we propose a new architecture for dynamic group data replication which has two added components to OptorSim architecture: Group Replication Management component (GRM) and Management of Popular Files Group component (MPFG). This paper is organized in the following way: Section 2 gives a brief introduction of related work on architecture for data grid. In section 3, the architecture of OptorSim is presented. Section 4 describes proposed architecture and finally concludes our presents some future work.

2. RELATED WORK

Chang et al. [6] presented a hierarchical architecture with concept of clustering. Cluster grid is a simple hierarchical form of a grid system. There are two kinds of communications between grid sites in a cluster grid. Intra-communication is the communication between grid sites within the same cluster and inter-communication is the communication between grid sites across clusters. Network bandwidth between grid sites within a cluster will be larger than across clusters. In this architecture, clusters are connected via internet. A job scheduling policy called HCS is presented based on this architecture that considers not only computational capability and data location but also cluster information. Also a dynamic replica optimization strategy (HRS) is suggested where the nearby data has a higher priority to access than to generate new replicas. The simulation results showed that HCS successfully reduced data access time and the amount of inter-cluster-communications in comparison with LRU (Least Recently Used), LFU (Least Frequently Used), BHR (Bandwidth Hierarchy-based Replication) [10]. Since the file transmission time is the most important factor to influence the job execution time for data-intensive jobs in data grids, HCS with HRS can reduce the file transmission time effectively by virtue of valid scheduling and proper data replication. Sepahvand et al. [11] presented three-level hierarchical architecture. This architecture represents a real structure in most academic data centers, cities and countries. First level is grid sites that contain personal computers. These sites are connected by a high bandwidth network. Second level contains LAN. Compared with first level, LANs are connected by a low bandwidth network. Finally, there are

several LANs in each region which are connected via Internet having a low bandwidth network. If there is not space for replica, only those file will be deleted that have a low cost of transfer i.e. considering the bandwidth between source and destination. So it deletes those files that are available in local LAN. In comparison to BHR algorithm which considers 2-level, the 3 level has performed better and it is more realistic. The simulation results with OptorSim have showed better performance comparing to LRU and BHR.

Sashi and Thanamani [12] presented a replication algorithm which is called Modified BHR with multi-tier architecture based on region. Region comprise group of sites that are geographically located close together. Each region has a header. All files were produced in a master site and were distributed in each region headers. The Modified BHR Region increases the data availability by replicating files within the region to the region header and storing them in the site where the file has been accessed frequently. Instead of storing files in many sites, Modified BHR stores them in a particular site so that the storage usage can be reduced. In comparison to No Replication, (LFU), (LRU) and BHR algorithms, Modified BHR reduces mean job execution time and the network traffic too.

Chang et al. [9] presented a replication algorithm which is called Latest Access Largest Weight (LALW) with multi-tier architecture based on a centralized data replication management which has a Dynamic Replication Policymaker (Policymaker) that responsible for replica management. This architecture contains grid sites within a cluster. There is a header used to maintain the site's information in a cluster. In the time interval, Policymaker sends a request for collecting site's information. Each header sends the information of accessed files from all sites to Policymaker. LALW selects a popular file for replication and calculates a suitable number of copies and grid sites for replication. According to access frequencies for all files that have been requested, a popular file is found and replicated to grid sites. In LALW, the data access records in the nearer past have higher weigh and higher value of references. The simulation results showed that the average job execution time of LALW is similar to LFU optimizer, but exceeded in terms of effective network usage. Saadat and rahmani [13] presented a replication algorithm named PDDRA hierarchical architecture supporting their dynamic replication technique. Grid sites is first level several grid sites constitute a virtual organization (VO). Next level is Local Server for each VO. Regional Server (RS) comprise the final level. Each RS consists of one or more VOs. Due to the far distance between the RS, they are connected via internet which has low bandwidth. Sites within a VO have similar interests. PDDRA predicts future needs of grid sites and pre-fetches a sequence of files to the requester grid site, so the next time that this site needs a file, it will be locally available. The simulation results showed that PDDRA has better performance in comparison with No Replication, LRU, LFU, EcoModel, EcoModel Zipf-like distribution and PRA [14] in terms of job execution time, effective network usage, total number of replications, hit ratio and percentage of storage filled.

3. THE ARCHITECTURE OF OPTORSIM

OptorSim is used as the simulator tool written in Java to evaluate the performance of replication strategies. It was developed by the European Data Grid projects [15]. It was developed to study the effectiveness of replica optimization algorithms within a data grid environment [16]. The architecture used in OptorSim is the CMS testbed architecture [17]. Figure 1, describes the Grid topology; that is, the resource available and the network connections to other sites. Sites are represented as green nodes and routers as red nodes. In this architecture, there are twenty sites, two of which only have a storage element and act as the master node. CERN and FNAL are considered the master sites where data is produced initially. The master site has the most capacity, which allows it to hold all the master files at the beginning of the simulation. The storage capacity of the master site is 100 GB, and the storage capacity of all other sites is 50 GB. Each data file to be accessed is 1 GB. Jobs are processed in the remaining sites that have computing elements. There are eight routers that are used to forward requests to other sites.

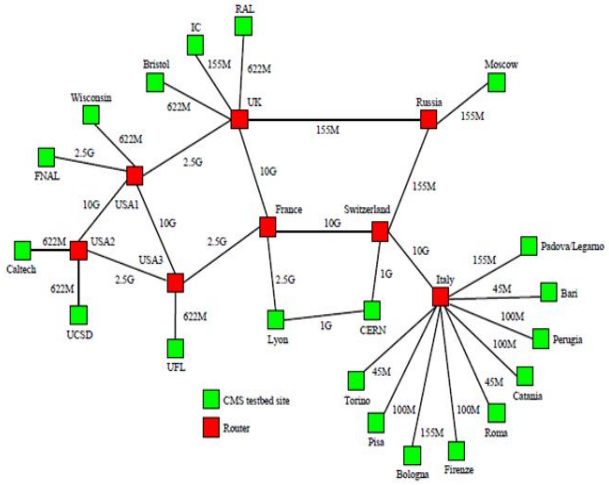


Figure 1. CMS topology

The internal architecture [18] of OptorSim and the content of each site is illustrated in Figure 2, Each site may provide computational and data storage resources called the Computing Element (CE) and the Storage Element (SE). CEs run jobs by processing data files, which are stored in the SEs. A Resource Broker (RB) controls the scheduling of jobs to Grid Sites, and schedules jobs to CEs according to scheduling algorithm. Each site handles its file content with Replica Manager (RM), within which a Replica Optimizer (RO) contains the replication algorithm which drives automatic creation and deletion of replicas [18]. Jobs are submitted to the grid over a period of time via the RB. The RB schedules each job to the CE with the goal to improve the overall throughput of the grid. RM at each site manages the data flow between sites. The RO inside the RM is responsible for the selection and dynamic creation and deletion of file replicas.

4. PROPOSED ARCHITECTURE

Our proposed architecture contains Local Servers (LS) and grid sites. We have used virtual organization concept in our

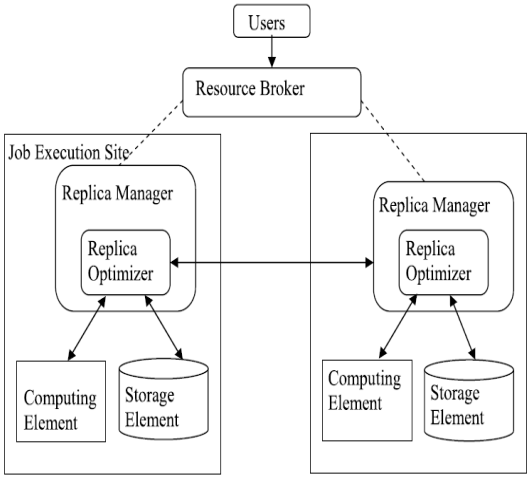


Figure 2. OptorSim architecture

architecture. Collection of grid sites constitute a VO. Grid sites within a VO have similar interests and request similar files. There is also a LS within each VO. LSs are connected via internet which has low bandwidth. Therefore, speed of data access within VO is larger than across VOs. OptorSim [19] assumes that each grid sites contains zero or more Computing Elements (CE) to run jobs and zero or more Storage Elements (SE) to store files, or a combination of both. In OptorSim, there is a Resource Broker (RB) that controls job scheduling between different CEs. Figure 3 shows the proposed architecture. First of all, end users submit their jobs to RB. Then RB schedules jobs between LS by scheduling optimization and are appropriate jobs to computing sites which have CE for execution. Computing sites request some resources for running job that they can be files. If these files are not available locally then they will be accessed remotely.

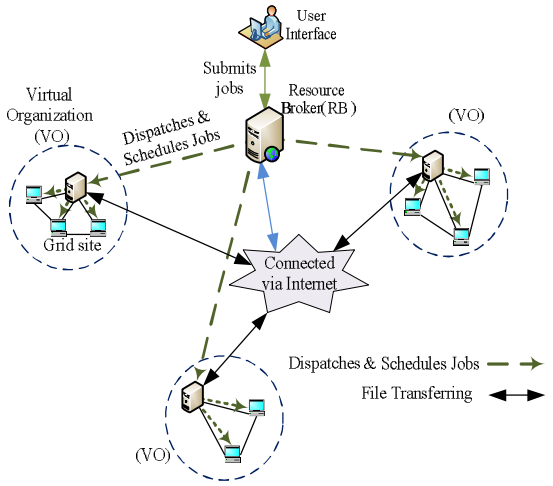


Figure 3. group replication architecture

4.1 The architecture of LS and grid sites

In this section, the LS components and components of grid sites and communications between them are presented. Figure 4 shows messages passing between LS components and grid sites.

4.1.1 LS Components

LS is composed of two components as follows:

4.1.1.1 Replica Catalogue (RC)

this component maps between physical address and logical name of a replica.

4.1.1.2 Replica Manager (RM)

after getting information from the Replica Catalogue, the RM checks the locations of the physical file and selects the best replica of file. It is important that the file must be fetched from a low cost grid site. OptorSim finds the best replica according to minimum cost of replication and then RM selects replicas that have lowest instance of CE.

4.1.2 Components of grid sites

Each grid site is composed of two components as follows:

4.1.2.1 Management of Popular Files Group component (MPFG)

This component is composed of two parts as follows:

- Access history database: Each job must have access to a set of requested files and send them to a grid site. Sequence of the requested files in each grid site is stored in a local database.

- Produce engine: This component is responsible for processing on database and finding the most popular files group (PFG).

4.1.2.2 Group Replication Management component (GRM)

In a predefined time interval, this component sends a request for MPFG component. Replacement Management (RM) is part of Replication Management. If there is not enough space for replicating of the PFG to a requester grid site, then RM will replace the PFG with old replica according to the replacement algorithm.

4.2 Communication between grid sites and LS

Internal components of proposed architecture and messages passing between them are shown in figure 3. It consists of two new components which are shown by dashed lines in figure 3. At the beginning of time interval GRM sends a replication request to MPFG component. MPFG processes on the access history database and finds PFG by using existing replication algorithm. Then it sends the requested replica of PFG to LS of grid sites. Also, it sends the name of requester site to LS with each replication request. Then, Replica Catalogue component finds physical addresses of each replica of PFG and transfers them to the Replica Manager component. RM checks the locations of the physical files and determines the best replica by minimum cost of replication. Finally, it will begin the group replication process for the requester sites.

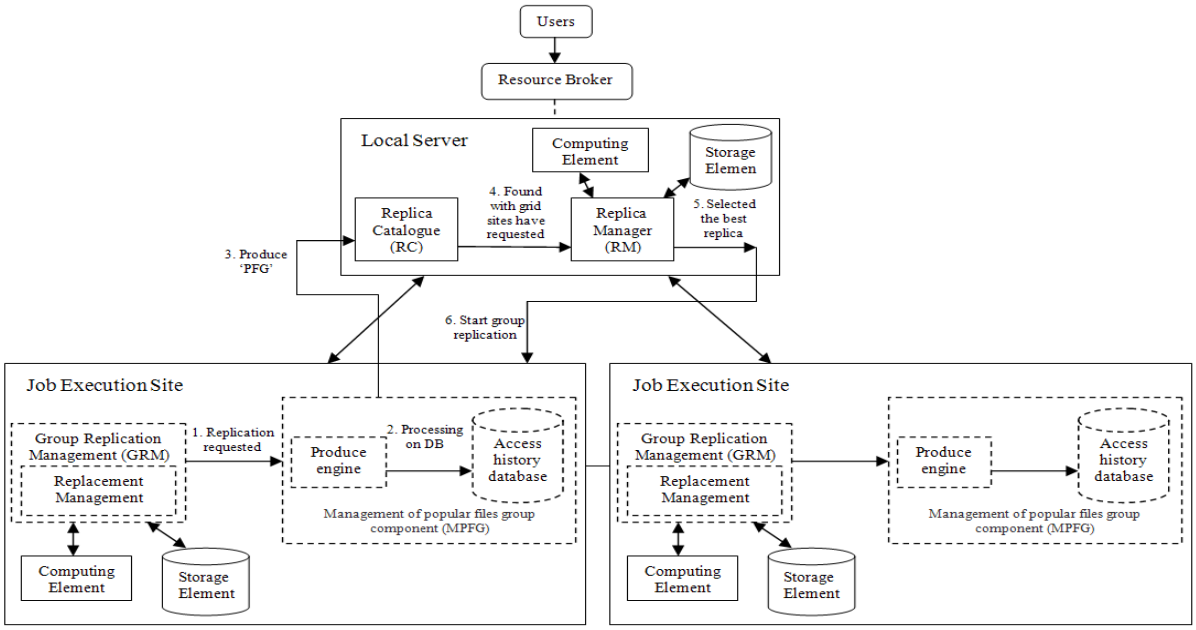


Figure 4. Messages passing between grid sites and LS.

5. CONCLUSION AND FUTURE WORK

In grid systems, heterogeneous computational resources and data should be shared between independent organizations that are scatter geographically. On the other hand, the data Grid is a kind of grid services that provides services and infrastructure for distributed data applications with large volumes of data. Data replication is one of the main services for managing volume data in data grid. This service saves replica in different locations. Grid architecture has an efficient factor in replication technique. In this paper, we proposed a new architecture for group replication in data grid. We added two components in our architecture, (MPFG) for Management of Popular Files Group and (GRM) for Group Replication Management. By using this architecture, popular files group will be replicated in grid sites at the end of predefined time interval. For future works, we plan to implement this architecture and to combine it with group replication and replacement technique.

6. REFERENCES

[1] Foster, I., Kesselman, C., Tuecke, S., "The anatomy of the grid: Enabling scalable virtual organizations", International Journal of Supercomputer Applications, pp. 200-222, 2001.

[2] Jacob, B., Brown, M., Fukui, K., Trivedi, N., "Introduction to Grid Computing ",IBM Red books , pp. 3-6, 2005.

[3] Amjad, T., Sher, M., Daud, A., "A survey of dynamic replication strategies for improving data availability in data grids", Future Generation Computer Systems 28, pp.337–349, 2012.

[4] Ming-Chang, L., Fang-Yie, L., Ying-ping, Ch., "PFRF: An adaptive data replication algorithm based on star-topology data grids", Future Generation Computer Systems 28, pp.1045–1057, 2012.

[5] The MONARC project. http://monarc.web.cern.ch/MONARC/, [Accessed 15 Jan 2012].

[6] Chang, R-S., Chang, J-S., Lin, S-Y., "Job scheduling and data replication on data grids", Future Generation Computer Systems 23, pp. 846-860, 2007.

[7] Ranganathan, K., Foster, I., "Design and evaluation of dynamic replication strategies for a high performance data grid", in: International Conference on Computing in High Energy an Nuclear Physics, vol. 2001, 2001.

[8] Ranganathan, K., Iamnitchi, A., Foster, I., Improving data availability through dynamic model driven replication in large peer-to-peer communities, in: CCGrid, p. 376, 2002.

[9] Chang, R-S., Chang, H-P., Wang, Y-T., "A Dynamic Weighted Data Replication Stratrgy in Data Grids", The Journal of Supercomputing, 45(3), pp. 277-295, 2008.

[10] Park, S.-M., Kim, J.-H., Go, Y.-B., Yoon, W.-S., "Dynamic grid replication strategy based on internet hierarchy, in: International Workshop on Grid and Cooperative Computing", in: Lecture Note in Computer Science, vol. 1001, pp. 1324–1331, 2003.

[11] Sepahvand, R., Horri, A., Dastghaibyfard, Gh., "A New 3-layer Replication and Scheduling Strategy in Data Grid", International Symposium on Telecommunications, pp. 464-469, 2008.

[12] Sashi, K., Thanamani, A.S., "Dynamic replication in a data grid using a Modified BHR Region Based Algorithm", Future Generation Computer Systems 27, pp. 202-210, 2011.

[13] Saadat, N., rahmani, A-M., "PDDRA: A new pre-fetching based dynamic data replication algorithm in

data grids", Future Generation Computer Systems 28, pp. 666–681, 2012.

[14] Tian, T., Luo, J., Wu, Z., Song, A., "A pre-fetching-based replication algorithm in data grid, in: 3th International Conference on Pervasive Computing and Applications", pp. 526–531, 2008.

[15] The European DataGrid Project, http://www.edg.org, [Accessed 15 Jan 2012].

[16] Bell, W.H., Cameron, D.G., Capozza, L., Millar, A.P., Stockinger, K., Zini, F., "Simulation of dynamic grid replication strategies in OptorSim", International Journal of High performance Computing Applications 17 (4), 2003.

[17] CMS Data Challenge, 2004: http://www.uscms.org/s&c/dc04/, [Accessed 15 Jan 2012].

[18] Cameron, D.G., Millar, A.P., Nicholson, C., "OptorSim: a simulation tool for scheduling and replica optimization in data grids", Proceedings of Computing in High Energy and Nuclear Physics (CHEP) , 2004.

[19] OptorSim – A Replica Optimiser Simulation, http://grid-data-management.web.cern.ch/grid-data-management/optimization/optor, [Accessed 15 Jan 2012].

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 152 - 154, 2013, ISSN: 2319–8656

A Novel Method for Encoding Data Firmness in VLSI Circuits

V. Karthikeyan
Department of ECE
SVS College of Engineering
Coimbatore, India

V. J. Vijayalakshmi
Department of EEE
Sri Krishna College Of Engineering & Technology
Coimbatore, India

P. Jeyakumar
Department of ECE
Karpagam University
Coimbatore, India

Abstract: The number of tests, corresponding test data volume and test time increase with each new fabrication process technology. Higher circuit densities in system-on-chip (SOC) designs have led to drastic increase in test data volume. Larger test data size demands not only higher memory requirements, but also an increase in testing power and time. Test data compression method can be used to solve this problem by reducing the test data volume without affecting the overall system performance. The original test data is compressed and stored in the memory. Thus, the memory size is significantly reduced. The proposed approach combines the selective encoding method and dictionary based encoding method that reduces test data volume and test application time for testing. The experiment is done on combinational benchmark circuit that designed using Tanner tool and the encoding algorithm is implemented using Model -Sim

Key words: Test data volume, Test data compression, Selective encoding, Dictionary based encoding

1. INTRODUCTION

Testing is a process of checking the fabricated IC's for any incorrect behaviour due to faults like logical fault, delay fault, fabrication faults [1]. Test data volume is now recognized as a major contributor to the cost of manufacturing testing of integrated circuits (ICs). Test vector compression has been an active area of research, yielding a wide variety of techniques. There are various methods for test data compression but code based data compression scheme is more useful for intellectual property (IP) cores, since their structure is often hidden from the system integrator [2]. A test pattern compression scheme is proposed in order to reduce test data volume and generation time. Test application time and test data volume is affected by a number of parameters, such as the number of patterns ,the number of scan chains, and number of scan cells and the scan frequency. Scan design methods reduce test data volume and test application time by partitioning scan chains to shorter segments and broadcast the same test data to multiple scan chains. While compaction schemes try to reduce the number of patterns generated without compromising fault coverage levels, compression schemes in turn target reduction of the storage requirements of the compacted test patterns. While compression of the original test vectors provides some level of test volume reduction, the compression schemes also try to compress the difference between the successive vectors to improve compression efficiency. Data compression techniques are used to alleviate the ATE test data volume problem.Dictionary-based test data compression is a promising approach for test data volume reduction. they provide a dual advantage of good compression efficiency as well as fast decompression mechanism. We present a selective encoding method that reduces test data volume and test application time for the scan testing of IP cores. This method encodes the slices of test data that are fed to the scan chains in every clock cycle. Unlike many prior methods, the proposed method does not encode all the specified (0's and 1's) and unspecified (don't care) bits in a slice. They encode only the target symbols.

2. EXISTING METHODS

Many research works have tried to solve the data volume problem in high performance VLSI circuits. An efficient test data compression technique reduces the test data volume considerably. Test data compression offers a promising solution to the problem of increasing test data volume. A test set for the circuit under test (CUT) is compressed to a much smaller data set, which is stored in ATE memory. Huffman codes are the most effective ones, since it probably result in the shortest average codeword length, Then the main problem is the high hardware overhead of the required de-compressors. Huffman decoding leads to both large de-compressors and very low compression ratios. Since the vast majority of the cores have multiple scan chains, a serial-in, parallel-out register must be used for spreading the decoded data in them and thus, no test-time savingsLei Li, Krishnendu Chakrabarty and Nur A. Touba present dictionary-based test data compression approach for reducing test data volume in SOCs. The proposed method is based on the use of a small number of ATE channels to deliver compressed test patterns from the tester to the chip and to drive a large number of internal scan chains in the circuit under test. Jun Liu1, Yinhe Han1, Xiaowei Li1, propose an extended selective encoding which presents Flexible grouping strategy is able to decrease the number of encoded groups to improve compression ratio. It can exploit a large number of don't care bits to reduce testing power with no compression ratio loss.In the selective Huffman coding method of compression, the area overhead is high compared to other techniques. In the dictionary based approach the occurrence of mismatches will be high. The bitmask based compression method creates more matching patterns but the compression efficiency is less compared to the dictionary based approach. The bit encoding method encodes all the bits in the data. An efficient compression method can be achieved by encoding the selected symbols in the test vector set. That is only the targeted symbols will be encoded in this method. And hence the compression efficiency will be more compared to other techniques. But the efficiency is only for those circuits which are having test vectors with higher length of runs of zeroes or ones.

3.BACKGROUND AND RELATED WORK

Data compression technique is eliminating coarse-grained redundant data, typically to improve storage utilization. It helps reduce the consumption of expensive resources, such as hard disk space or transmission bandwidth. Compression is used just about everywhere. The task of compression consists of two components, an encoding algorithm that takes a data and generates a "compressed" representation (hopefully with fewer bits), and a decoding algorithm that reconstructs the original data or some approximation of it from the compressed representation. These two components are typically intricately tied together since both have to understand the shared compressed representation. The amount of data required to test ICs is growing rapidly in each new generation of technology. Increasing integration density results in larger designs with more scan cells and more faults. Moreover, achieving high test quality in ever smaller geometries requires more test patterns targeting delay faults and other fault models beyond stuck at faults. Conventional external testing involves storing all test vectors and test response on an external tester, which is ATE. Test data compression consists of test vector compression on the input side and response compaction on the output side. Test vector compression has been an active area of research, yielding a wide variety of techniques. The proposed approach combines the selective encoding method and dictionary based encoding method that reduces test data volume and test application time for testing.

4. PROPOSED METHOD

4.1 Dictionary Based Encoding

This method combines the dictionary base encoding method and the selective encoding method Dictionary-based methods are quite common in the data compression domain. While statistical methods use a statistical model of the data and encode the symbols using variable-size codewords according to their frequencies of occurrence, dictionary-based methods select strings of the symbols to establish a dictionary, and then encode them into equal-size tokens using the dictionary. The dictionary stores the strings, and it may be either static or dynamic (adaptive). The former is permanent, sometimes allowing for the addition of strings but no deletions, whereas the latter holds strings previously found in the input stream, allowing for additions and deletions of strings as new input is processed. A simple example of a static dictionary is an English dictionary used to encode English text that consists of words. A word in the input text is encoded as an index to the dictionary if it appears in the dictionary. Otherwise it is encoded as the size of the word followed by the word itself. In order to distinguish between the index and the raw word, a flag bit needs to be added to each codeword.

In the dictionary-based test data compression method, each codeword is composed of a prefix and a stem. The prefix is a 1-bit identifier that indicates whether the stem is a dictionary index or a word of uncompressed test data. If it equals 1, the stem is viewed as a dictionary index. On the other hand, if the prefix equals 0, the stem is an uncompressed word and it is m bits long. The length of the dictionary index depends on the size of the dictionary. If D is the set of the entries in the dictionary, the length of the index l_{index}=ceil [$\log_2$ $|D|$, where|D| is the size of the dictionary. Since $l$index is much smaller than m, the compression efficiency is greater if more test data words can be obtained from the dictionary. However, the dictionary must be reasonably small to keep the hardware overhead low. Fortunately, since there are many don't-care bits in scan test data for typical circuits, we can appropriately map these don't-care bits to binary values and carefully select the entries for the dictionary, so that as many words as possible are mapped to the entries in the dictionary.

4.2 Selective Encoding Method

This approach encodes the slices of test data. Each slice is encoded as a series of C-bit slice-codes, where C=K+2, K=ceil (log2 (N+1)), and N is the number of internal scan chains in the CUT. The number of slice codes needed to encode a given slice depends on the distribution of 1's, 0's, and don't cares in the slice. The proposed technique does not require dedicated test pins for each core in SoC. If cores are tested sequentially, only one common test interface is needed. If some cores are tested in parallel, then they can together be viewed as a larger core with more scan chains. However, if the test sets for the cores are delivered with the don't care bits to the system integrator, an appropriate compression method can be used at the system level to reduce test data volume and testing time. This imposes no additional burden on the core vendor. Un-modelled faults can still be detected if the compression method does not arbitrarily map all don't cares to either 1's or 0's. The proposed approach only encodes a subset of the specified bits in a slice. First, the encoding procedure examines the slice and determines the number of 0s and 1svalued bits. If there are more 1's (0's) than 0's (1's), then all X's in this slice are mapped to 1(0), and only 0's (1's) are encoded. The 0's (1's) are referred to as target-symbol*s* and are encoded into two data codes in two modes. i) Single bit mode and ii) Group copy mode. In the single-bit-mode, each bit in a slice is indexed from 0 to N-1. A target-symbol is represented by a data-code that takes the value of its index. In the group-copy mode, a bit slice is divided into groups, and each group is bits wide. If a given group contains more than one target symbol, then the group-copy mode is used. Two data codes are needed to encode a group. The first data code specifies the index of the first bit of the group, and the second data code contains the actual data. In the group-copy mode, don't cares can be randomly filled instead of being mapped to 0 or 1 by compression scheme. The encoding procedure is as follows:

Step1: Format the given test vectors into slices

Step2: For each slice, determine the number of 0s (k0) and 1s (k1) in the slice.

Step3: If k0 > k1, then target-Symbol: = 1, 1st control-code: = 00; else target-Symbol: = 0; 1st control-code: = 01;

Step4: For each group of the slice, calculate the number of target-symbols;

Step5: If number-of-target-symbols > 1 then encode the group using the group-copy-mode;

else encode the group using the single-bit-mode;

Step6: End for (group);

Step7: Generate slice-codes for the current slice;

Step8: End for (slice);

In Step 1, each test vector is divided into a series of slices. Encode each slice as a series of slice codes. In Steps 2–3, the numbers of 0's and 1's are calculated, and the target symbol as well as the control code of the first slice code is set. The first slice code of each slice must contain an initial-control code (00 or 01). Steps 4-6 encode all the groups of a slice. For each group of a slice, if it contains more than one target symbol, it is encoded using the group-copy mode, otherwise it is encoded using the single-bit mode. Once all groups have been encoded, the slice code generation step (Step 7) becomes straightforward.

5. CONCLUSION

In VLSI design process, data volume minimization and power optimization is major concern. In this project a novel method is proposed for test data volume minimization. The proposed algorithm is to reduce the data volume by compressing the test vectors. The proposed method delivers compressed patterns from the tester to the chip.

6. REFERENCES

[1] M. Abramovici, M.A. Breuer and A.D. Friedman, "Digital Systems Testing And Testable Design", Computer Science Press, 1990

[2]N. A. Tauba, "Survey of Test Vector Compression Techniques", IEEE Transaction Design & Test of Computers, 2006.

[3] Zhanglei Wang, Krishnendu Chakrabarty, "Test Data Compression Using Selective Encoding of Scan Slices" IEEE transactions on Very Large Scale Integration (VLSI) systems, Vol. 16, No. 11, November 2008.

[4] Usha S. Mehta, Niranjan M Devashrayee, Kanker S. Dasgupta, "Hamming Distance Based 2-D Reordering With Power Efficient Don't Care Bit Filling Optimizing the Test Data Compression Method", IEEE, 2010.

[5] Patrick Girard, Laboratory of Informatics, Robotics and Microelectronics of Montpellier "Survey of Low Power Testing of VLSI Circuits", IEEE Design & Test of Computers, 2002.

[6] Witold A. Pleskacz, Tomasz Borejko, Tomasz Gugala, Pawel Pizon and Viera Stopjakova,Def Sim –The Educational Integrated Circuit for Defect Simulation, MSE'05 Anaheim, California, USA– June 12-13, 2005.

[7]K.Paramasivam, Dr.K.Gunavathi, Reordering Algorithm for Minimizing Test Power in VLSI Circuits, Engineering Letters Vol. 14, No. 1, February 2007, pp: 78-83.

[8] Lei Li , Krishnendu Chakrabarty, Nur A. Touba, "Test Data Compression Using Dictionaries with Selective Entries and Fixed- Length Indices", ACM Transactions on Design Automation of Electronic Systems, Vol. 8, No. 4, October 2003, Pages 470–490.

[9] http://www.ece.uic.edu/~masud/resources.html

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 155 - 159, 2013, ISSN: 2319–8656

A Novel Color Image Fusion for Multi Sensor Night Vision Images

J.Jenitha Christinal
Department of Information Technology,
Karunya University
Coimbatore, Tamil Nadu,
India

T. Jemima Jebaseeli
Department of Information Technology,
Karunya University
Coimbatore, Tamil Nadu,
India

Abstract: In this paper presents a simple and fast color fusion approach for night vision images. Image fusion involves merging of two or more images in such a way, to get the most advantageous characteristics of each image. Here the Visible image is fused with the InfraRed (IR) image, so the desired result will be single, highly informative image providing full information. This paper focuses on color constancy and color contrast problem.

Firstly the contrast of the infrared and visible image is enhanced using Local Histogram Equation. Then the two enhanced images are fused in three compounds of a LAB image using aDWT image fusion. This paper adopts an approach which transfer color from the reference image to the fused image using Color Transfer Technology. To enhance the contrast between the target and the background, a scaling factor is introduced in the transferring equation in the b channel. Finally our approach gives the Multiband Fused image with the natural day-time color appearance and the hot targets are popped out with intense colors while the background details present with the natural color appearance.

Keywords: Image Fusion, Histogram Equalization, Color Contrast Enhancement, Color Transfer Technology.

1. INTRODUCTION

The IR image records the thermal radiations emitted by the objects in a scene and can be utilized to discover targets as it has better hot contrast and can present camouflaged targets. The visible image has much higher-frequency information on the background, which is essential for target localization and situation awareness in remote sensing. The IR image contains the information that is not available in the visible image. The IR reflectance of objects will be different from the visible light. A Fusion of IR and visible images with different contents could be utilized to enhance the image quality.

The image fusion method goal is for enhancing the interesting objects to be visible in thermal images against the visible image surroundings. The results can contain the IR band data highlighted with unnatural colors for better perception [1]. The next goal in multiband fused image is to create the colored night vision image. These false colored night images are more pleasing to look than the plain IR images. The color mapping technique produces the results that resembles slightly the natural coloring in the daylight [2].

The color level which human can distinguish is about a hundred times more than the gray level and many experiments shows that the color fusion may improve the feature contrast of the image, which allows for better scene segmentation and object detection [4,5]. Here is to enhance the false color image, we use the color transfer technology which will give the multiband fused image as the natural day-time color appearance and the hot targets pops out with intense colors while the background details present with the natural color appearance. So color fusion is becoming more and more important in the research field and a number of color fusion methods have been proposed.

The Multiband Fusion method for combining infrared image with a visible image concentrates heavily on the surveillance and remote sensing applications. The fusion goal in surveillance is to enhance the interesting objects visible in thermal images against the visible image surroundings. In remote sensing applications Multiband image data are fused to increase the spatial resolution and to improve the information representation [3].

2.ANALYSIS ON MULTI-BAND FUSED IMAGE METHODS

A survey has been done on a different multi-band fused image based on its image fusion method and color transfer method. This analysis help to get the detailed information on various procedures, algorithms, Color Space Transform, Histogram Analysis and accuracy of Segment Recognition.

A. Local-Coloring method: The Local-Coloring method [4] is based on Image Segmentation and Recognition and Local Color Transfer methods are used to enhance the color mapping effect. However, these methods are even more expensive than the global method since they are time-consuming procedures such as Nonlinear Diffusion, Local Recognition, Local Comparisons and Image Segmentation.

B. Fast Natural Color Mapping Method: The Fast Natural Color Mapping method [5] consistently renders the Multi-Band Night Vision Imagery in the natural colors. This method was implemented using standard color lookup table techniques to optimize the match between the false color fused image and the reference image. Once the lookup-table has been derived, the color mapping can be deployed to different multi-band image sequences with similar scenes.

C. One Color Contrast Enhanced Method: The One Color Contrast Enhanced Image Fusion method [6] introduces a ratio of local to global divergence of the IR image into the color transfer equations. As a result, both hot and cold targets are popped out, where hot target appears in intense red and cold targets appears in cyan.

D. EM Algorithm: In EM algorithm [7] the low frequency band image and high frequency band images are fused by Non-Subsampled Contourlet domain. Then the color transfer

method is implemented using YUV color space to make the final fused image. It gives very abundant detail information and the color metric representation.

E. Adaptive Color Fusion Method: In adaptive color fusion method [8] both the Infrared and visible source images are fused using NSCT domain, so as to produce an intermediate fused gray scale image. Then it is mapped into the YUV color space to form a pseudo-color image. Finally, the Color Transfer technique is employed, to give the pseudo-color image with the natural color appearance.

F. Fast Color Contrast Enhancement method: In Fast color contrast enhancement method [9] visible and IR images are pre-processed using Local Histogram Equalization. Consequently, the two enhanced images are fused into the three components of a Lab image by means of a simple linear fusion strategy. Then the color transfer technology in simplified by the Lab color space. But it is different from the global statistic method, by means of transferring equation in the 'b' channel is amended by a stretch factor. It will change according to the distance between the current luminance value and the mean luminance value.

These surveys present different methods with its own strengths and weaknesses. The block diagram of Image Fusion for Night Vision Image is shown in Figure 1

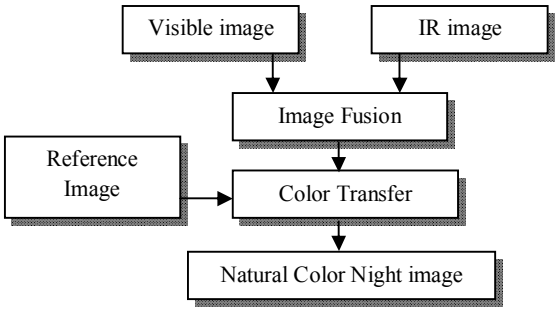


Figure 1 Block diagram of Image Fusion for Night Vision Image

3. IMAGE FUSION

The IR and visible light cameras have their own unique characteristics. Images taken in the visual spectrum tend to preserve good contextual information, while in night vision they usually show poor perception among objects due to the low contrast. IR images are almost insensitive to the change of light condition, so it may be more reliable to distinguish the targets from the background by the thermal contrast. To improve this, the contrast histogram equalization is done before the image fusion.

3.1 Image Enhancement

The proposed method consists of Histogram equalization; it's an effective method of improving the quality of low contrast images that is done by stretching the dynamic range of an image's gray level. This Histogram equalization method consists of global and local methods. Histogram equalization methods rescale the pixel values in an input image, to cover the entire available gray level image.

The contrast of an image is enhanced by the Global Histogram Equalization which is performed by enlarging the intervals of dense gray levels and also reducing those of sparse gray levels. The global Histogram Equalization method brings more noise if they occupy many numbers of pixels and other disadvantage is the images with extra high contrast make observer tired and anxious, which are not suitable for long time observation. To overcome these drawbacks, enhanced Visible and IR images were used.

In this method, First step is image segmenting, the input image is divided into several non-overlapping regions with the size of 5x5 and cumulative distribution function (CDF) is applied to the divided image, rather than the entire image. Then neighbouring regions are combined using bilinear interpolation to remove the artificially induced boundaries. The new pixel value is $f'(i,j)$ at the position (i,j) is[7]:

$$f'(i,j) = (1-u)(1-v)f(i,j) + (1-u)vf(i,j+1) + u(1-v)f(i+1,j) + uvf(i+1,j+1) \quad (1)$$

where $f'(i,j), f(i,j+1), f(i+1,j)$ *and* $f(i+1\ (j+1)$ are the values before interpolation in the enhanced image and u, v are constant values $u, v \in [0,1]$

3.2 Fusion of Infrared and Visible Image

The enhanced Visible and IR image is fused by an Advanced Discrete Wavelet Transform (aDWT) method that incorporates the Principal Component Analysis (PCA) and Morphological Processing into a regular DWT fusion algorithm. The DWT method follows the multi-scale analysis method as same as the pyramid method. In DWT, the co-efficients of two input images are fused pixel-by-pixel by choosing the average of the approximation co-efficients in the highest transform scale,in order to find largest absolute value of the detail co-efficients at each transform scale is processed. Then the inverse DWT is performed to obtain the fused image.

We incorporate Principal Component Analysis (PCA) and Morphological Processing into a DWT algorithm in order to obtain aDwt image fusion.

Step 1: To get DWT co-efficients of an image, the image is divided into four quarters: approximation detail, vertical detail, horizontal detail and diagonal detail.

Step 2: Apply PCA to the two input images approximation co-efficients at the highest transform scale that is by using the principal eigenvector derived from the two source images, as described below[6]:

$$E_F = (a_1 \cdot E_A + a_2 \cdot E_B)/(a_1 + a_2) \quad (2)$$

where E_A and E_B are approximation co-efficients transformed from input images A and B. E_F represents the fused co-efficients, a_1 and a_2 are the elements of the eigenvector, which are computed by analyzing the original input images.

Step 3: Apply morphological processing, such as 'filling' and 'cleaning' operation to the image. Both filling and cleaning are the Matlab built-in morphological operation. Filling is used to fill the isolated interpixels and cleaning is used to remove the isolated pixels. These operations increase the consistency of co-efficient selection there by reducing the distortion in the fused image.

4. COLOR TRANSFER

In this proposed color transfer method, Color Based Clustering is applied on the Lab color space. Then Cluster Based Color Transfer is performed from natural color images using color similarity metric. The block diagram of the Color Transfer method is shown in Fig. 2.

The false color fusion can translate the gray information into easily distinguishable color information. Therefore

combining all the bands in color space, it provides a method to increase the dynamic range of a sensor system. In the proposed method the false color fusion is performed in RGB color space. The false color fused RGB image can be represented by the following equations[11]:

$$R(m,n) = 1/2\ \left(vis(m,n) + IR(m,n)\right) \quad (3)$$

$$G(m,n) = IR(m,n) \quad (4)$$

$$B(m,n) = |vis(m,n) - IR(m,n)| \quad (5)$$

Here m, n are the co-efficients values of each transforms. So the formed false color fused image has the intensity variations similar to the visible and IR source images. In order to achieve better separation in color based clustering, Decorrelation Stretch will be performed for color enhancement and Linear Contrast Stretch performed for intensity enhancement. Decorrelation Stretch increases the color separation across highly correlated channels by keeping the band variance as same. It is followed by a linear contrast stretch on individual RGB channels. The enhanced false color image obtained has more color variation and better contrast which significantly facilitates the subsequent clustering process.

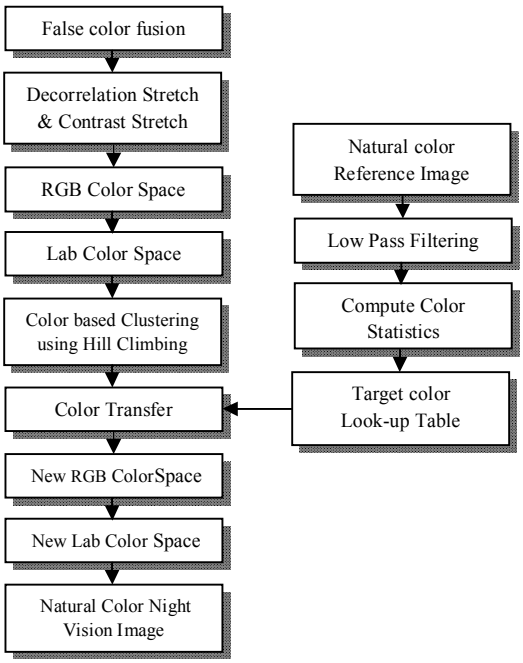


Fig. 2 Block diagram of the Color Transfer method for the Fused Image

4.1 Color Based Clustering

The enhanced false color fused image is converted to an indexed image where each pixel contains a single index which refers the RGB value in a color lookup table or color space. The RGB color space is then transformed into Lab color space to generate the Lab color space of the same size. Performing the color space transform decorrelates the three color components (i.e. L, a and b) so that manipulations such as statistic matching on each color component can be performed independently.

Color Based Clustering is performed on the Lab color space using the Hill Climbing Algorithm. A color based image segmentation method using Hill Climbing algorithm is utilized for Coloma clustering. The numbers of clusters required for proper classification of colormap are automatically determined by the Hill Climbing algorithm. The entries of the color space are then associated with the local maxima detected by the algorithm, to generate several coherent clusters in the Lab color space. The color transfer based on target color look-up table derived from the reference color images, gives the consistent color rendering and more natural appearance [4].

The target color look-up table is created as follows: From each image from the natural color target image is smoothed by the low pass filter and then transformed into the Lab color space and first order statistics, mean and standard deviation, are computed for each band.

4.2 Color Transfer Technique

Color transfer opertation is performed by cluster-by-cluster using standard statistics matching method,Toet [5].

Then Lab color transformation is performed.

$$L = 116 \times f(Y/Y_n) - 16 \quad (6)$$

$$a = 500 \times f(X/X_n) - f(Y/Y_n) \quad (7)$$

$$b = 200\ \times f(Y/Y_n) - f(Z/Z_n) \quad (8)$$

Here X_n,Y_n, Z_n are the tristimulus values of reference white point, a line passing through an opposite color. Then the transformation is accelerated and normalized as follow: X_n,Y_n, Z_n are the values used to normalize X, Y, Z separately. In order to obtain the natural appearance, enhance the color transfer based on the color contrast.

Step 1: Subtract the mean value from the fused image data points, (i,e,)

$$\tilde{L} = L - \langle L_{fue} \rangle \quad \tilde{a} = a - \langle a_{fue} \rangle \quad \tilde{b} = b - \langle b_{fue} \rangle \quad (9)$$

Here $L_{fue}, a_{fue,} b_{fue}$ is mean value of each channel.

Step 2: Then the data point are scaled with the help of the standard deviation of the fused image to the reference image.

$$L' = \frac{\sigma_{n,t}^{L}}{\sigma_{k,s}^{L}}\ \tilde{L} + L_{fue} \quad a' = \frac{\sigma_{n,t}^{a}}{\sigma_{k,s}^{a}}\ \tilde{a} + a_{fue} \quad b' = \frac{\sigma_{n,t}^{b}}{\sigma_{k,s}^{b}}\ \tilde{b} + b_{fue} \quad (10)$$

where k[th] cluster is associated with n[th] natural image in the color look-up table, and s and t denote source and target respectively. The modified values of each transformation L, a, b form a new transformation in Lab color space such that L', a', b'.

4.3 Enhancing the Target Detection

After applying the color transformation to the fused image, the target detection is still ambiguous. The target detection cannot be achieved only by the intensity information in the color image fusion scheme.

Fortunately, the color contrast provides another cue in the color fused image, which makes the separation between the target and the background easier. So, the color image fusion should pop out targets in an instant color to improve their delectability.

To enhance the color contrast between the target and the background, we process each pixel in the blue - red channel with a stretch factor w

$$b' = w.\frac{\sigma_{n,t}^{b}}{\sigma_{k,s}^{b}}\,\tilde{b} \quad (11)$$

Here in the IR image, the hot targets have larger luminance values. To maintain these characteristics, the stretch factor $w(i,j)$ of each pixel (i,j) in the fused image is defined as, [4]

$$w(i,j) = k \cdot dist(i,j) \,/\, \langle dist \rangle \quad (12)$$

$$\langle dist \rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} dist(i,j) \,/\, m \times n \quad (13)$$

$$dist(i,j) = \|L(i,j) - \langle L \rangle\| \quad (14)$$

where k is a constant that can be modified according to the actual requirement for the enhancement. $dist(i,j)$ denotes the luminance divergence of the pixel (i,j) from the mean intensity of L channel in the fused image. $L(i,j)$ and $m \times n$ are luminance value of the pixel (i,j) and the size of the fused image separately.

As the hot target has great divergences to the mean intensity of L channel, it can be enhanced. Due to the color contrast enhancement, the hot targets are showed as intense red colors and the background are in natural color. Once the color processing is completed, the Lab color space is converted back to RGB color space.

5. EXPERIMENTAL RESULTS

The experimental result for UN camp image corresponding to the forest environment is shown in Fig.3. As shown Fig 3 (a) is a Visible image, in which the background is clearly showed, Fig 3(b) is an Infrared image in which source information cannot be detected, where the thermal information is visible. Both visible and infrared are the two input images. Fig 3 (c) is a reference color image of same size as the source image. Fig 3 (d) is a result of aDWT image fusion. Fig 3(e) is a result of the color transformation, where the color appearance indeed looks more natural, but the target can be hardly distinguished. Fig 3(f) the target is popped out with the intense red color. The average computational time to generate the color night vision image is 6-7 seconds and to obtain the fused image is 3-4 seconds.

Entropy is used to measure the information content of an image. The entropy of the natural colored night vision image is computed for each band in RGB color space and the average of the entropy of the three bands is considered for evaluation.

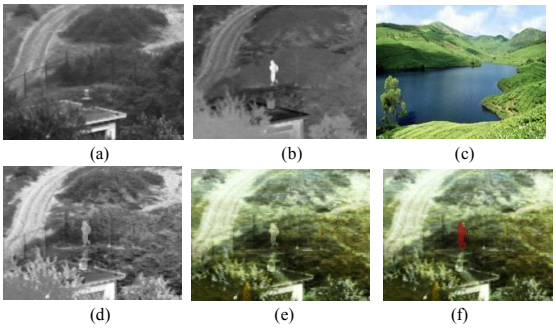


Fig 3 (a) Visible image (b)Infrared image (c) Reference image (d) aDwt fused image (e) Natural color image without target enhancement (f) Natural color image with target enhancement

Fig. 3 Result of UN Camp Night Vision Image

Colorfulness Metric is an efficient metric for calculating the colorfulness of the images; therefore the proposed method has the higher colorfulness metric. Finally the proposed method gives the Multiband Fused image as the natural daytime color appearance. From the proposed method the obtained entropy value and colourfulness metric value which is compared with statics matching method [4] and shown in Table 1.

Table 1. Comparison on Multi Band Fused Image

Parameters	Statistics Matching [4]	Proposed Method
Entropy Value	6.6375	6.7294
Colorfulness Metric	0.1852	0.3982

6. CONCLUSION

In this paper, we proposed a simple and fast fusion approach for night vision image. Before fusion, the quality of both visible image and Infrared image is improved by using the Local Histogram equation and then the images are fused. To get the natural color image, the color is transferred from the reference image to the fused image by using Lab color space and the contrast between the target and the background is enhanced using a scaling factor. So the hot targets are popped out with intense red colors while the background details present with the natural color appearance.

7. REFERENCES

[1] A. Toet, J.I.J speert, A. Waxman, and M. Aguilar, "Fusion of visible and thermal imagery improves situational awareness," Displays, vol. 18, pp.85-95, 1997

[2] C. Pohl and J. L. van Gendern, "Multisensor image fusion in remote sensing concepts, methods and applications," International Journal of Remote Sensing, vol. 19, pp. 823-854, 1998.

[3] G.L. Walls. "The vertebrate eye and its adaptive radiation", Granbrook Institute of Science, Bloomfield Hills, Michigan, 2006.

[4] M.A. Hogervorst, A. Toet, "Fast natural color mapping for night-time imagery", Information Fusion 11 (2010).

[5] A. Toet, "Natural color mapping for multiband night vision imagery", Information Fusion 4 (2003)

[6] Y. Zheng and E. A. Essock, "A local-coloring method for night-vision colorization utilizing image analysis and fusion" Information Fusion, vol. 9, pp. 186 - 199, 2008.

[7] S.F. Yin, L.C. Cao, Y.S. Ling, et al., "One color contrast enhanced infrared and visible image fusion method", Infrared Physics and Technology 53 (2010) 146– 150.

[8] Gang Liu1, Guohong Huang2 "Color Fusion Based on EM Algorithm for IR and Visible Image" 2010 IEEE

[9] Weihua He, YongcaiGuo, Chao Gao "An adaptive color fusion method for night-vision images with NSCT" 2011 Elsevier.

[10] IshitMakwana, TanishZaveri and Vivek Gupta "Efficient Color Transfer Method based on Colormap Clustering for Night Vision Applica- tions " 2011 IEEE.

[11] "Night vision multiband source images data set available: http://www.imagefusion.org."

[12] M. A. Hogervorst and A. Toet, "Evaluation of a color fused dual-band nvg," International Conference on Information Fusion,

[13] R. S. Blum and Z. Liu, "Multi-sensor image fusion and its applications," Taylor & Francis, CRC Press, 2006.

[14] D. Hasler and S. Suesstrunk, "Measuring colorfulness in natural images," Proc of Human Vis and Elect. Image. VIII. Santa Clara, CA, USA, 2003.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 160 - 165, 2013, ISSN: 2319–8656

A new Approach towards Cost and Benefit Enterprise Architecture Analysis

Ali Abediniyan
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Khouzestan, Iran

Mehran Mohsenzadeh
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Tehran, Iran

Mashalla Abbasi Dezfouli
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Khouzestan, Iran

Abstract: Organizations managers need to develop comprehensive information technology programs with an Enterprise Architecture (EA) strategy, in order to decrease the costs and different risks, and also increase efficiency, utility and effectiveness of the organization. Due to expensive implementation of enterprise-wide scenarios, a continuous evaluation can measure different strategies in terms of different aspects, and according to the current conditions of the organization and select the most suitable strategy. Therefore organizations can analyze different strategies and decision options in terms of cost and benefit in order to make suitable decisions according to the utilities of the organization. In this paper, a new method has been used to analyze the Enterprise Architecture scenarios in terms of cost and benefit. The suggested method is presented by a step by step process in which CBAM method has been utilized to measure the cost. This approach ranks enterprise scenarios, using knowledge and experiences of the enterprise experts. The applicability of the proposed approach is demonstrated using a practical case study.

Keywords: Enterprise Architecture Analysis, Return of Investment (ROI), quality attributes, cost and benefit, organizational capitals.

1. INTRODUCTION

Enterprises are complex, highly integrated systems comprised of processes, organizations, information and supporting technologies, with multifaceted interdependencies and interrelationships across their boundaries [4]. Conduct and control of organization changes need to have exact information from the current conditions, a good view toward the desirable conditions and a clear program to move from the current conditions to a desirable and pleasant status [1].

Organizations managers need to develop comprehensive information technology programs with an Enterprise Architecture (EA) strategy, in order to decrease the costs and different risks, and also increase efficiency, utility and effectiveness of the organization [1]. Enterprise Systems Architecting is a new strategic approach which takes a systems perspective, viewing the entire enterprise as a holistic system encompassing multiple views such as strategic view, policy/external environment view, organization view, process view, knowledge view, information technology view, product view, service view and relations among these views, in an integrated framework [4][5]. Enterprise architecture provides necessary information platform and strategies to analyze organizations' current conditions, recognize desirable targets by analyzing, examining and selecting from the different variables, and also move from the current status to the desired status. Decisions are made about the alternatives in the context of the business model, technology strategy, culture, purpose, and other factors [4]. By including all such data the architecture can provide the capability to make informed investment decisions, decisions based on a complete understanding of the complex interrelationships that exist among the people, processes, and technology solutions that make up the enterprise. [4]. EA analysis is the application of property assessment criteria on EA models [2].

Due to expensive implementation of enterprise-wide scenarios, examining advantages and disadvantages of the suggested programs before execution would be valuable. In this case, waste of enterprise resources will be significantly prohibited, and the analysis and examination of different approaches can determine not only the selection of the best approach among others, but also the weakness and strengths of the current condition of the organization, in order to determine the guidelines of organization development in future [3].

One of the Software Architecture analysis methods is CBAM. CBAM makes a bridge between development of software and organization economy during the architecture process [17]. One of the main advantages of this method is to provide a measurement scale to return investments and help prepare an evaluated program for architecture development and investment [18]. In the suggested method, CBAM idea was used to measure the benefit of organizational decisions.

Different methods have been already presented to analyze enterprise architecture but none has directly assessed organizational decisions in terms of cost and profit. The main purpose of this paper is to suggest a method to analyze cost and profit of enterprise architecture based on quality attributes. In the suggested method options of enterprise architecture are be profitable and then their costs will be estimated. Therefore investment return of each plan will be obtained. By measurement of investment return of scenarios, waste of financial , human and organizational capitals can be prevented. Also, the enterprise options can be explained economically to execute the decisions with the minimum risk. Presence of a method to analyze cost and benefit of EA can help the organizations select the optimum EA scenarios according to organizations' utilities. In the suggested method, the organization utilities include quality attributes.

It is noteworthy, in during this paper, cases is compared that these can be decisions, scenarios, projects, or goals.

This paper is structured in the following way. Section 2 introduces the current methods in the field of Enterprise Architecture Analysis. In section 3 the proposed method is presented to analyze the cost and benefit of EA scenarios. In section 4, a case study has been applied to demonstrate the application of the suggested method and provide an environment to measure its executive credit and the results show the internal validity of the method. Finally, the paper concludes and future work are discussed in section 5.

2. RELATED WORK

Different methods have been presented to analyze Enterprise Architecture (EA). Some of the methods are based on a special framework and some are independent from framework and are provided based on EA concepts. Some of the methods concentrate on analysis and measurement of EA projects in terms of techniques.

The related work is discussed in this paper are from three perspectives:

1. It is clear from the study of the Enterprise Architecture analysis methods that the most provided methods analyze data according to EA models and consider quality attributes. Only the approaches provided by Neimann [6], Khayyami [3] and Razavi [2] use both EA information and EA models.

2. from the studies methods, the one presented by Yu and associates [7], incompletely and in elementary forms, the one introduced by Jacob and Jonkers [8], the one presented by KHayyami [3], the one provided by Razavi [2] and also the ones presented by researcher group of KTH university of sweden [9][10][11][12][13][14][15], directly analyze quality and quantity properties of the methods and other methods analyze non applicable properties or enterprise efficiencies.

3. In Neimann [6], cost and benefit of enterprise efficiency are studied abstract . Frank and associates [16], is also a method to project and apply business indicator system in which most attributes are economical and indicators data are provided based on statistical data obtained from the enterprise behavior.

These methods mostly study the EA models formally and determine the analysis parameters, but no method has been provided to analyze the cost and benefit of organization decisions directly. The proposed method has been analyzed based on quality attributes' benefits and decisions cost. Due to expensive implementation of enterprise-wide scenarios, their evaluations is very important in terms of cost and benefit, and the organization can estimate cost and benefit of their decisions and find a way for accurate and informed decisions.

3. THE PROPOSED METHOD

The suggested process is shown in figure 1, As it can be seen in the figure, the process includes six main steps. In this process, in step 5 divide difference interpolation method has been used to obtain quality attributes utility. In steps 2,3 and 4 information are collected according to the knowledge and experience of enterprise experts. Also, total cost is estimated by managers and advisors for each project of the organization.

It should be noted that there are different formal methods of estimating costs according to the activities and the organization can use any of the current methods in this step. In step 6, organizational scenarios prioritized according to ROI.

Step 1 Step 1-1	Determination of scenario organization Determination of scenarios activities
Step2	Determination of quality attributes
Step 3	Determination of the levels of activities response
Step 4	Assignment of activities benefits
Step 5	Computation of the quality attributes utility and estimation of total cost
Step 6	Analysis and ranking based on ROI

Figure 1. The proposed process towards Enterprise Architecture scenarios analysis

3.1 The proposed method steps

Step1: Determination of scenarios of the organization

Enterprise goals may include adding/changing new business processes, changing enterprise structure, changing enterprise departments, variation of business market, changing economic policies and ....

In this step, managers and consultants of the organization, determine scenarios of the organization. These scenarios can have any level of granularity or be related to any time section. For example, annual projects of an organization. Sometimes, organizations need to perform projects to make changes regarding their needs.

Step1-1: Determination of scenarios activities.

Organizations need to do some activities in order to reach and execute EA scenarios, and they are specified in this step. These activities contain sub activities and these need executable programs to be performable.

Step2: determination of attributes

In each organization, there are some specified attributes and indicators for measuring efficiency of organization decisions. The indices of organization purpose measurement can be determined by Delphi technique. Delphi technique is a method which gathers opinions of experts by distribution of a questionnaire and then reaches them to the opinion of the majority.

In the proposed method a questionnaire is distributed between experts of different regions and their opinions are collected. Therefore, the most important quality attributes will be determined. It should be noted that indices and attributes are named as quality attributes here.

Step3: Determination of the levels of activities response

In this step best, worst, current and desired responses of the quality attributes are extracted for each of the goal activities. Quality attributes response levels are weighted by each of the experts. These values are assigned in percent.

The four independent values are described as below:

The best status: In this status the best status of the goal is expressed from the view point of stakeholders and of course there is no need to improve more than this value.

The worst status (minimum needs): This status specifies the minimum expectations. It should be

considered that the best and the worst status are assumed as the reference points and, current and desired status are measured on their basis.

Current status: A ratio of the best and the worst- X%

Desired status: A ratio of the best and the worst- Y%

Regarding the fact that attributes and utilities are for the decisions and goals of the whole organization, a scenario or goal could not have a zero value for an attribute in all statuses.

Step4: assignment of activities benefits

In this step a utility is assigned to each level of quality attributes response (Best, Worst, Current and Desired status), related to it. This value assignment is done by the enterprise experts.

utility: The profit obtained for the stakeholders of the organization is called utility. The value of utility is from 100.

Step 5: Computation of the quality attributes utility and estimation of total cost

In this step, the desired utility of quality attributes is obtained by Formula.1 and F(x) is obtained by divide difference interpolation method. In interpolation, Xi is the levels of activities response (output of step 3) and, Yi is the utility of activities or duties (output of step 4). After obtaining function F(x), level of response of the quality attribute in the project are given values and the desired utility will be obtained. Then the quality attribute utility is obtained by formula.2.

F(x= reply of quality attribute by scenario)= Desired utility (1)

The quality attribute utility= desired utility - current utility (2)

Utility of the project is the sum of utility from each activity. Also, in this step the total cost is estimated by the organization.

Step6: Analysis and ranking based on ROI

In previous steps, the total benefit of the project was measured for each of the purposes or the organization projects towards the quality attributes. The project cost is also estimated. Therefore, ROI can be measured for each scenario in EA regarding formula.3.

$$ROI_i = \frac{B_i}{C_i} \quad (3)$$

4. A CASE STUDY USING THE METHOD

In this section it`s been tried to check the validity of the suggested method by choosing an appropriate project for a case study. Our case study is conducted in Ports & Maritime Organization of Iran (PMO). This enterprise as the maritime administration of Iran administers the ports and commercial maritime affairs of the country. Till some time ago, this enterprise was working according to the responsibilities defined by the Ministry of Road and Transport, but now some changes has occurred to the responsibilities and the organizational structure, and a new version of organizational chart and functionality description will be announced. So business process and functionality maintenance seems to be an important issue to be considered in an EA solution proposed for PMO.

In the following, steps of the suggested method will be described with the so-called case study.

Step1: Determination of scenarios of the organization

The following scenarios are parts of immense goals of the organization in 2011.

1- Increasing the capacity of passenger transportation

2- Improvement of the security level

Step1-1: Determination of scenarios activities

In this stage, activities and duties considered to reach the immense goals are determined.

1-Increasing capacity of passenger transportation

1-1-Completion and development of passenger wharves

2-Improvement of security level

2-1- preferment of security level of maritime in navy

2-2-Improvement of security level of sailor degrees

2-3-Establishment and execution of Information Security Management System(ISMS)

2-4-Design and development of Information Technology

2-5-Estimation of damages, design and performance of protective systems

Step2: Determination of attributes

As mentioned above, indicators are the quality attributes of an organization , and are as follow:

1- Flexibility
2- Efficiency or on time services
3- Security
4- Interaction and extensibility levels
5- Usability or satisfaction of the customers
6- Investment absorption

Step3: Determination of the levels of activities response

In this step and the next one, four expert viewpoints were used regarding the goals and activities of the organization. Table 1 shows response levels of the attributes by one of the experts which is related to the first goal. Also, table 2 shows results of the second goal by three other experts of the organization.

Step4: assign of activities or duties benefit

In this step, a utility was assigned to each response level of the quality attributes (the best, worst, current and desired status), relating to that status. Information about this stage is shown in tables 3 and 4.

Step5: Computation of the quality attributes utility and estimation of total cost

Table 2. Quality attributes response levels associated by expert #2, #3, #4

Table 1. Quality attributes response levels associated by expert #1

States	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best
Activities \ Attributes	1				2				3				4				5				6			
1-1	15	50	80	95	10	60	90	100	5	50	70	90	0	40	60	85	10	40	85	100	5	55	85	100
2-4	0	0	0	0	0	0	0	0	10	61.67	90	100	8.33	48.33	81.67	91.67	0	0	0	0	0	0	0	0
2-5	0	0	0	0	0	0	0	0	5	45	90	100	0	0	0	0	0	0	0	0	0	0	0	0

In this step, by using Newton divided difference interpolation method, utility of each quality attribute was measured for each goal and their results are shown in tables 5 and 6.

	Attributes	response by scenario	

Table 3. Utility associated activities by expert #1

States	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best
Activities \ Attributes	1				2				3				4				5				6			
1-1	5	60	95	100	20	55	90	100	10	55	70	95	0	55	60	85	10	40	90	100	10	45	85	100

Table 4. Utility associated activities by experts #2, #3, #4

States	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best	Worst	Current	Desires	Best
Activities \ Attributes	1				2				3				4				5				6			
Utility associated activities by group																								
2-1	0	0	0	0	0	0	0	0	10	53.33	83.33	100	0	0	0	0	0	0	0	0	0	0	0	0
2-2	0	0	0	0	0	0	0	0	6.67	55	85	98.33	0	0	0	0	0	0	0	0	0	0	0	0
2-3	0	0	0	0	0	0	0	0	11.67	45	83.33	100	0	0	0	0	0	0	0	0	0	0	0	0
2-4	0	0	0	0	0	0	0	0	15	51.67	85	100	8.33	53.33	86.67	100	0	0	0	0	0	0	0	0
2-5	0	0	0	0	0	0	0	0	6.67	51.67	90	100	0	0	0	0	0	0	0	0	0	0	0	0

Step6: Analysis and ranking based on ROI

For each one of the purposes or projects of the organization the level of its benefit has been calculated against the quality attributes and the project cost was also estimated.
Therefore, for each scenario of EA the ROI can be calculated. Formulas 4 and 5 obtain the ROI for each project.

$$ROI_1 = \frac{175.1253}{150} = 1.1675 \quad (4)$$

$$ROI_2 = \frac{167.8127}{130} = 1.2909 \quad (5)$$

So, ranking of scenarios are shown in table 7. As it was mentioned scenario 2 is more prioritized than scenario 1 in terms of ROI. In addition the organization can explain its projects economically and then codify a program to execute it.

Table 5. Utility associated for scenario 1

Scenario	Quality	Quality attribute	Utility
1	1	0/7	24.5788
	2	0/8	18.5565
	3	0/8	25.6731
	4	0/8	21.6667
	5	0/95	57.3086
	6	0/75	27.3416

Table 6. Utility associated for scenario 2

Scenario	Quality Attributes	Quality attribute response by scenario	Utility
	3	0/85	32.9106
	3	0/7	15.6008

2	3	0/85	52.4593
	4	0/7	33.3978
	3	0/75	14.1398
	3	0/8	29.3044

5. CONCLUSION AND FUTURE WORK

In this paper, we present a cost and benefit method to evaluate scenarios of EA. The proposed method helps managers and decision makers select EA decisions regarding cost and benefit ranking and the best scenario of EA in terms of ROI. Also, organization can explain its projects economically and then codify a program to execute it.

As future work, indices can be divided into two positive and negative (benefit and cost) groups and weighted. To do this, group decision making methods like AHP and TOPSIS can be introduced to evaluate EA scenarios.

6. REFERENCES

[1] Samadi Avansar, A., "An Introduction to The Enterprise Architecture (For Managers)", 2006.

[2] Razavi, M., "A New Framework for EA Quality Attribute Analysis", thesis, Science and Research Branch, Islamic Azad University,Tehran, Iran, 2011.

[3] KHayami, R., "Enterprise Architecture Analysis and Evaluation", thesis, Department of Engineering, Shiraz University, Iran, 2009.

[4] Nightingale, D.J., Rhodes, D.H., "Enterprise Systems Architecting: Emerging Art and Science within Engineering Systems", MIT Engineering Systems Symposium, pp. 29-31, 2004.

[5] Rhodes, D.H., Ross, A.M., Nightingale, D.J., "Architecting the System of Systems Enterprise: Enabling Constructs and Methods from the Field of Engineering Systems", 3rd Annual IEEE Systems Conference, Vancouver, BC, pp. 190-195, 2009.

[6] Niemann, K.D., "From Enterprise Architecture to IT Governance ElementsofEffective IT Management, Vieweg+Teubner, Wiesbaden, Germany, 2006.

[7] Yu, E., Strohmaier, M., Deng, X., "Exploring intentional modeling and analysis for enterprise architecture", Proceedings of the EDOC 2006 Conference Workshop on Trends in Enterprise Architecture Research (TEAR 2006), Hong Kong, IEEE Computer Society Press, pp. 32, 2006.

[8] Jacob, M.E, Jonkers, H., "Quantitative analysis of enterprise architectures", In Konstantas, D., Bourrieres, J.P., Leonard, M., Boudjlida, N., eds.: Interoperability of Enterprise Software and Applications, Geneva, Switzerland, Springer, pp. 239-252, 2006.

[9] Johnson, P., Johansson, E., Sommestad, T., Ullberg, J., "A Tool for Enterprisen Architecture Analysis", in Proceedings of the 11th IEEE Enterprise Distributed Object Computing Conference, IEEE Computer Society, USA, pp. 142-156, 2007.

[10] Johnson, P., Lagerström, R., Närman, P., Simonsson M., "Enterprise architecture analysis with extended influence diagrams", Information Systems Frontiers. 9(2-3), pp. 163-180, 2007.

[11] Johnson, P., Lagerström, R., Närman, P., Simonsson, M., "Extended Influencen Diagrams for System Quality Analysis", Journal Of Software (JSW), 2(3), pp. 30-42, 2007.

[12] Johnson, P., Lagerström, R., Närman, P., Simonsson, M., "Extended Influence Diagrams for Enterprise Architecture Analysis", in Proceedings of the 10th IEEE Enterprise Distributed Object Computing Conference, pp. 3-12, 2006.

[13] Johnson, P., Nordstrom, L., Lagerstrom, R., "Formalizing analysis of enterprise architecture", In: Doumeingts G, Muller J, Morel G et al (eds) Enterprise Interoperability-New Challenges and Approaches, Springer London, pp. 35-44, 2006.

[14] Lagerström, R., "Analyzing System Maintainability Using Enterprise Architecture Models" Proceedings of the 2nd Workshop on Trends in Enterprise Architecture Research (TEAR'07), St Gallen, Switzerland, pp. 31-39, 2007.

[15] Lagerström, R., Johnson, P., "Using Architectural Models to Predict the Maintainability of Enterprise Systems", 12th European Conference on Software Maintenance and Reengineering, pp. 248-252, 2008.

[16] Frank, U., Heise, D., Kattenstroth H., Schauer H., "Designing and utilizing business indicator systems within enterprise models-outline of a method", in Proceedings of Modeling Business Information Systems Conference (MobIS 2008), Saarbrucken, Germany, pp. 89-1, 2008.

[17] Clements, P., Kazman, R., Klein, M., "Evaluating Software Architecture: Methods and Case Studies",2nded Addison- Wesley, Reading, MA, USA, 2002.

[18] IEEE, "IEEE standard recommended practice for architecture description", IEEE Std 1471-2000, 2000.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 166 - 169, 2013, ISSN: 2319–8656

An improvised tree algorithm for association rule mining using transaction reduction

Krishna Balan
Pondicherry Engineering College
Pondicherry, India

Karthiga
Pondicherry Engineering College
Pondicherry, India

Sakthi Priya
Pondicherry Engineering College
Pondicherry, India

Abstract: Association rule mining technique plays an important role in data mining research where the aim is to find interesting correlations between sets of items in databases. The apriori algorithm has been the most popular techniques in finding frequent patterns. However, when applying this method a database has to be scanned many times to calculate the counts of the huge umber of candidate items sets. A new algorithm has been proposed as a solution to this problem. The proposed algorithm is mainly concentrated to reduce the candidate sets generation and also aimed to increase the time of execution of the process.

Keywords: Apriori; association; candidate sets; data mining; itemsets;

1. INTRODUCTION

As the rapid growth of the information technology the data's has been stored in the form of digital systems. As tremendous amounts of data are thus generated due to the full digitization. Data mining plays an important role to extract meaningful information from the scattered data. Association rule is a popular technique which is used for finding interesting relationship between variables in large databases. R. Agrawal and R. Srikant in 1994 presented the apriori algorithm for mining frequent itemsets which is based on the generation of candidate itemset. Several different algorithms have been proposed for association rule. In this paper a new algorithm has been proposed for association rule. The proposed algorithm has been implemented by comparing all the demerits of the existing systems. The main goal of the proposed system is to speed up the computation process.

2. RELATED WORKS

There are various algorithms were proposed for finding the frequent itemsets . The best well known for the rule mining is the apriori algorithm which was proposed by the Agrawal and Srikant (1994) [2]. This uses the concept of candidate generation. Although the apriori algorithm is efficient in finding the item sets the execution time gets longer when the database size increases since it has to generate the candidate item-sets. Many algorithms have been proposed to overcome the drawbacks of the a priori such as the FP-Growth algorithm [4] were proposing a new idea for the candidate set generation problem where it introduces a Tree structure concept where it distributes the workload as it relies on the depth first search. It implies that it is faster than the apriori where there is no candidate generation as it uses the divide and conquer approach such that the database is scanned only twice. The matrix Apriori algorithm[6] is proposed in order to improve the efficiency time of the apriori algorithm where this uses the combined approach of the apriori and the fp-growth algorithm. The description and implementation of the above algorithms are briefly explained below.

2.1 Apriori Algorithm [2]

One of the first algorithms to evolve for frequent itemset and Association rule mining was Apriori. Two major steps of the Apriori algorithm are the join and prune steps. The join step is used to construct new candidate sets. A candidate itemset is basically an item set that could be either Frequent or infrequent with respect to the support threshold. Higher level candidate itemsets (Ci) are generated by joining previous level frequent itemsets are Li-1 with it. The prune step helps in filtering out candidate item-sets whose subsets (prior level) are not frequent. This is based on the anti-monotonic property as a result of which every subset of a frequent item set is also frequent.Thus a candidate item set which is composed of one or more infrequent item sets of a prior level is filtered(pruned) from the process of frequent itemset and association mining.[4]

2.2 FP-Growth Algorithm [6]

The FP-Growth methods adopts a divide and conquer strategy as follows: compress the database representing frequent items into a frequent-pattern tree, but retain the itemset association information, and then divide such a compressed database into a set of condition databases, each associated with one frequent item, and mine each such database [8].

First, a scan of database derives a list of frequent items in descending order. Then the FP - tree is constructed as follows. Create the root of the tree and scan the database second time. The items in each transaction are processed in the order of frequent items list and a branch is created for each transaction. When considering the branch to be added

to a transaction, the count of each node along a common prefix is incremented by 1. After constructing the tree the mining proceeds as follows. Start from each frequent length-1 pattern, construct its conditional pattern base, then construct its conditional FP-tree and perform mining recursively on such a tree. The support of a candidate (conditional) itemset is counted traversing the tree. The sum of count values at least frequent item's nodes gives the support value.

2.3 DH Algorithm [1]

In order to improve the execution time of the apriori algorithm there are many algorithms have been implemented. The DH (Direct Hashing) algorithm has been proposed for reducing the database rescanning. The DHCP algorithm is an effective hash based algorithm for the candidate set generation. It reduces the size of the candidate set of filtering any k item set out of the hash table if the hash entry does not have minimum support. The hash table structure contains the information regarding the support of each item set. The DHP algorithm consists of three steps. The first step is to get a set of large itemsets and constructs a hash table for 2 itemset. The second step generates the set of candidate itemsets Ck. The third step is the same as the second step except it does not use the hash table in determining whether to include a particular itemset into the candidate itemsets.

2.4 Transaction Reduction Algorithm:

The classical Apriori algorithm generates a large number of candidate sets if the database is large. And due to large number of records in database results in much more I/O cost. In this project, we proposed an optimized method for Apriori algorithm which reduces the size of the database. In our proposed method, we introduced an attribute Size_Of_Transaction (SOT) , containing a number of items in individual transaction in the database. The deletion process of transaction in database will made according to the value of K. Whatever the value of K, the algorithm searches the same value for SOT of the database. If the value of K matches with a value of SOT then delete only those transactions from the database.

3. PROPOSED SYSTEM

3.1 Improved Apriori Algorithm

Our Improved Apriori algorithm which uses the data structure which represents the hash table. This algorithm proposes to overcome the weakness of Apriori by reducing the candidate sets. The proposed algorithm does a three stage process where the first process is a hash based step is used to reduce the candidate itemsets generated in the first phase. We assure that the number of itemset generated using hashing can be reduced. In this algorithm each transaction counts all the itemset at the same time possible 2-itemsets in the current transactions are hashed to a hash map. After the 2-itemset the individual items which has less frequent are deleted from the transaction database and the final step is the construction of a tree where we apply a divide and conquer strategy for mining the frequent itemsets from the transaction database. And in this process the frequent itemsets are listed in descending order. A root of the tree is constructed first and then the branches are added according to the count of the itemset. Once the tree is constructed the frequent itemsets are minined by traversing through the tree. Since the construction of the tree is made simple as by reducing the items from the transaction database.

The algorithm is as follows

Input: The Transaction database and the minimum support.
Output: All the frequent itemsets in the transaction database.
The following is the description of the algorithm

1. The transaction database is scanned and create a possible 2-itemsets.
2. Let the Hash table of size 8.
3. For each bucket assign a candidate pair using the ASCII values of the item sets.
4. Each bucket in the hash table has a count, which is increased by 1 each item an item set is hashed to that bucket.
5. If the bucket count is equal or above the minimum support count, the bit vector is set to 1. Otherwise it is set to 0.
6. The candidate pairs that hash to locations where the bit vector bit is not set are removed.
7. Modify the transaction database to include only these candidate pairs
8. Then the candidate itemsets which has less frequent are then removed from the transaction database.
9. And the database is scanned for minimum support threshold, frequent items are selected and sorted.
10. Initialization of the FP-tree is done. From the frequent items a node list is created which will be connected to nodes of the tree. After initialization the database is read again. This time, if an item in a transaction is selected as frequent then it is added to the tree structure.
11. Beginning of the least frequent item, a frequent pattern finder procedure is called recursively. The support count of the patterns is found and displayed if they are frequent.
12. End.

Table 1. Transaction Database

TID	ITEMS
T1	I1, I3, I7
T2	I2, I3, I7
T3	I1, I2, I3
T4	I2, I3
T5	I2, I3, I4, I5
T6	I2, I3
T7	I1, I2, I3, I4, I6
T8	I2, I3, I4, I6
T9	I1
T10	I1, I3

Table 2.Hash Table Data Format

TID	ITEM SET
T1	I1I3, I1I7, I3I7
T2	I2I3, I2I7, I3I7
T3	I1I2, I1I3, I2I3
T4	I2I3
T5	I2I3,I2I4,I2I5,I3I4,I3I5,I4I5
T6	I2I3
T7	I1I2,I1I3,I1I4,I1I6,I2I3,I2I4,I2I6,I3I4,I3I6,I4I6
T8	I2I3,I2I4,I2I6,I3I4,I3I6,I4I6
T9	I1
T10	I1I3

HASH COUNT:

{I1I3}=4,{I1I7}=1,{I3I7}=2,{I2I3}=7,
{I2I7}=1,{I3I7}=2,{I1I2}=2,{I1I3}=3,
{I2I4}=3,{I2I5}=1,{I3I4}=3{I3I5}=1,
{I4I5}=1,{I1I4}=1,{I1I6}=1,
{I2I6}=2,{I3I6}=2,{I4I6}=2.

MINIMUM SUPPORT=3 ,

FREQUENT ITEM SET {I1I3, I2I3, I3I4},
FREQUENT ITEM SET= {I1, I2, I3, I4}

Table 3. Transaction Reduction Table

TID	ITEMS
T1	I1, I3
T2	I2, I3
T3	I1,I2,I3
T4	I2,I3
T5	I2,I3
T6	I2,I3
T7	I1,I2,I3,I4
T8	I2,I3,I4
T9	I1
T10	I1,I3

Table 4. Maximum Item Set Count

ITEMS	COUNT
I3	8
I2	7
I1	5
I4	3

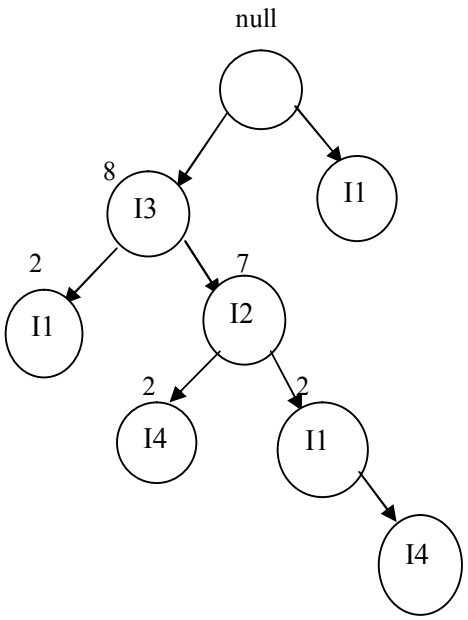


Figure 1. Tree Structure

3. EXPERIMENTAL RESULTS

In this section we have taken the market basket analysis and compare the efficiency of the proposed method to the existing algorithms which is mentioned above. All these algorithms are coded using the eclipse IDE which uses JAVA programming language. The data sets have been generated for testing these algorithms.

Two case studies have been done in analyzing the algorithm

i) the execution time of the algorithm is tested to the number of transactions,

ii) The execution time is executed to the number of the support.

Case i:

In this case where we are comparing the execution time of the transaction where any transaction may a contain more than one frequent itemsets. Here the minimum support is made constant. Here we assume the minimum support is being 40% and the comparison table is shown below.

Table:6 Execution Time based on Transactions

Transactions	Exec Hash Apriori	Transaction Reduction	Exec Apriori	Improved Apriori
1000	0.326	0.986	1.247	0.238
750	0.275	0.731	1.136	0.19
500	0.186	0.051	1.041	0.13
300	0.165	0.192	0.961	0.05

Case ii:

Now the execution time of different algorithms is compared by varying the minimum support. The comparison table is shown below.

Table:7 Execution Time Based on Support

Support %	Exec Hash Apriori	Exec Apriori	Transaction reduction	Improved Apriori
70	0.065	0.146	0.056	0.04
60	0.066	0.151	0.06	0.045
50	0.061	0.301	0.096	0.055
40	0.165	0.406	0.205	0.135

4. CONCLUSION

In this paper a new algorithm has been proposed for association rule mining for finding the frequent itemsets.

The present apriori algorithm has some bottlenecks we need to optimize and the proposed algorithm will give a new way for association rule where it reduces the candidate item sets. And we have also done some case studies about the existing algorithm above and we also listed the demerits of the existing systems and our proposed work is assured to overcome these bottlenecks we mainly concentrated to reduce the candidate itemset generation and also to increase the execution time of the process.

5. REFERENCES

[1] J. S. Park, M.S. Chen, and P.S. Yu. “An Effective Hash Based Algorithm for Mining Association Rules”. Proceedings of the 1995 ACM SIGMOD International Conference on Management of Data, San Jose, CA, USA, 1995, 175186.

[2] R. Agrawal and R. Srikant, “Fast Algorithms for Mining Association Rules in Large Databases,” Prof. 20th Int’l Conf. Very Large Data Bases, pp. 478499, 1994.

[3] A. Savasere, E. Omiecinski, and S. Navathe. “An Efficient Algorithm for Mining Association Rules in Large Databases”. Proceedings of 21th International Conference on Very Large Data Bases (VLDB’95), September 1115, 1995, Zurich, Switzerland, Morgan Kaufmann, 1995, 432444.

[4] J. Han and J Pei, “Mining frequent patterns by pattern growth: methodology and implications”. ACM SIGKDD Explorations Newsletter 2, 2, 1420. 2000.

[5] G. PiatetskyShapiro. “Discovery, analysis, and presentation of strong rules. Knowledge Discovery in Databases”, 1991: p. 229248.

[6] Barış Yıldız, Belgin Ergenç. “Comparison Of Two Association Rule Mining Algorithms Without Candidate Generation”, In IASTED International Conference on Artifical Intelligence and Applications (AIA 2010), Austria, Feb 15-17, 2010.

[7] Jiawei Han, Hong Cheng, Dong Xin, Xifeng Yan, “Frequent pattern mining: current status and future directions”, In the Journal of Data Min Knowl Disc (2007) 15:55–86,Springer Science+ Business Media, LLC 2007.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 170 - 175, 2013, ISSN: 2319–8656

Advanced Authentication Scheme using Multimodal Biometric Scheme

Shreya Mohan
Karunya University
Coimbatore, India

Ephin M
Karunya University
Coimbatore, India

Abstract: Fingerprint recognition has attracted various researchers and achieved great success. But, fingerprint alone may not be able to meet the increasing demand of high accuracy in today's biometric system. The purpose of our paper is to inspect whether the integration of palmprint and fingerprint biometric can achieve performance that may not be possible using a single biometric technology. Pre-processing is done for fingerprint and palmprint images separately in order to remove any noise. The next step is feature extraction. Minutiae algorithm is used for fingerprint feature extraction and Local Binary pattern for palmprint. Wavelet fusion is applied in order to fuse the extracted features and Support Vector Machine is used for matching. The main highlight of the project is multimodal biometrics which will give a better security and accuracy comparing to unimodel system.

Keywords: fingerprint; palmprint; multimodal biometrics; minutiae; Local Binary Pattern.

1. INTRODUCTION

All The rapid growth in the use of Internet applications and the great concern of security require reliable and automatic personal identification. Traditional automatic personal identification schemes can be divided into two categories: knowledge-based approach, such as a password and token-based approach, such as an ID card, physical key and a passport. However, these approaches have limitations. In the knowledge-based approach, there are chances that, the "knowledge" can be guessed, forgotten or shared. In the token-based approach, there are chances that the "token" can be stolen or lost. These figures strongly indicate that we need a more effective and reliable solution for human identity management. Biometrics is regarded as the potential solution.

Biometric authentication refers to the technology for personal identification or authentication based on our physiological and/or behavioural characteristics. Biometrics is mainly concerned with 'what you are' rather than 'what you carry'. Biometrics is mainly used in computer science as a form of identification and access control. Biometrics is very essential in today's world in order to protect sensitive areas where public interaction is more, like railway stations and airports. Applications of biometrics can be found in many areas including electronic commerce, electronic banking and many security applications. Various methods are available and are based on different personal characteristics. Human characteristics proposed as biometric traits have both advantages and disadvantages. The selection of biometric traits depends on requirements of applications. Retina, hand geometry, iris, voice, fingerprint, face are some of the commonly used biometric traits.

Existing biometric modalities including palmprint, fingerprint, face, voice, signature etc. is now widely used in many security applications. Each one has its individual merits and demerits. Five objectives, cost, accuracy, user acceptance and environment constraints, computation speed and security should be considered when designing a biometric system. Each of the above parameters are inter-related. Reducing accuracy can increase speed. Reducing user acceptance can improve accuracy. Increasing cost can enhance security. A practical biometric system should balance all the five objectives.

Based on the literature survey, the hand-based biometric acquisition has many advantages. It has higher user acceptance and is more user friendly. The fingerprint, face, iris, palmprint modalities have been highly explored, and are nowadays available in real-world practice. Among the hand based biometric system, fingerprint identification is the oldest and the most popular one. It is the method of identification using the impressions made by the minute ridge formats or patterns found on the fingertips. The ridge patterns will be different throughout the life for every individual. Fingerprints will offer an infallible means of personal authentication. Other personal characteristics may change, but fingerprints do not. A lot of study has been carried on based on iris, finger, face etc. But the developments under palmprint is comparatively less. The inner surface of the palm normally contains distinct features like principle lines, wrinkles and ridges. The principle lines and wrinkles are formed between the third and fifth months of pregnancy and superficial lines appear after we born. Even identical twins have different palm prints. Fingerprint is a popular biometric identification technology and studies are still going on in the palmprint identification. In order to increase the performance of the automated system, it is advisable to go for multimodal biometrics. A biometric system which uses information from different biometrics is termed as multimodel biometrics. Eg: fingerprint and palmprint, iris, palmprint and face etc. Multimodal biometric techniques have attracted much attention as the add-on information between different modalities could improve the recognition performance.

A typical multimodal biometric authentication system consists of five parts. Image capture, pre-processing, feature extraction, fusion and matching. Special biometric scanners are used for image capturing. It may vary depending on the type of biometric traits used [1,2]. At the pre-processing stage the image is enhanced to remove noise and unwanted areas. Feature extraction gets effective features from the pre-processed biometric trait. Feature extraction for palmprint and fingerprint are different. After feature extraction fusion is carried out to combine different features and stored in the database as templates. A matching algorithm is used to compare it with the stored one in the database. Fig 1 gives the

basic block diagram of a biometric system. Attention should have to be paid in the security of biometric trait also.

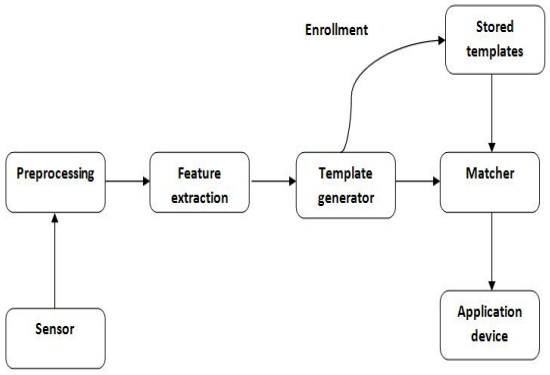


Figure 1. Basic Biometric System

Before performing multi-biometrics based on palmprint and fingerprint, it is important to understand the background for mono-modal biometrics. Various studies have shown how the palmprint and fingerprint are viable biometric features. Due to the availability of different features, different methods of evaluation, and different methods of combining the evaluations, here we will analysis some commonly available biometric methods.

2. RELATED WORKS

One of the initial step called pre-processing is carried out for palm print and fingerprint separately. After the image is captured by the scanner it may be distorted or blurred due to the bad environmental conditions. In these conditions a good pre-processing method is a must. Low pass filters like Gaussian can be used for smoothening. In [32] in addition to Gaussian filter, Short Time Fourier Transform (STFT) analysis is adopted to enhance fingerprint image quality. Sometimes the binarized fingerprint image contains a number of false minutiae. In [27] a detailed pre-processing is mentioned to remove false minutiae has been described.

For palmprint images, the central part, called the Region of Interest should have to be extracted. For extracting the central part, a coordination system should have to be established. There are several implementations including tangent [1], bisector [6,7] and finger based [8,9] to detect the key points between fingers.

After computing the coordinate systems, the central parts of palmprints, which is called the Region of Interest (ROI) are segmented. In most of the pre-processing algorithms, ROI will have square shape but some of them will have circular [10] and half elliptical shapes [11].

For extracting the features from the fingerprint image, a popular method is minutiae extraction. A fingerprint is made of a series of ridges and furrows on the surface of the finger. Minutiae extraction algorithm will find out the minute points from the fingerprint and then map their relative placement on the finger. When the fingerprint is of low quality, it will be difficult to extract the minutiae points. For that only we are using different filters and other image enhancement techniques at the pre-processing stage. The output of this algorithm will be the image template containing the minutiae details. There are two types of minutiae points. Ridge ending and Ridge bifurcation[4]. In [26] an advanced fingerprint feature extraction method is introduced through which minutiae are extracted directly from original gray-level fingerprint images without binarization and thinning. Gabor filter bank can also be used to extract features from fingerprint [24].

Comparing to fingerprint, palmprint contains more features. So a good method should be applied in order to extract all the features. The feature extraction methods can be divided into three types. Line based approach, Subspace based approach and Statistical approach. In line based approaches, they use existing edge detection methods to extract palm lines[12]. Subspace-based approaches also called appearance-based approach. They use Principal Component Analysis (PCA) [20,16], Linear Discriminant Analysis (LDA) [25] and Independent Component Analysis (ICA) [28]. Paper [21] proposes Matrix-based Complex PCA (MCPCA), that uses a complex matrix to denote two biometric traits from one subject.

Statistical approaches are two types. Local and global statistical approach. Local statistical approaches transform images into another domain and then divide the transformed images into several small regions[13,14]. Gabor, wavelets and Fourier transforms have been applied. Global statistical approaches [15] compute global statistical features directly from the whole transformed images. Moments, center of gravity and density have been regarded as the global statistical features. An advanced technique called Local Binary Pattern can also be used [3] to for palmprint feature extraction.

At the earlier stages researchers used only filters to extract features from palm. In [5] palmprint is considered as a piece of texture and 2-D Gabor filter is used to extract the features. This is called texture based feature extraction. The main disadvantage of this method is that filters cannot extract all the features.

The important aspect in multimodal biometric is the fusion or the combination of modalities. Many biometric traits including fingerprint and palmprint[17],face, palmprint and fingerprint[18], fingerprint, iris and face[19] have been used. But fusion of palmprint and fingerprint will give better result comparing to others. There are four levels of information fusion. Feature level fusion [17], score level fusion [32], pixel level fusion, and decision level fusion. Fusion increases accuracy, but it generally increases template sizes, computation costs and reduces user acceptance.

The task of matching is to calculate the degree of similarity between the input test image and a training image from database. Matching can be carried out in three ways: hierarchical approach [19], classification and coding. KNN classifier [17], nearest neighbour classifier (1-NN) based on the Euclidean space [31] are some of the commonly used classification approach.

Multimodal biometric systems have better accuracy and reliability. But sufficient attention has not been paid to security of multibiometric template. They are vulnerable to attacks including reply, database and brute-force attacks [23]. All the information that is generated by the scanners are stored as templates in the database. So leakage of biometric template information to unauthorized individuals constitutes a serious security issue. Therefore multibiometric template

protection [22] should be carried out for security and privacy issues.

This paper mainly discusses the fusion of palmprint and fingerprint biometrics. However, the algorithm and analysis presented here can also be applied to other multimodal biometric fusion applications. Here Figure 1 illustrates a typical multimodal biometric authentication system. It consists of three main blocks that of pre-processing feature extraction and fusion. Bellow steps give a brief summary about the different steps involved in the proposed system.

1. Input image palmprint and finger print is given.

2. Selected features such as line, texture for palmprint and line and minutiae for fingerprint.

3. The features are merged by wavelet data fusion.

4. Support Vector Machine algorithm is used for classification of the image.

3. PROPOSED DESIGN

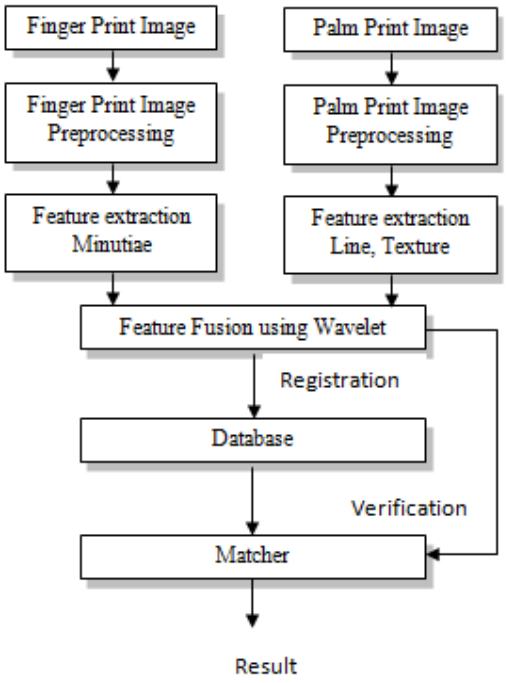


Figure 2. Proposed Multimodal Biometric System

Figure 2 shows the basic block diagram of the proposed method. Proposed system for multimodal biometric focuses on the feature level fusion. This methodology has the benefit of exploiting more amount of information from each biometric. Above figure comprises of pre-processing, feature extraction, fusion and matching. Pre-processing is used to remove the unwanted data in the input image. Feature extraction is done using Minutiae extraction for fingerprint and Local Binary Pattern for palmprint. Fusion is done using the Wavelet Fusion method. Fused images are stored in the database at the enrollment stage. Above steps are again done for palmprint and fingerprint images at the authentication stage. The features are then compared with the templates of the database to produce the output. Matching is done using the SVM. Combining more than one biometric system improves accuracy and reduces error rates. The proposed multimodal biometric system overcomes the limitations of individual biometric systems and also meets the accuracy requirements. Following sections will the details of the steps involved in the proposed system.

3.1. Pre-processing

The images must be pre-processed before going for next stage. Image pre-processing is done with the intention of removing unwanted data in the image such as noise, reflections etc.

All the images should have to be normalised in order to make it a single image size. This is the first stage of pre-processing.

Low pass filter is applied for both palmprint and fingerprint images to enhance the image. Electronic filter that pass low frequency signals but attenuates signals with frequency higher than the cut-off frequency is called low pass filter.

The next step is thresholding. Thresholding is used for binarization of images. Threshold Tp is used to convert

original image into binary image. Mathematically this transformation can be represented as

$$B(x,y) = 1 \quad \text{if } O(x,y)*L(x,y) >= Tp \qquad (1)$$

$$B(x,y) = 0 \quad \text{if } O(x,y)*L(x,y) < Tp \qquad (2)$$

Where B(x,y) and O(x,y) are the binary images and the original image respectively. L(x,y) represents a lowpass filter such as Gaussian and * represents an operator of convolution.

3.2. Minutiae Extraction

For extracting the features from the fingerprint image, minutiae extraction algorithm is used. The output of this algorithm will be the image template containing the minutiae details. There are two types of minutiae points. Ridge ending and Ridge bifurcation. A brief description of minutiae extraction algorithm is given bellow.

1) Consider the input image.

2) Scan the image from left to right, top to bottom order by following only ridges

3) Find the 0-1 transition ,calculate the width of the ridge by noting the 1-0 transition.

4) Move to the next row and follow the same ridge. Note the width.

5) If the width >=width in previous row there may be a top to bottom bifurcation. Then call the bifurcation function to check if it is a minutiae point.

Else

If the width =< width in previous row there may be a bottom to top ridge bifurcation. Then call the bifurcation function to check if it is a minutiae point.

6) Continue with the next row and repeat this for all the ridges in the given image or until 90 minutiae points have been obtained.

3.3. Local Binary Pattern

Unlike fingerprint which flows in uniform structure with alternating ridges and furrows, the texture of palmprint is irregular and the lines and ridges can flow in various directions. LBP is then used to analyse and describe the texture of the palmprint. The LBP operator is a simple but powerful texture descriptor that has been used in various applications. High discrimination ability and simplicity in computation have made it very suitable for palmprint feature extraction. LBP operator labels every pixel in an image by thresholding its neighboring pixels with the center value Bellow figure illustrates an example how the binary label for a pixel value is obtained.

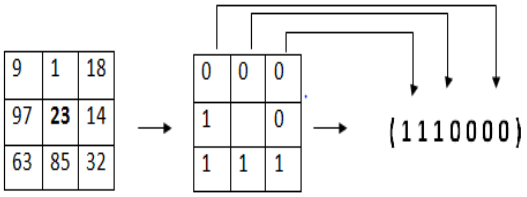


Figure 3. Local Binary Pattern

It is found that certain fundamental patterns in the bit string account for most of the information in the texture. These fundamental patterns are termed as “uniform” patterns and they are bit strings with at most 2 bitwise transitions from 0 to 1 and vice versa. Examples of uniform patterns include 00000000, 11110000, 00001100. A label is given to each of the uniform patterns and the other “non-uniform” patterns are assigned to a single label. The next step is calculating the histogram of the labels.

3.4. Wavelet fusion

To fuse two images using wavelet fusion the two images should be of the same size and should be associated with the same color. Here we use wavelet data fusion to fuse the features of both palmprint and fingerprint.

3.5. Support Vector Machine

Support Vector Machine is a powerful learning tool based on statistical learning theory. An SVM is a binary classifier that makes its decision by constructing a linear decision boundary or hyper plane that optimally separate data points of the two classes in feature hyperspace [29] and also makes the margin maximized. SVMs have many advantages over Neural Networks. ANN are prone to the danger of over training [30] resulting in a solution over-fitted to the database being worked on. This could lead to overly optimistic results and accuracy outcomes. Secondly it has been found that SVMs are comparatively faster to train than ANNs.

4. Results and Experimentations

The effectiveness of our proposed multimodal biometric authentication scheme is evaluated on the palmprint and fingerprint database. The experiments are conducted in MATLAB with image processing Toolbox and on a machine with an Intel core 2 Duo CPU Processor. Bellow figures shows some experimental results. Fig. 4(a) is the original input image. Binarization should have to be done before thinning. Fig. 4(c) shows the thinned image. Minutiae points are marked in 4(d). The two points, ridge ending and ridge bifurcations are differentiated with two colors. Fig. 4(e) is the original palmprint image. Region of Interest is taken from the palm image and that is given as input. Local Binary Pattern is used to extract the features. Fig 5(g) explains the fused image using palmprint and fingerprint line image.

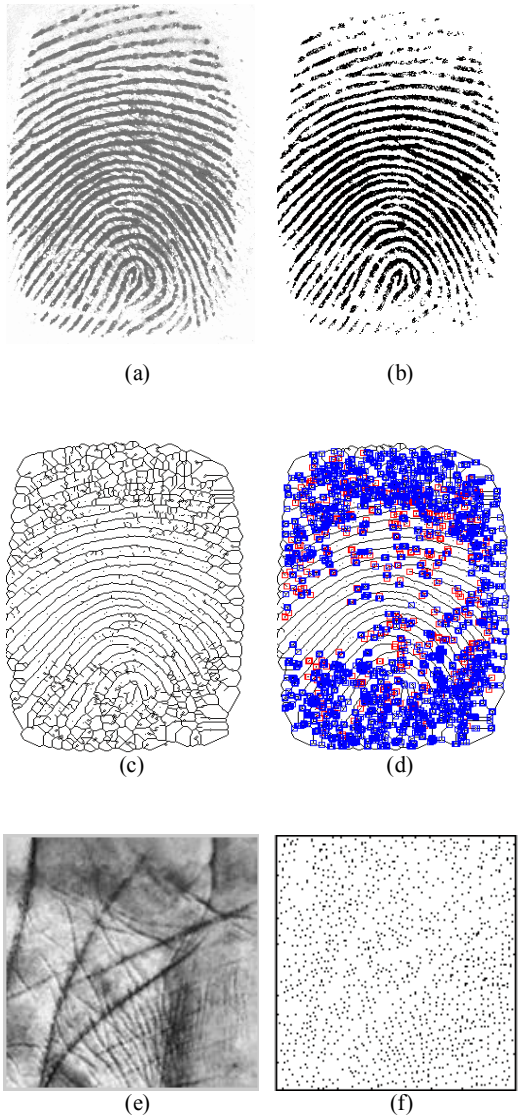
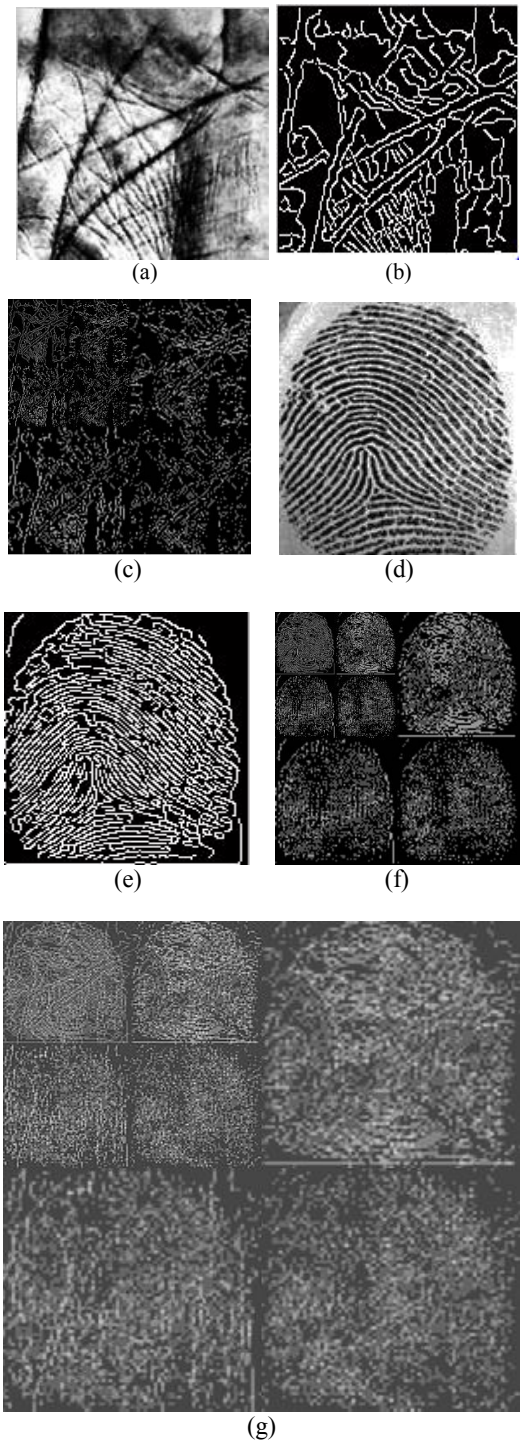


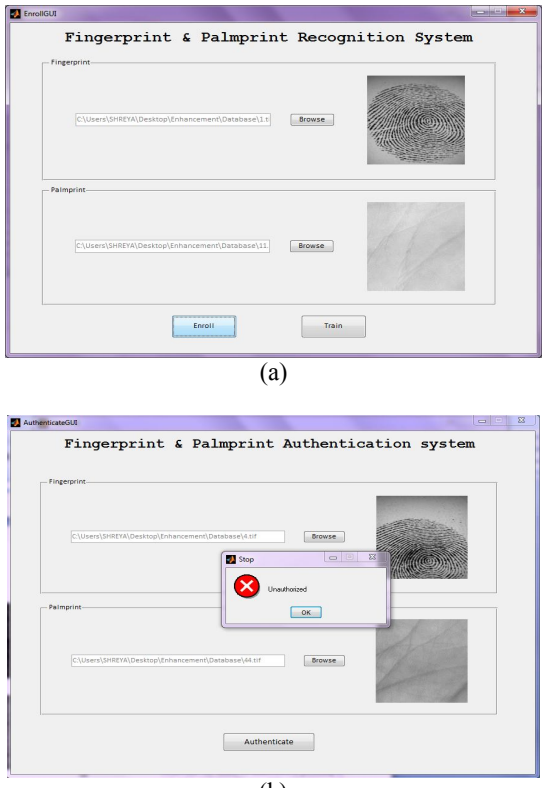
Figure 4. Feature Extraction : (a) Fingerprint image, (b) Binary image, (c) Thinned image, (d) Minutiae extraction, (e) Palmprint image, (f) Feature extraction using Local Binary Pattern.



(a) (b) (c) (d) (e) (f) (g)

Figure 5. Feature Fusion : (a) Palmprint image, (b) Palmprint line detection, (c) Decomposition of palmprint image, (d) Fingerprint image, (e) Fingerprint line detection, (f) Decomposition of fingerprint image, (g) Fused image.

Fig. 6 shows the authentication part. Fig 6(a) shows the actual interface to select the images for the enrollment stage. After the enrollment we can choose images for autherisation(Fig 6(b)).



(a) (b)

Figure 6. Authentication : (a) Enrollment stage, (b) Authentication stage.

5. CONCLUSION

We often face problems due to the fact that there exists only a single sample for personal identification in practice. The biometrics fusion technology is considered to be an effective solution to improve the performances of single sample biometrics systems. Meanwhile, the fusion of hand-based is promising in real world application because of the convenience and acceptance of the public. We have presented a feature level fusion scheme for palmprint and finger print verification and identification system using the combination of three palmprint representations. The extracted features from fingerprint and palmprint are fused using a wavelet based feature fusion technique. The combination of minutiae, line and Local Binary Pattern outperforms than using them individually.

6. REFERENCES

[1] D. Zhang, W.K. Kong, J. You, M. Wong. “On-line palmprint identification”, In Proceedings of IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 1041–1050.

[2] C.C. Han. “A hand-based personal authentication using a coarse-to-fine strategy”, Image and Vision Computing, 2004, 909–918.

[3] Hanmandlu, M., Gureja and Jain, A. “Palm print recognition using Local Binary Pattern operator and support vector machines”. Signal and Image Processing

[4] (ICSIP), 2010 International Conference on (pp. 158-162). IEEE.

[5] Deshpande, A., S., Patil, S., M., Lathi, R. "A Multimodel Biometric Recognition System based on Fusion of Palmprint Fingerprint and Face". International Journal of Electronics and Computer Science Engineering. ISSN-2277-1956.

[6] Kong, W. K., Zhang, D., Li, W. "Palmprint feature extraction using 2-D Gabor filters". Pattern recognition, 36(10), 2003, 2339-2347.

[7] W. Li, D. Zhang, Z. Xu. "Palmprint identification by Fourier transform". International Journal of Pattern Recognition and Artificial Intelligence, 2002, 417–432.

[8] X. Wu, K. Wang, D. Zhang. "HMMs based palmprint identification". Lecture Notes in Computer Science. Springer, vol. 3072, 2004. pp. 775–781.

[9] Han, C., C. "A hand-based personal authentication using a coarse-to-fine strategy". Image and Vision Computing 22 (11), 2004, 909–918.

[10] Han, C. C., Cheng, H. L., Lin, C. L., Fan, K. C. "Personal authentication using palm-print features". Pattern Recognition, 36(2),2003, 371-381.

[11] Kumar, A., Zhang, D. "Integrating shape and texture for hand verification". International Journal of Image and Graphics, 6(01), 2006,101-113.

[12] Poon, C., Wong, D. C. M., & Shen, H. C. "A new method in locating and segmenting palmprint into region-of-interest". In Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on (Vol. 4, pp. 533-536). IEEE.

[13] Wu, X., Wang, K., Zhang, D. "Line feature extraction and matching in palmprint". In Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series (Vol. 4875, pp. 583-590).

[14] Han, C. C., Cheng, H. L., Lin, C. L., & Fan, K. C. "Personal authentication using palm-print features". Pattern Recognition, 2003, 36(2), 371-381.

[15] You, J., Kong, W. K., Zhang, D., & Cheung, K. H. "On hierarchical palmprint coding with multiple features for personal identification in large databases". Circuits and Systems for Video Technology, IEEE Transactions on,14(2), 2004, 234-243.

[16] Pang, Y. H., Connie, T., Jin, A., & Ling, D. "Palmprint authentication with Zernike moment invariants". In Signal Processing and Information Technology, 2003. ISSPIT 2003. Proceedings of the 3rd IEEE International Symposium on (pp. 199-202). IEEE.

[17] Albert, T., A. Ganesan, S. "Application of Principal Component Analysis in Multimodel Biometric Fusion System". European Journal of scientific research, 2012, Vol 67, No. 2.

[18] Gayathri, R. Ramamoorthy, P. "Fingerprint and palmprint Recognition Approach based on Multiple Feature extraction". European Journal of scientific research, 2012, Vol 76, No 4.

[19] Deshpande, A., S., Patil, S., M., Lathi, R. "A Multimodel Biometric Recognition System based on Fusion of Palmprint Fingerprint and Face". International Journal of Electronics and Computer Science Engineering, 2012, ISSN-2277-1956.

[20] J. You, W.K. Kong, D. Zhang, K.H. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases", IEEE Transactions on Circuits and Systems for Video Technology 14 (2) ,2004, 234–243.

[21] Joshitha N., J. Medona S., R. "Image Fusion using PCA in Mutifeature Based Palmprint Recognition". International Journal of soft computing and Engineering, 2012, ISSN:2231-2307,Volume-2,Issue-2.

[22] Xu, Y., Zhang, D., & Yang, J. Y. "A feature extraction method for use with bimodal biometrics". Pattern recognition, 43(3), 2010, 1106-1115.

[23] Nagar, A., Nandakumar, K., & Jain, A. K. "Multibiometric Cryptosystems Based on Feature-Level Fusion". Information Forensics and Security, IEEE Transactions on, 7(1), 2012, 255-268.

[24] Ratha, N. K., Connell, J. H., Bolle, R. M. "Biometrics break-ins and band-aids". Pattern Recognition Letters, 24(13), 2003, 2105-2113.

[25] Jain, A. K., Prabhakar, S., Hong, L. "A multichannel approach to fingerprint classification". Pattern Analysis and Machine Intelligence, IEEE Transactions on, 21(4), 1999, 348-359.

[26] Cui, J., Xu, Y. "Three dimensional palmprint recognition using linear discriminant analysis method". In Innovations in Bio-inspired Computing and Applications (IBICA), 2011 Second International Conference on. IEEE.

[27] Zhao, F., Tang, X. "Preprocessing and post-processing for skeleton-based fingerprint minutiae extraction". Pattern Recognition, 40(4), 2007, 1270-1281.

[28] Zhao, F., Tang, X. "Preprocessing and post processing for skeleton-based fingerprint minutiae extraction". Pattern Recognition 40, 2007, 1270 – 1281.

[29] Zhao, F., Tang, X. "Preprocessing and post processing for skeleton-based fingerprint minutiae extraction". Pattern Recognition 40, 2007, 1270 – 1281.

[30] Vapnik, V. "The nature of statistical learning theory". Springer-Verlag, Berlin, 1995.

[31] Bernhard Schölkopf and Alex Smola, "Learning with Kernels" (MIT Press, Cambridge, MA, 2002).

[32] Zhang, Y., Sun, D., Qiu, Z. "Hand-based feature level fusion for single sample biometrics recognition". In Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB), 2010 International Workshop on (pp. 1-4). IEEE.

[33] Kumar, A., Zhang, D. "Combining fingerprint, palmprint and hand-shape for user authentication". In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on (Vol. 4, pp. 549-552). IEEE.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 176 - 179, 2013, ISSN: 2319–8656

Spatial Keyword Ranking (SKR) based Dominated Location with Safe Zone

Krishna Balan
Pondicherry Engineering College
Pondicherry, India

Karthiga
Pondicherry Engineering College
Pondicherry, India

Sakthi Priya
Pondicherry Engineering College
Pondicherry, India

Abstract: Generally, spatial objects (e.g., Hotels) not only have spatial locations but also have quality attributes (e.g., star, price etc). In wild animal rehabilitation, an appropriate location is selected from a set of options for returning an animal to the nature, after its treatment in a rehabilitation center. A location is preferred if it is far away from (competing) animals with multiple better abilities (e.g., speed, weight, age). Since those animals are much stronger in fighting for essential resources, e.g., water and food, they will endanger the rehabilitated animal that is still unaccustomed to wildlife. By maximizing the distances to potential nearest dominators (NDs), the preferred location improves the survival chance of the rehabilitated animal in the nature. Hence the safe zone is created to retrieve result within the region. If the query moves from the safe zone another safe zone is created fot that query, the intersected part are purned. These reduce the database storage.

Keywords: Anonymizer; Database Management; Safe zone; Spatial Database; Spatial Objects;

1. INTRODUCTION

In reality, spatial objects (e.g., hotels) not only have spatial locations but also have quality attributes (e.g., star, price). An object p is said to dominate another one p_0, if p is no worse than p_0 with respect to every quality attribute and p is better on at least one quality attribute. Traditional spatial queries (e.g., nearest neighbor, closest pair) ignore quality attributes, whereas conventional dominance-based queries (e.g., skyline) neglect spatial locations. From this Farthest Dominated Location (FDL) [1] retrieves the results, includes both quality attributes, and spatial objects with sufficient R-Tree algorithm to retrieve the data. For each query, Location based Server (LBS) need to analyze the query objects and the query location. Then LBS search its entire database to give respective queries result. This process is effective for static object. If it is for dynamic object means the server sends the result for one location point that is not sufficient if the object moves to another location. For this, the proposed system include safe zone. This zone creates a circular zone with range for the query, and location will be analyzed. We propose an efficient index called Spatial Keyword Ranking (SKR) Tree data structure which performs 1) Spatial filtering, 2) Textual filtering and 3) Object ranking in a fully integrated manner.

2. RELATED WORKS

Terminal devices, which are the monitored moving objects, obtain their own location information from the GPS system and transmit it to the server via a wireless communication network. The whole system's timeliness and efficiency is affected by the wireless communication bandwidth. The location information updates are often the bottleneck because of the limited wireless bandwidth and the high sampling rate in the traditional uniform time/distance interval strategies.The idea behind the rectangular safe region (RSR) algorithm is to define a rectangular safe region for every object according to the registered query and the latest location obtained. As long as the object's motions do not exceed its safe region, all the query result sets of the object remain unchanged.

The terminal device is informed of the safe region assignments dynamically. Hence when a terminal device finds that it has exceeded the safe region, it will report its new location information.

2.1 Naive Iterative Incremental (NII) NN Search

Naive Iterative Incremental NN (nearest neighbour) search is for processing the FDL query. NII takes as input 1) a two dimensional R-tree Rp on the spatial object set P, 2) a set of locations L, and 3) a c-dimensional design competence [4]. It examines each location s of set L and computes the nearest dominator of s, by performing the incremental nearest neighbour search [3] of s on the tree Rp.

During the iterative search, the largest ndd (nearest dominated distance) is maintained together with the corresponding location. After all locations are examined, the maintained location is returned as the query result.

2.2 Best-First Search (BFS) Algorithm

The Best-First Search Algorithm is a basic graph-searching algorithm. Best-First makes use of a heuristic (or quickly computed estimate of the cost to reach the goal from each node), called $\hat{h}$, to guide its search. The idea behind using a heuristic to guide the search is that the algorithm will not waste time probing paths that do not seem likely to lead to the goal state (node). However, this means that an inaccurate $\hat{h}$

function can misguide the search, which can result in the search finding a path to the goal that is not optimal. For this reason, one of the greatest challenges in graph searching is to develop a heuristic function that can be quickly computed and that will be a very close estimate of the actual cost to the goal.

2.3Spatial Join Based (SJB) Algorithm

Spatial join algorithm can be classified into three categories. Assume that it have spatial join relation on R1 and R2

2.3.3 Nested Loop

In this algorithm, for each tuple of R1, entire R2 is scanned; any pair of tuples of R1 and R2 which satisfies the spatial join predicate is added to the result.

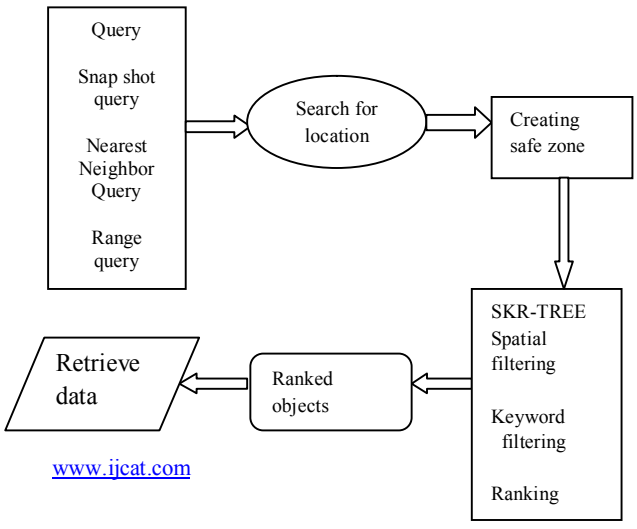
2.3.4 Tree Matching

Tree matching algorithm can be applied when indices are available on both the relations. For this discussion, it will assume that R-tree index is available. When index exists for only one relation, the index on the other relation is built on the fly and tree-matching technique is applied.

2.3.5 Partition-Based Spatial Merge Join

In this algorithm, first both of the relations are divided into *p* partitions if both of them do not fit in main memory. After that partition *i* of R1, where $1 \le i \le p$, is compared with corresponding partition *i* of R2. This strategy is very good when no indices are present on both the relation.

3. DESIGN FOR PROPOSED WORK



4. SKR TREE

We propose an efficient indexing scheme called SKR tree (Spatial Keyword Range tree),which indexes both the textual and spatial contents of objects to support data retrievals based on their combine textual and spatial relevance, which, in turn, can be adjusted with different relative weights. In fig.1 structure of SKR tree has nodes which have both spatial and non spatial information of the data object.

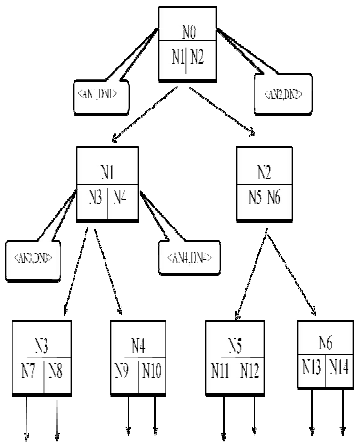


Figure 1. Structure of SKR tree

$\mathbf{N}_1$ and $\mathbf{N}_2$ are the child nodes,
$\mathbf{AN}_1$ - keyword, and $\mathbf{DN}_1$ - spatial data.

SKR Tree Construction Algorithm

Input: Set of Objects D
Output: Root of SKR tree

Procedure:
1: Ne ← 0
2: For each p ЄD do
3: geo code p and represent Lp with MBB mp
4: if for some e ЄNe, me = mp then
5: add p to e′s dataset De;
6: else
7: create a new entry e;
8: set me ← mp and De ← {p};
9: Ne ←Ne U {e};
10: End if
11: End for
12: For each e Є Ne do
13: While Ne> n max do
14: Cluster the data according to min/max into nodes
15: Ne ← Ne′
16: End while
17: End for

5. SAFE REGION BASED LOCATION UPDATES

Figure 2 demonstrates the infrastructure of a moving object query system. The kernel of the system is the control center (the main server of the system) in the center of the figure which runs the Moving Object Device (MOD) engine, collects location information, handles continues queries and provides query results to the application servers to the right of the figure. Therefore, the major computation workload is applied to the main server/control center of a MOD system. For simplicity, we refer to the main server/control center as server. Terminal devices, which are the monitored moving objects, obtain their own location information from the GPS system and transmit it to the server via a wireless communication network. The whole system's timeliness and efficiency is affected by the wireless communication bandwidth. The location information updates are often the bottleneck because of the limited wireless bandwidth and the high sampling rate in the traditional uniform time/distance interval strategies. As long as the object's motions do not exceed its safe region, all the query result sets of the object remain unchanged shown in **Figure 3**.

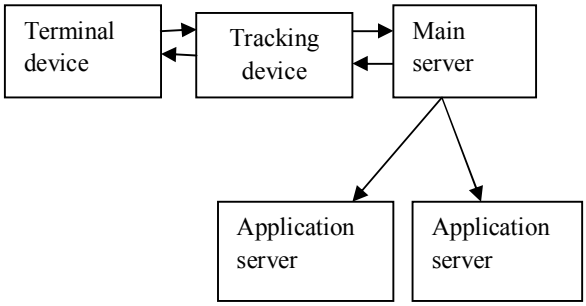


Figure 2. Infra structure of object system

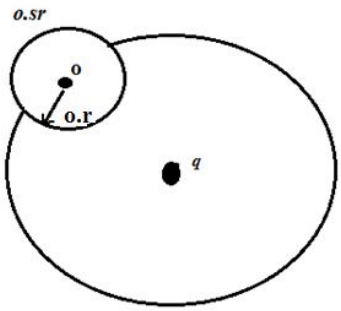


Figure 3. Location update of a moving object with circular safe region under continuous query.

The safe region of object *o* (referred to as *o.sr*) as a circle with the center at the location of the object and the radius of *o.r* (**Figure 3**). By assuming the maximum speed of the object is *o.maxspd*, then the continuous query result of query *q* will not be affected within the time interval of *o.r/o. maxspd*. Hence the server can issue a location report query to the terminal device at the time of (*o.r/o.maxspd* -δ)
where

δ is the sum of communication and computation delays.
o.r is Radius of the object safe region.
o.sr is Object safe region.
o.maxspd is Maximum speed of the moving object.

5.1 Circular Safe Region Calculation and Updates for Continuous kNN Queries

Following is the formula to update the safe region radius for the i^{th} object in the object set ascending sorted by distance to ordered kNN query q. The first object in the result set is q and the extra object o_{k+1} is kept for calculation of safe region radius of o_k.

$$oi.\mathrm{r} = \begin{cases} min\left\{oi.r, \frac{dist(oi, oi-1)}{2}, \frac{dist(oi, oi+1)}{2}\right\}, if\ o < i \le k \\ min\{oi, r, dist(oi, q) - quar(q), if\ i > k \end{cases}$$

where $quar(q)$ is the radius of the quarantine region for query q which surround and only surround the safe regions of all objects in the result set. Therefore, $quar(q) = dist(o_k, q) + o_k$.

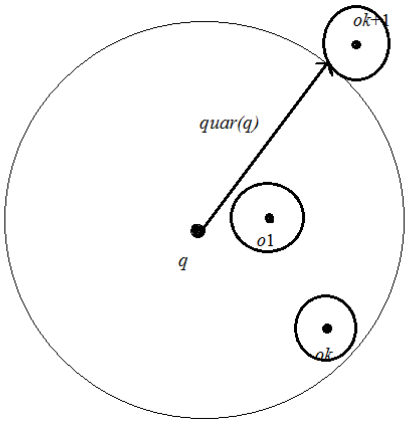


Figure 4. Quarantine region assignment for an ordered kNN query.

Figure 4 shows how such a quarantine region is assigned for such an ordered kNN query q. Hence the following property: either in or out of the kNN query result set (inside or outside the quarantine region), none of the safe regions of objects overlaps with each other. Therefore, when all the objects are moving inside their own safe regions, the result set and its order are not affected.

6. CONCLUSION

Safe zone is created to get the optimal location while comparing with farthest dominated location. Safe zone is created so as to reduce the search space and time for server because it retrieves the data within that region specified by the user. A quarantine region is also

assigned for one or more objects present in the same zone. This project proposes an efficient index SKR-tree and algorithms which perform spatial filtering, textual filtering and object ranking in a fully integrated manner is expected to have reduce the database storage and reduction of CPU time.

7. REFERENCES

[1] Hua Lu and Man Lung Yiu, "On Computing Farthest Dominated Locations", IEEE Transactions on Knowledge and Data Engineering, Vol. 23, No. 6, pp. 928-941, 2011.

[2] M.A. Cheema, L. Brankovic, X. Lin, W. Zhang, and W. Wang, "Multi-Guarded Safe Zone: An Effective Technique to Monitor Moving Circular Range Queries", Proceedings of IEEE 26th International Conference on Data Engineering (ICDE), pp. 189-200, 2010.

[3] G. Hjaltason and H. Samet, "Distance Browsing in Spatial Database", ACM Transaction on Database Systems, Vol. 24, No. 2, pp. 265-318, 1999.

[4] N. Roussopoulos, S. Kelley, and F. Vincent, "Nearest Neighbour Queries", Proceedings of ACM International Conference on Management of Data, pp. 71-79, 1995.

[5] Y. Du, D. Zhang, and T. Xia, "The Optimal-Location Query", Proceedings of International Symposium on Spatial and Temporal Databases, pp. 163-180, 2005.

[6] X. Huang and C.S. Jensen, "In-Route Skyline Querying for Location-Based Services", Proceedings international Workshop on Web and Wireless Geographical Information Systems, pp. 120-135, 2004.

[7] D. Papadias, Y. Tao, G. Fu, and B. Seeger, "An Optimal and Progressive Algorithm for Skyline Queries", Proceedings of ACM International Conference Management of Data, pp. 467-478, 2003.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 180 - 184, 2013, ISSN: 2319–8656

Survey on Service Oriented Architecture to Support the Deployment of Web Services on Sensor Nodes

Vinodhini.J
Department of CSE,
Agni College of Technology,
Chennai, India

Vasantha.R
Department of CSE,
Agni College of Technology,
Chennai, India

Dhivya.M
Department of CSE,
Agni College of Technology,
Chennai, India

W.Mercy
Department of CSE,
Agni College of Technology,
Chennai, India.

Abstract: Service Oriented Architecture (SOA) seamlessly interconnects sensors (embedded devices) inside and between four distinct domains - the business, telecommunication, automotive and home automation domain. In this paper, Simple Object Access Protocol (SOAP)-based web services are directly deployed on the sensor nodes without using any gateways in order to ensure interoperability. This approach provides easy integration with bequest IT systems and supports heterogeneity at the least level.

Keywords: Service-oriented architecture (SOA), simple object access protocol (SOAP).web services, embedded devices (sensors).

---

1. INTRODUCTION

Embedded systems are small, fast, and very great tools, gadgets and equipment which have become part of our everyday life. They monitor and control various physical parameters of the environment as well as communicate the information over the internet. Though the benefits of integrating these devices with business applications are evident, this raises a few technical issues regarding,

(i) interoperability between sensor nodes and business applications,
(ii) heterogeneity of acquired sensor data,
(iii) confidentiality

are presented in the work of Laurent *et al.* [5].

Dealing with the heterogeneity of devices and software systems requires a flexible solution that can lower the complexity and reduce the development, deployment and system maintenance expenses. Service- Oriented Architecture (SOA) has proven successful in controlling these expenses [3]. Also, research study has shown its applicability for embedded systems development [4].

Service oriented architecture (SOA) is computing paradigm that aims to build information system with services as basic units or building blocks. The architectural challenge of SOA can be described as follows.

- ability to access heterogeneous resources(data and others) and services on the web over http protocol
- ability to publish services globally
- ability to make services to discover each other and consume automatically

However, the majority of research studies have been directed towards using middleware software running on more competent devices or gateways as suggested by Wolff *et al*. in [8] or in the work of Bosman*et al*.[9]. Devices Profile for Web Services (DPWS) is implemented on these middleware software systems in order to perform following tasks

(i) Sending secure messages to and from a Web service.
(ii) Dynamically discovering a Web service.
(iii) Describing a Web service.
(iv) Subscribing to, and receiving events from, a Web service.

This approach has the advantage of leaving the resource-intensive tasks to the gateway as described in [2], but also has few drawbacks such as single point of failure, an inability to support heterogeneity on the node level [6], etc. Even though the node-level service implementations have previously been proposed, there are no studies investigating the applicability of deploying fully interoperable and compliant services, such as those described in WS-I Basic profile 1.0,directly on the sensor nodes. In this paper, we present few techniques to improve efficiency that allow us to deploy standard SOAP web services on resource constrained sensor nodes.

1.1 Problem analysis

Problem that an SOA to deeply constrained device such as sensor nodes is still an open research problem since unacceptable overhead is caused by use of Devices Profile for Web Services (DPWS) on the middleware is described by Rumen *et al.* [1]. The unacceptable overhead is due to power consumption, latency, RAM and CPU usage. The Security outline defined by DPWS enables protection of the service

executions in three directions: authentication of the parties involved, message integrity protection, and confidentiality. While the majority of the target applications will not require confidentiality for sensor data, the presented approach is only appropriate for noncritical applications where sensor nodes are behind enterprise firewall.

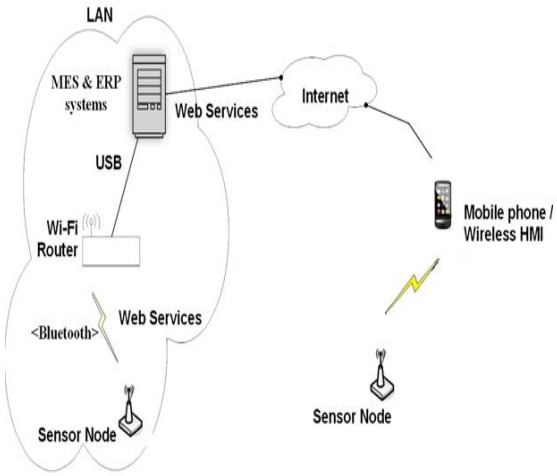


Figure.1 Sensor nodes are incorporated with enterprise systems using standard SOAP-based web services.

The remainder of this paper is organized as follows: Section II describes about the terms and technologies used. Section III summarizes about the related work. Section IV describes about the architecture that connects sensor nodes to an enterprise application. In Section V, the possible improvements and extensions to our work are discussed, and Section VII concludes this paper.

2. RELATED WORK

The analysis performed in research projects such as SOCRADES and within ITEA gives priority to SOAP based web services in which devices are integrated with the IT systems using DPWS.

The work presented by Leguay*et al*. [7] provides the translation between internal and external DPWS-compatible services was done on the gateway. The architecture supports one-to-one, but also many-to-one, relations between the services with a highly flexible eventing mechanism built upon hierarchical subscriptions.

The work presented by Rumen et al [1], usesgSOAP runtime since sensors supports embedded platforms and it includes a highly efficient runtime environment to process SOAP messages.

Another approach more closely related to our paper is that by Priyantha*et al*, at Microsoft Research [11].Instead of using specialized, ad-hoc services for node-to-node communications; they proposed to use web services described by WSDL. To keep the overhead low, these services were implemented using HTTP binding and not SOAP.

3. SOCRADES CROSS LAYER APPROACH

SOCRADES (Service-Oriented Cross-layer Infrastructure for Distributed smart Embedded devices) is a European research and innovative development project [10]. A diagram from the SOCRADES Roadmap shown in Fig.2 represents the concept of applying SOA approach for vertical inter- enterprise integration.The goal of the SOCRADES project is to create new procedures, technologies and tools for the modeling, design, execution and operation of networked hardware/software systems embedded in smart physical objects. The use of the SOA paradigm at the device level enables the adoption of a unifying technology for all levels of the enterprise, from sensors and actuators up to enterprise processes. This will lead to information being available "on demand" and allow business applications to use high-level information for such purposes as diagnostics, traceability and performance indicators resulting in increased overall equipment effectiveness and business agility.

3.1 Service-Oriented Architecture

The SOA denotes the usage of exact and self-contained function calls between distributed nodes independent of the locality and platform of the parties involved.Service Oriented Architecture is specific reference architecture that helps solve the data and functionality duplication, thus making the companies that apply this moreflexible, and operate more efficiently.

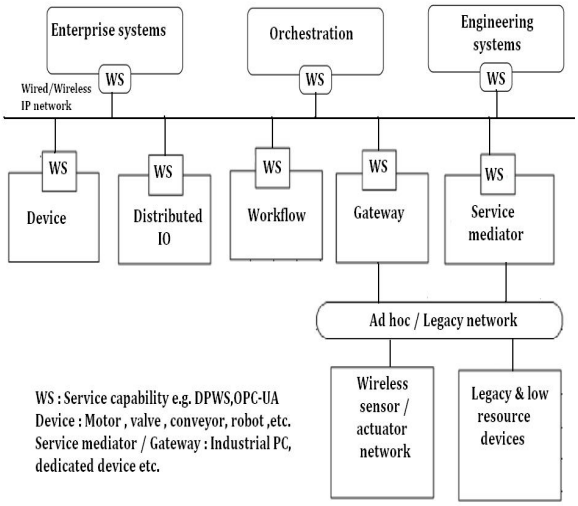


Figure. 2 The SOCRADES cross-layer approach

There are many different concrete implementations of the SOA approach: web services, CORBA, UPnP, OPC-UA, Jini etc. This paper implements SOA using SOAP-Web Services. Based on the characteristic of our target domain, the required

properties of the SOA runtime system and supporting tools are as follows:

- Written in programming language that is used for sensor and actuator nodes development-currently used are C and its dialect nesC.
- Easily portable on different embedded platforms.
- Featuring small footprint implementation.
- Highly configurable-it should be possible to remove features that are not used or needed.

3.2 Web Service

A *web service* is a network accessible interface to application functionality, built using standard Internet technologies. Web services are a messaging framework. The only requirement placed on a web service is that it must be capable of sending and receiving messages using some combination of standard Internet protocols. In general, there are two types of web services: SOAP-based web services and RESTful web services. Simple Object Access Protocol (SOAP) is a XML based messaging protocol that wraps business logic. REpresentational State Transfer (REST) is an application-specific architecture that accesses the resources or data. The web service presented in this paper is built upon SOAP.

3.3 SOAP web service

SOAP web services are designed with a common XML-based protocol. It provides a flexible way for applications to communicate, and forms the basis of SOAP. Because XML is not tied to a particular application, operating system, or programming language, XML messages can be used in all environments. The important drawback of using SOAP-web services is the need to parse verbose XML documents. However there are already a number of compression techniques that require a factor of ten less RAM, CPU, and bandwidth as compared to text-based XML. The most promising of these is Efficient XML Interchange (EXI) which is an alternative mean to represent the XML Information set that provides one-to-one translation to text-based XML representation. The work presented in this paper shows that even verbose XML can be used as a service message protocol for sensor nodes. Introducing the EXI coding to embedded service implementations however, will require the ability to change the XML parser and serializer with EXI ones.

3.4 JAX-WS

Java API for XML Web Services (JAX-WS) is a technology for developing SOAP based and Restful Java Web services. It provides a complete web services stack that eases the task of developing and deploying web services. JAX-WS supports the WS-I Basic Profile 1.1, which ensures that the web services developed using the JAX-WS stack can be consumed by any clients developed in any programming language that adheres to the WS-I Basic Profile standard. The JAX-WS API provides a great environment for writing interoperable SOAP-based Web Services and Web Service Clients. To ensure interoperability, SOAP web services are entirely based on open standards and rely heavily on the usage of XML and XML Schema Definition Language (XSD).SOAP and XML messaging is a complex domain, but JAX-WS aims to hide the complexity of that domain. JAX-WS runtime is written with the perception that the network interface it uses supports sequential execution, which requires the use of threading.

Thread-based network APIs provide abstraction of the complex event-driven nature of network communications. The tradeoff inherited from this abstraction is a high resource consumption, which makes it not suitable for highly constrained sensor nodes. So, to use the event based "raw" lwIP API, the network layer of JAX-WS runtime was rewritten and additional lwIP wrapper was introduced. This includes the splitting of the sequential execution blocks that contain blocking network operations into smaller nonblocking programming sequences connected with callback functions. As an example, consider the following simplified programming fragment that uses threaded network layer.

```
Block 1 ( ) {
        blocking connect ( );
        /* The TCP connection is established* /
        serialize_http_header ( );
        blocking send ( );
        /* The http header is sent* /
        serialize_soap ( );
        blocking send ( );
        /* The soap message is sent* /
        cleanup ( );
}
```

The equivalent functionality based on nonblockingIwIP network operations and callbacks is coded as follows.

```
Block_1 ( ) {
        store soap state ( );
        lwip_connect ( ); /*calls Block_2 ( ) when
connected*/
}
Block 2 ( ) {
        serialize http header ( );
        lwip send ( ); /*calls Block_3 ( ) when the
header is sent*/
}
Block_3 ( ) {
        serialize soap ( );
        lwip_send ( ); /*calls Block_4 ( ) when the
soap is sent*/
}
Block_4 ( ) {
        cleanup ( );
}
```

The listings also present the concept of transmission on the fly-when the HTTP header is serialized, it is sent over the network. Then, the sending buffer is released and used for storing the SOAP message before its transmission. The same technique is used on the receiving side: when the HTTP header is received it is parsed and then the receiving buffer is released. In this way, the size of the buffers, and hence the RAM usage, can be restricted.

4. PROOF-OF-CONCEPT

The technologies discussed in Section II are implemented in a proof-of-concept application that connects sensor nodes to a business application. The overall architecture is depicted in Fig. 3.The modules responsible for power management, sampling the sensors and aggregating the data are not affected by the service interface; hence, legacy code can be reused.

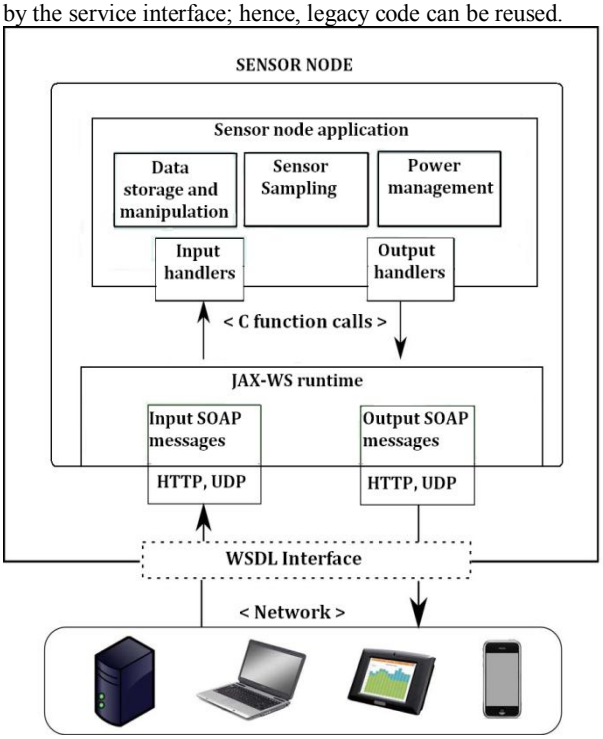


Figure.3 System architecture

Sensor data aggregation is applied for reducing the transmission time and battery life. In [7], Lee et al. used similar approach for industrial monitoring application. Instead of connecting the input and output of the sensor application to a network API implementing proprietary, specialized protocols, the data are passed to the JAX-WS runtime using handlers. In [1], Rumen et al. used similar approach using gSOAP runtime. The runtime serializes the output data to a SOAP message, and then uses lwIP to send it over a network. The interface describing the services provided by and consumed by the nodes is available through the use of standardized Web Service Description Language. This allows for so-called top-down SOA development, where the WSDL interfaces for the nodes are defined first –usually using graphical tools- and then are used to generate the SOAP runtime. At the end, the developer connects the provided interface with sensor application.

4.1Mulle Sensor Platform

The Mulle is a miniature wireless Embedded Internet System (EIS) suitable for wireless sensor networking and rapid prototyping. The Mulle platform has ultra-low power consumption and its large number of I/Os makes it ideal as a building block for wireless sensors. The Bluetooth version is capable of communicating with most Bluetooth-enabled devices, e.g. computers, PDAs and mobile phones. The use of TCP/IP enables the Mulle to transmit sensor data directly to the Internet and the small form factor allows it to be easily embedded in any product.

The nodes in the Mulle sensor were equipped with temperature and humidity sensors, and the data sent to the server consisted of multiple metrics, such as current sensor readings as well as the average, minimum, maximum, and standard deviation of the temperature and humidity for a given period, as shown in Fig. 4.

```
        <hts:GetSummary>
<Temp>
        <Current>19.3</Current>
        <Average>18.2</Average>
        <Min>17.4</Min>
        <Max>21/0</Max>
</Temp>
<Humidity>
        <Average>65</Average>
        <StdDeviation>5.0</StdDeviation>
</Humidity>
        <hts:GetSummary>
```

Figure.4 Segment of the service request initiated by the Mulle sensor node. It contains an aggregation of the sensor node for the period of interest.

Proof of concept Experiment

To test the applicability and performance of our solution, several services were implemented. In all cases the interactions between the sensor node and the PC proceeded without any compatibility problems. In this paper, we present two possible scenarios to experiment the project.

1) District Heating Scenario: In today's district heating substations, different sensors and actuators are hard-wired together. This restricts the information interchange between the communicating devices. With wireless sensor platforms integrated in such district heating devices, greater opportunities for system optimization are achieved as information can be interchanged without limitations.

With a Service-oriented architecture integrated in the sensor nodes, there is no direct need for a central control unit, as the sensor nodes are powerful enough to control the relatively slow heating process. The PC is plugged with a Bluetooth Dongle for communication with sensor. The Swing Application developed on the PC displays the sensor data (temperature, humidity, etc) by making the sensor nodes to invoke the JAX-WS deployed on the server. The nodes are in sleep mode most of the time with short active intervals for sensor sampling and data aggregation.

The implementation started with modeling the desired interactions between the sensors and the business system using Web Service Description Language. The abstract WSDL

service definitions were then fed into Apache Tomcat framework to generate the serialization and parsing code. The same WSDL interface was used by the JAX-WS code generation tools. The code produced was then combined with our network layer wrapper, which were deployed on the Mulle sensor platform. To avoid manual configuration of the server address for each sensor node, two operations of the Ws-Discovery were also implemented and deployed on the sensor platform to dynamically locate the heating service.

2) Mobility Scenario: In this scenario, the sensor node is being carried by a person with Bluetooth-enabled Android mobile phone. The phone provides access to a 3G network that enables connectivity of the sensor node and the Java server on a TCP/IP layer. The Android application installed on the mobile displays the sensor data from the sensor by making it to invoke the web service deployed on the server.

5. CONCLUSION

Integration of high-end systems with deeply embedded sensor nodes enables standard based and direct application-layer integration between web service enabled IT systems and resource constrained sensor nodes. Our future work to apply the same SOA approach to sensor nodes for critical applications where security mechanisms are essential is on research analysis.

6. ACKNOWLEGEMENT

This paper has benefited from conversations with many different people – far more than can be acknowledged completely here. Still we would like to particularly thank Dr.P.S.K.PATRA, HOD, CSE for his guidance and support.

7. REFERENCES

[1] Rumen Kyusakov and Jens Eliasson, "Integration of Wireless Sensor and Actuator Nodes with IT infrastructure using Service-oriented Architecture", IEEE Trans.Industrialinformatics, vol.9, no.1, Feb 2012.

[2] Devices Profile for Web Services Version 1.1, OASIS Std., 2009.[Online] .Available:http://docs.oasis-open.org/wsdd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.pdf

[3] L. D. Xu, "Enterprise systems: State-of-the-art and future trends,"IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.
.

[4] S. de Deugd, R. Carroll, K. E. Kelly, B.Millett, and J. Ricker, "SODA:Service oriented device architecture," IEEE Pervasive Comput., vol. 5,no. 3, pp. 94–96, Jul.-Sep. 2006.

[5] Laurent Gomez, Annett Laube and Alessandro Sorniotti,"Design Guidelines for Integration of Wireless Sensor Networks with Enterprise Systems ",IEEETrans,Computer Society,Jun.2007.

[6] G.Moritz, E. Zeeb, F. Golatowski, D. Timmermann, and R. Stoll, "Webservices to improve interoperability of home healthcare devices," inProc. 2rd Int. Conf. Pervasive Comput. Technol. Healthcare, Pervasive Healthcare, 2009, pp. 1–4.

[7] J. Leguay, M. Lopez-Ramos, K. Jean-Marie, and V. Conan, "An efficientservice oriented architecture for heterogeneous and dynamicwireless sensor networks," in Proc.33rd IEEE Conf. Local Comput.Networks, LCN'08, 2008, pp. 740–747.

[8] A.Wolff, S. Michaelis, J. Schmutzler, and C.Wietfeld, "Network-centric middleware for service oriented architectures across heterogeneous embedded systems," in Proc. IEEE 11th Int. EDOC Conf. Workshop,EDOC'07, 15–16, 2007, pp. 105–108.

[9] R. Bosman, J. Lukkien, and R. Verhoeven, "Gateway architectures for service oriented application-level gateways," IEEE Trans. Consumer Electron., vol. 57, no. 2, pp. 453–461, May 2011.

[10] A. Cannata, M. Gerosa, and M. Taisch, "Socrades: A framework for developing intelligent systems in manufacturing," in Proc. Int. Conf.Ind. Eng. Eng. Manage., IEEM'08, 8–11, 2008, pp. 1904–1908.

[11] N. B. Priyantha, A. Kansal, M. Goraczko, and F. Zhao, "Tiny web services: Design and implementation of interoperable and evolvablesensor networks," in *Proc. 6th ACM Conf. Embedded Network Sensor Syst., SenSys'08*, New York, NY, USA, 2008, pp. 253–266.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 185 - 187, 2013, ISSN: 2319–8656

A Review of Machine Learning based Anomaly Detection Techniques

Harjinder Kaur
Dept of Computer Science and Engineering,
Punjabi University Regional Centre of IT & Management,
Mohali, Punjab, India

Gurpreet Singh
Dept of Computer Science and Engineering,
DAV Institute of Engineering & Technology,
Jalandhar, Punjab, India

Jaspreet Minhas
Dept of Computer Science and Engineering,
DAV Institute of Engineering and Technology,
Jalandhar, Punjab, India

Abstract: Intrusion detection is so much popular since the last two decades where intrusion is attempted to break into or misuse the system. It is mainly of two types based on the intrusions, first is Misuse or signature based detection and the other is Anomaly detection. In this paper Machine learning based methods which are one of the types of Anomaly detection techniques is discussed.

Keywords: Intrusion; Anomaly; Machine learning; IDS

1. INTRODUCTION

Intruders may be from outside the host or the network or legitimate users of the network. Intrusion detection is the process of monitoring the events that are occurring in the systems or networks and analyzing them for signs of possible incidents, which are violations or threats to computer security policies, acceptable use policies, or standard security practices [1]. That system which detects the intrusion in the system is known as IDS (Intrusion detection System).This concept has been around for two decades but recently seen a dramatic rise in the popularity and incorporation into the overall information security infrastructure [1]. Thus the intrusion can be found mainly using two classification techniques: Misuse or signature based detection and the other is Anomaly detection.

2. DETECTION TECHNIQUES

First technique of detection, Signature based also referred to as pattern based, looks for evidence known to be indicative of misuse. Whether it's looking for specific log entries or a specific payload in a data packet, the NIDS/HIDS is looking for something it knows about – a signature of misuse. While Anomaly based detection looks for signs that something is out of the ordinary that could indicate some form of misuse. Anomaly based systems analyze current activity against a "baseline" of "normal" activity and look for deviations outside that which is considered normal [2]. These two techniques applied for the major classification of IDS named Host based IDS (HIDS), Network based IDS (NIDS) and the Hybrid IDS [1].

3. MACHINE LEARNING BASED TECHNIQUES

Anomaly detection techniques can be sub categorized into Statistical Approaches, Cognition and Machine learning. Today, Machine learning techniques are popular for so many real time problems. Machine learning techniques are based on explicit or implicit model that enables the patterns analyzed to be categorized. It can be categorized into Genetic Algorithms, Fuzzy Logic, Neural Networks, Bayesian networks and outlier detection [3] [4].

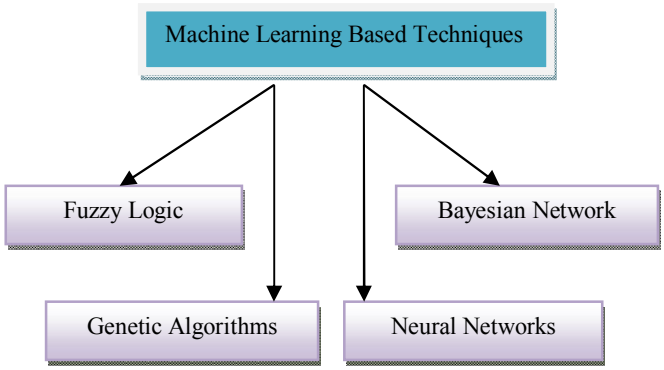


Figure 1: Categories of Machine learning based techniques

3.1 Fuzzy Logic

Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely derived from classical predicate logic. Fuzzy techniques are thus used in the field of anomaly detection mainly because the features to be considered can be seen as fuzzy variables. Although fuzzy logic has proved to be effective, especially against

port scans and probes, its main disadvantage is the high resource consumption involved. [5].

3.2 Genetic Algorithms

Genetic Algorithms are biologically inspired search heuristics that employs evolutionary algorithm techniques like crossover, inheritance, mutation, selection etc. So, genetic algorithms are capable of deriving classification rules and selecting optimal parameters for detection process. The application of Genetic Algorithm to the network data consist primarily of the following steps [6]:

i. The Intrusion Detection System collects the information about the traffic passing through a particular network.
ii. The Intrusion Detection System then applies Genetic Algorithms which is trained with the classification rules learned from the information collected from the network analysis done by the Intrusion Detection System.
iii. The Intrusion Detection System then uses the set of rules to classify the incoming traffic as anomalous or normal based on their pattern.

3.3 Neural Networks

A neural network is the ability to generalize from limited, noisy and data that is not complete. This generalization capability provides the potential to recognize unseen patterns, i.e., not exactly matched patterns that are different from the predefined structures of the previous input patterns. The neural network has been recognized as a promising technique for anomaly detection because the intrusion detector should ideally recognize not only previously observed attacks but also future unseen attacks [7].

3.4 Bayesian Networks

A Bayesian network is a model that encodes probabilistic relationships among the variables of interest. This technique is generally used for intrusion detection in combination with statistical schemes, a procedure that yields several advantages, including the capability of encoding interdependencies between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data [5].

4. PROS/CONS OF ANOMALY DETECTION

Because anomaly based systems are capable of detecting misuse based on network and system behavior, the type of misuse does not need to be previously known. This allows for the detection of misuse a signature based system may not detect. While behavior on a system or a network can vary widely, anomaly based systems have the tendency to report a lot of false alarms. The art of effectively identifying “normal” activity vs. truly abnormal is extremely challenging [8] [3].

Techniques	Pros/Cons
Fuzzy Logic	• Reasoning is Approximate rather than precise. • Effective, especially against port scans and probes. • High resource consumption involved.
Genetic Algorithm	• Biologically inspired and employs evolutionary algorithm. • Uses the properties like Selection, Crossover, and Mutation. • Capable of deriving classification rules and selecting optimal parameters.
Neural Network	• Ability to generalize from limited, noisy and incomplete data. • Has potential to recognize future unseen patterns.
Bayesian Network	• Encodes probabilistic relationships among the variables of interest. • Ability to incorporate both prior knowledge and data.

Table 1: Various Machine learning based anomaly detection Techniques

5. CONCLUSION

In this review paper, types of intrusion detection have been discussed along with the brief introduction of the categories of the Anomaly detection which is one of the types of IDS. Machine learning based anomaly detection techniques are also discussed from the suitable references.

6. REFERENCES

[1] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," Department of commerce, National Institute of Standards and Technology, Gaithersburg, 2007.

[2] Asmaa Shaker ashoor and Sharad Gore, "Intrusion Detection System (IDS): Case Study," in *IACSIT Press*, Singapore, 2011, pp. 6-9.

[3] Chris Petersen. (2012, February) LogRhythm website. [Online]. www.logrhythm.com

[4] V. Jyothsna, V.V Ramaprasad, and K Munivara Prasad, "A Review of Anomaly based Intrusion," *International Journal of Computer Applications*, vol. 28, no. 7, pp. 26-35, August 2011.

[5] P Garcia Teodora, J Diaz Verdejo, G Macia Farnandez, and E Vazquez, "Anomaly-based network intrusion detection:Techniques,Systems and Challenges," *Journal of Computers & Security*, vol. 28, no. 1, pp. 18-28, February 2009.

[6] Rajdeep Borgohain, "FuGeIDS : Fuzzy Genetic paradigms in Intrusion Detection Systems," *International Journal of Advanced Networking and Applications*, vol. 3, no. 6, pp. 1409-1415, 2012.

[7] Sang Jun Han and Sung Bae Cho, "Evolutionary Neural Networks for Anomaly," IEEE Transaction on Systems, Man, and Cybernetics,Part B: CYBERNETICS, vol. 36, no. 3, pp. 559-570, June 2006.

[8] Peng Ning and Sushil Jajodia. (2012, February) Intrusion Detection Techniques.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 188 - 194, 2013

Ensuring Privacy and Security in Data Sharing under Cloud Environment

Shilpa Elsa Abraham
Nandha Engineering College
Erode, India

R.Gokulavanan
Nandha Engineering College
Erode, India

Abstract: An important application of data sharing in cloud environment is the storage and retrieval of Patient Health Records (PHR) that maintain the patient's personal and diagnosis information. These records should be maintained with privacy and security for safe retrieval. The privacy mechanism protects the sensitive attributes. The security schemes are used to protect the data from public access. The data are allowed to be accessed only by authorized individuals. Each party is assigned with access permission for a set of attributes. Data owners update the patient data into third party cloud data centers. The attribute based encryption (ABE) scheme is used to secure these patient records. Multiple owners are allowed to access the same data values. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism due to its vast access. The MA-ABE model is not tuned to provide identity based access mechanism. Distributed storage model is not supported in the MA-ABE model.The proposed system is designed to provide identity based encryption facility. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

Keywords: Personal health records, cloud computing, multi-authority attribute-based encryption, distributed environment, attribute based encryption

---

1. INTRODUCTION

Cloud computing is the use of computing resources which may be hardware or software that are delivered as a service over a network. Cloud computing entitles resource sharing to achieve best utility over a network. Resources are shared on a need basis in the best possible manner under clouds. The Personal Health Record (PHR) sharing among a wide range of personnel has been identified as an important application in the field of cloud computing. A personal health record is a health record where health data and information related to the care of a patient is maintained by the patient himself. The purpose of PHR is to provide accurate medical details about the patient, which can be accessed online also. PHR can cover a wide variety of information including prescription report, family history, allergy details, and laboratory test results and so on.

In recent years, personal health record has emerged as a prominent patient-centric model of health information exchange. The patient himself is the core owner of his /her data. This record enables the patient to create and control her medical data that are placed data center, from where different individuals access the data values. These data centers

incur heavy cost in their construction and maintenance. Therefore, many PHR services are outsourced to or provided by third-party service providers like Microsoft Health Vault, Google Health.

The data outsourced to service providers are largely consumed by wide variety of individuals. Hence the need of security and privacy in personal health records is an important issue. This brings the idea of encrypting the data before outsourcing to the servers. To ensure best policy, it is the patient herself who should encrypt the data and determines which users shall have access in what manner. This often conflicts with scalability since there are a wide variety of personnel who try to access the PHR data. The data access may be for professional purposes or personal purposes which are categorized as professional users and personal users. Professional users include doctors, researchers, lab technicians etc whereas personal users include family members and friends. This large scale of users may lead to key management overhead upon the patient. In order to overcome this overhead, a central authority (CA) has been appointed to perform key management of professional users[1]. But this again requires too much trust on single authority, which possesses a serious challenge. However, key management of personal users have been managed by the patient herself

This leads to the adoption of a new encryption pattern namely Attribute Based Encryption (ABE)[2]. In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism.Each authority is permitted to run its own copy of SW and then combining the results so as to achieve encryption [3].

2. ACCESS CONTROL

Access controls are security features that control how users and systems communicate and interact with one another. From (ISC)2 Candidate Information Bulletin, Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. Access control mechanisms can be grouped into four main classes: *discretionary*, *mandatory*, *role-based and attribute based*[4]. A system that uses discretionary access control (DAC) allows the owner of the resource to specify which subjects can access which resources. The authorization rulesexplicitly state which subjects can execute which actions on which resources. Mandatory Access Control (MAC) is a type of access control in which only the administrator manages the access controls. The administrator defines the access policy, which cannot be modified or changed by users, and the policy will indicate who has access to which programs and files. In a role-based access control (RBAC) model, access control is based on user's roles and on rules defining which roles can perform which actions on which resources. Finally, in an attribute based access control model (ABAC), access is controlled based on user's attributes.

2.1 Attribute Based Access Control

Attribute Based Access Control uses attributes as building blocks that defines access control rules and describes access requests. These attributes are sets of labels or properties that can be used to describe all the entities that must be considered for authorization purposes ie, access is controlled not by the rights that are possessed by the user, but by the attributes of the user. An attribute-based access control policy specifies certain claims that need to be satisfied in order to grant access to a

resource. For instance the claim could be "older than 18". Any user that can prove this claim is granted access. This is the basic concept of attribute based access control.

3. PROBLEM DOMAIN

Now, problem is being extended to a wider range, where a number of PHR owners and users are involved. This is a bigger system of environment. The owners refer to patients whose medical related data are being controlled and maintained and the users are those who try to access them. There exists a central server where owners place their sensitive medical data, and is attempted by users to gain access. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. This leads to the need of Multi-Authority Attribute Based Encryption (MA-ABE). However, MA-ABE supports neither identity based access control nor distributed access[5]. Hence this paper focuses on providing distributed access control to the PHR data by extending MA-ABE.

3.1Design Goals

An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over her personal health record. She determines which all users shall have access to her medical record. User controlled read/write access and revocation are the two core security objectives for any electronic health record system [6]. User controlled writes access control in PHR context entitles prevention of unauthorized users to gain access to the record and modifying it. Fine grained access control should be enforces in the sense that different users are authorized to read different sets of documents[7].

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. Yet another design goal is on-demand revocation. These two objectives form the core of the paper. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation[8]. The PHR system should support users from both the personal domain as well as public domain. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

4. SOLUTION FRAMEWORK

As the main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management, the proposed idea is twofold.

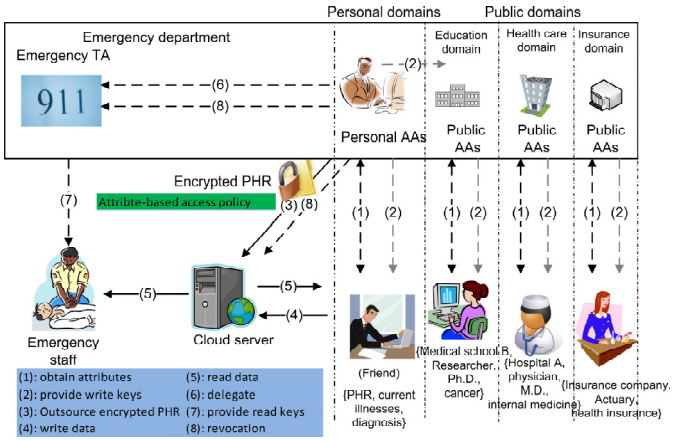


Fig 1. Sharing of PHR

First, the system is divided into multiple security domains like personal domain (PSD) and public domain(PUD). Each domain controls only a subset of its users. For each security domain, one or more authorities are assigned to govern the access of

data. For personal domain it is the owner of the PHR itself who manages the record and performs key management. This is less laborious since the number of users in the personal domain is comparatively less and is personally connected to the owner. On the other hand, public domain consists of a large number of professional users and therefore cannot be managed easily by the owner herself. Hence it puts forward the new set of public attribute authorities (AA) to govern disjoint subset of attributes distributively. Users from different sectors on submission of their identity information initially obtain attribute based secret keys from their attribute authorities. This attribute based key can be used to obtain authorized access to the medical records. In addition, AAs may also grant write keys to certain users based on their privilege. They are only permitted to make desired changes to the PHR record.In originality, PUD can be related to independent sectors like hhealth care, insurance, education etc. Hence, public domain users need not communicate with the PHR owner in order to obtain its access; instead it requires communication with the attribute authorities alone. Hence the involvement of attribute authorities greatly reduce the management overhead of PHR owners.

Secondly, so as to achieve security of health records, new encryption patterns namely attribute based encryption (ABE) is adopted. Data is classified according to their attributes. In certain cases, users may also be classified accordingly into roles. PHR owner encrypts her record under a selected set of attributes and those users that satisfy those attributes can obtain decryption key in order to access the data. However, in the new solution pattern, an advanced version of ABE called multi-authority ABE (MA-ABE) is used. In this encryption scheme, many attribute authorities operate simultaneously, each handing out secret keys for a different set of attributes.

4.1Multi-Authority ABE

A Multi-Authority ABE system is comprised of k attribute authorities and one central authority. Each attribute authority is also assigned a value,dk. The system uses the following algorithms:

Set up: A random algorithm that is run by the central authority or some other trusted authority. It takes as input the security parameter and outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

Attribute Key Generation: A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.

Central Key Generation: A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user.

Encryption: A randomized algorithm run by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the ciphertext.

Decryption: A deterministic algorithm run by a user. It takes as input a cipher-text, which was encrypted under attribute set and decryption keys for that attribute set. This decryption algorithm outputs a message m.

4.2 Security Analysis of the Proposed System

i) *Fine-grainedness of Access Control:* In the proposed scheme, the data owner is able to define and enforce expressive and flexible access structure for each user. Specifically, the access structure of each user is defined as a logic formula over data file

attributes, and is able to represent any desired data file set.

ii) *Data Confidentiality:* The proposed scheme discloses the information about each users' access on the PHR among one another. For eg, the data revealed to a research scholar may be unknown to a lab technician.

iii) *User Access Privilege Confidentiality*:The system does not reveal the privileges of one user to another. This ensures user access privilege confidentiality. This is maintained for public domain as well as private domain.

5. SECURE SHARING OF PERSONAL HEALTH RECORDS USING DISTRIBUTED ABE

The system is designed to manage Patient Health Records (PHR) with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities. The system is enhanced to support Distributed ABE model. The user identity based access mechanism is also provided in the system. The system is divided into six major modules. They are data owner, cloud provider, key management, security process, authority analysis and client.

5.1 DataOwner

The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities.

5.2 Cloud Provider

The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider.

5.3 Key Management

The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system.

5.4 Security Process

The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.

5.5 Authority Analysis

Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority.

5.6 Client

The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.

6. DESIGN ISSUES

The system scalability is enhanced using ABE and MA-ABE. There are some limitations in the practicality of using them in building PHR systems. For example, in workflow-based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. In those scenarios one may consider the use of attribute-based broadcast encryption. In addition, the expressibility of our encryptor's access policy is somewhat limited by that of MA-ABE's, since it only supports conjunctive policy across multiple AAs. In practice, the credentials from different organizations may be considered equally effective, in that case distributed ABE schemes will be needed. The following drawbacks are identifying from the existing system. User identity bases access control mechanism is not supported under the situation. Dynamic policy management is yet another issue.

Advantages of the system are as follows:

- Distributed environment
- Security of sensitive fields
- Break glass access for emergency situations
- On-demand revocation

7. CONCLUSION

The patient health records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records under distributed environment in cloud computing has been proposed in this paper .Public and personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced while guaranteeing the privacy compared with previous works. The attribute-based encryption model is enhanced to support distributed ABE operations with MA-ABE. The system is improved to support dynamic policy management model. Thus, patient health records are maintained with security and privacy. It is a server choice based security model and possess central key management with attribute authorities.

8. REFERENCES

[1]M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept. 2010, pp. 89–106.

[2] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.

[3]Melissa Chase,"Multi-Authority Attribute Based Encryption", Computer Science Department, Brown University.

[4] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation,"Technical Report, University of Waterloo, 2010.

[5]S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute- based encryption," Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[6] H. Lohr, A.-R.Sadeghi, and M. Winandy, "Securing the e-health¨ cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[9] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications Magazine, Feb. 2010.

[10] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.

[12] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[13] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[15] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[16] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[17] S. M¨ uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption,"Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[18] "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 195 - 207, 2013, ISSN: 2319–8656

Cooperative Demonstrable Data Retention for Integrity Verification in Multi-Cloud Storage

Krishna Kumar Singh
GIDA Gorakhpur
U.P India

Rajkumar Gaura
GIDA Gorakhpur
U.P India

Sudhir Kumar Singh
GIDA Gorakhpur
U.P India

Abstract Demonstrable data retention (DDR) is a technique which certain the integrity of data in storage outsourcing. In this paper we propose an efficient DDR protocol that prevent attacker in gaining information from multiple cloud storage node. Our technique is for distributed cloud storage and support the scalability of services and data migration. This technique Cooperative store and maintain the client's data on multi cloud storage. To insure the security of our technique we use zero-knowledge proof system, which satisfies zero-knowledge properties, knowledge soundness and completeness. We present a Cooperative DDR (CDDR) protocol based on hash index hierarchy and homomorphic verification response. In order to optimize the performance of our technique we use a novel technique for selecting optimal parameter values to reduce the storage overhead and computation costs of client for service providers.

Keyword: Demonstrable Data Retention, homomorphic, zero knowledge, storage outsourcing, multiple cloud, Cooperative, data Retention.

1. INTRODUCTION

IN past few years, a cloud storage service has become a faster profitable growth point by providing their clients a reasonably scalable, low-cost, position-independent platform for client's data. As cloud computing environment is made based on open architectures and interfaces, it has the capability to incorporate multiple internal or/and external cloud services together to provide high interoperability. We say such a distributed cloud environment as a hybrid cloud (or multi-Cloud). Very often, we use virtual infrastructure management (VIM) [2], a multi-cloud allows clients to easily access his or her resources remotely through interfaces such as Web services provided by Amazon EC2. There exist various tools and technologies for multicloud, such as Vmware vSphere, Platform VM Orchestrator and Ovirt. These tools help cloud providers to construct a distributed cloud storage platform (DCSP) for managing client's data. However, such an important platform is vulnerable to be compromised, especially in a hostile environment and it would bring irretrievable losses to the clients. For examplethe confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or confidential data and archives may be lost or altered with when they are stored into a hostile storage pool outside the enterprise. Therefore, it is important and necessary for cloud service providers (CSPs) to provide security techniques for managing their storage services. Demonstrable data retention (DDR) [1] (or proofs of retrievability (POR) [2]) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The verification without downloading makes it especially important for large-size files and folders (typically including many clients' files) to check whether these data have been altered with or deleted without downloading the latest version of data. Thus, it is able to replace traditional hash and signature functions in storage outsourcing. Various DDR techniques have been recently proposed, such as Scalable DDR [4] and Dynamic DDR [5]. However, these techniques mainly focus on DDR issues atuntrusted servers in a single cloud storage providerand are not suitable for a multi-cloud environment (see the comparison of POR/DDR techniques in Table 1)**Motivation**: In order to provide a low-cost, scalable, location-independent platform for managing clients' data, current cloud storage systems adopt several new distributedfile systems, for example, Google File System (GFS),Apache Hadoop Distribution File System (HDFS), Amazon S3 File System, CloudStore etc.These file systems share

TABLE 1: Comparison of POR/DDR schemes for a file consisting of n blocks

Scheme	Type	CSP Comp.	Client Comp.	Comm.	Flag.	Privacy	Multiple Clouds	Prob. Of Detection
DDR[2]	$HomT$	O(t)	O(t)	O(1)		✓	#	$1-(1-\rho)t$
SDDR[4]	MHT	O(t)	O(t)	O(t)	✓	✓		$1-(1-\rho)t{\cdot}s$
CDDR-[5]	MHT	O(t.log n)	O(t.log n)	O(t log n)		✓		$1-(1-\rho)t$
CDDR-II[5]	MHT	O(t log n)	O(t log n)	O(t log n)				$1-(1-\rho)\Omega(n)$
CPOR-[6]	$HomT$	O(t)	O(t)	O(1)			#	$1-(1-\rho)t$
CPOR-II{6}	$HomT$	O(t+s)	O(t+s)	O(s)	✓		#	$1-(1-\rho)$t-s
OurScheme	HomR	O(t+c.s)	O(t+s)	O(s)	✓	✓	✓	$1-\Pi Pk\in\mathcal{P}$ $(1-\rho k)rk{\cdot}t{\cdot}s$

s is the number of sectors in each block, c is the number of CSPs in a multi-cloud, t is the number of sampling blocks, ρ and ρk are the probability of block corruption in a cloud server and k-th cloud server in a multi-cloud $\mathcal{P}=\{Pk\}$, respective, $\#$ denotes the verification process in a trivial approach, and $MHT, HomT, HomR$ denotes Merkle Hash tree, homomorphic tags, and homomorphic response respectively.

some similar features: a single metadata server provides centralized management by a global namespace; files are split into blocks or chunks and stored on block servers; and the systems are comprised of interconnected clusters of block servers. Those features enable cloud service providers to store and process large amounts of data. However, it is crucial to offer an efficient verification on the integrity and availability of stored data for detecting faults and automatic recovery. Moreover, this verification is necessary to provide reliability by automatically maintaining multiple copies of data and automatically redeploying processing logic in the event of failures. Although existing techniques can make a false or true decision for data retention without downloading data at untrusted stores, they are not suitable for a distributed cloud storage environment since they were not originally constructed on interactive proof system. For example, the techniques based on Merkle Hash tree (MHT), such as Dynamic DDR-I, Dynamic DDR-II [1] and scalable DDR [4] in Table-1. Use an authenticated skip list to check the integrity of file blocks adjacently in space Unfortunately, they did not provide any algorithms for constructing distributed Merkle trees that are necessary for efficient verification in a multi-cloud environment. In addition, when a client asks for a file block, the server needs to send the file block along with a proof for the correctness of the block. However, this process incurs significant communication overhead in a multi-cloud environment, since the server in one cloud typically needs to generate such a proof with the help of other cloud storage services, where the adjacent blocks are stored. The other techniques, such as DDR [1], CPOR-I, and CPOR-II [6] in Table 1, are constructed on homomorphic verification tags, by which the server can generate tags for multiple file blocks in terms of a single response value. However, that doesn't mean the responses from multiple clouds can be also combined into a single value on the client side. In case of lack of homomorphic responses, clients must invoke the DDR protocol repeatedly to check the integrity of file blocks stored in multiple cloud servers. Also, clients need to know the exact position of each file block in a multi-cloud environment. In addition, the verification process in such a case will lead to high communication overheads and computation costs at client sides as well. Therefore, it is of utmost necessary to design a Cooperative DDR model to reduce the storage and network overheads and enhance the transparency of verification activities in cluster-based cloud storage systems. Moreover, such a Cooperative DDR technique should provide features for timely detecting abnormality and renewing multiple copies of data. Even though existing DDR techniques have addressed various security properties, such as public verifiability [1], dynamics [5], scalability [4], and privacy preservation [7], we still need a careful consideration of some potential attacks, including two major categories: Data Leakage Attack by which an adversary can easily obtain the stored data through verification process after running or wire-tapping sufficient verification communications and Tag Forgery Attack by which a dishonest CSP can deceive the clients. These two attacks may cause potential risks for privacy leakage and ownership cheating. Also, these attacks can more easily compromise the security of a distributed cloud system than that of a single cloud system. Although various security models have been proposed for existing DDR techniques [1], [7], [6], these models still cannot cover all security requirements, especially for demonstrable secure privacy preservation and ownership verification. To establish a highly effective security model, it is necessary to analyze the DDR technique within the framework of zero-knowledge proof system (ZKPS) due to

the reason that DDR system is essentially an interactive proof system (IPS), which has been well studied in the cryptography community. In summary, an verification technique for data integrity in distributed storage environments should have the following features: **Usability aspect:** A client should utilize the integrity check in the way of collaboration services. The technique should conceal the details of the storage to reduce the burden on clients; **Security aspect:** The technique should provide adequate security features to resist some existing attacks, such as data leakage attack and tag forgery attack; **Performance aspect:** The technique should have the lower communication and computation overheads than non-Cooperative solution.

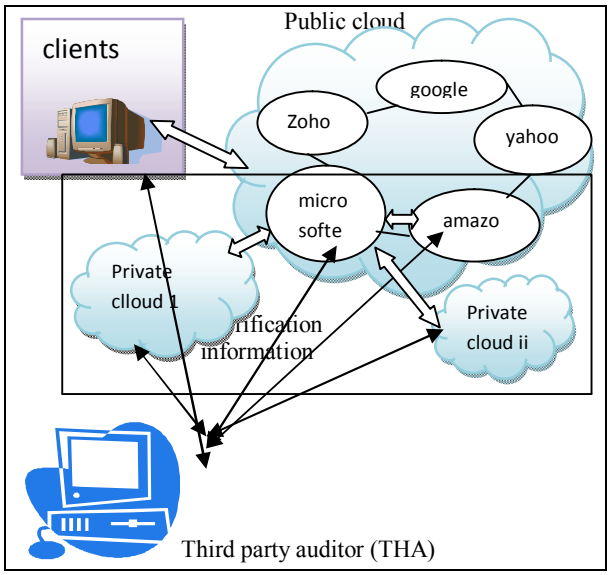
Related Works: To ensure the integrity and availability of outsourced data in cloud storages, researchers have proposed two basic approaches called Demonstrable data retention (DDR) [1] and Proofs of Retrievability (POR) [1]. Ateniese et al. [1] first proposed the DDR model for ensuring retention of files on untrusted storages and provided an RSA-based technique for a static case that achieves the (1) communication cost. They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data retention. This property greatly extended application areas of DDR protocol due to the separation of data owners and the users. However, these techniques are insecure against replay attacks in dynamic scenarios because of the dependencies on the index of blocks. Moreover, they do not fit for multi-cloud storage due to the loss of homomorphism property in the verification process. In order to support dynamic data operations, Ateniese et al. developed a dynamic DDR solution called Scalable DDR [4]. They proposed a lightweight DDR technique based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere. Based on this work, Erway etal. [5] Introduced two Dynamic DDR techniques with a hash function tree to realize (log n) communication and computational costs for a n-block file. The basic technique, called CDDR-I, retains the drawback of Scalable DDR, and in the 'blockless' technique, called CDDRII, the data blocks $\{mij\}j\in[1,t]$ can be leaked by the response of a challenge, $M = \sum_{j=1}^{t} a\,jmij$, where aj is a random challenge value. Furthermore, these techniques are also not effective for a multi-cloud environment because the verification path of the challenge block cannot be stored completely in a cloud [8]. Juels and Kaliski [3] presented a POR technique, which relies largely on preprocessing steps that the client conducts before sending a file to a CSP. Unfortunately, these operations prevent any efficient extension for updating data. Shacham and Waters [6] proposed an improved version of this protocol called Compact POR, which uses homomorphic property to aggregate a proof into (1) authenticator value and $O(t)$ computation cost for t challenge blocks, but their solution is also static and could not prevent the leakage of data blocks in the verification process. Wang et al. [7] presented a dynamic technique with (log n) cost by integrating the Compact POR technique and Merkle Hash Tree (MHT) into the CDDR. Furthermore, several POR techniques and models have been recently proposed including [9], [10]. In [9] Bowers et al. introduced a distributed cryptographic system that allows a set of servers to solve the DDR problem. This system is based on an integrity-protected error Correcting code (IP-ECC), which improves the security and efficiency of existing tools, like POR. However, a file must be transformed into l distinct segments with the same length, which are distributed across l servers. Hence, this system is more suitable for RAID rather than cloud storage. Our Contributions, in this paper, we address the problem of demonstrable data retention in distributed cloud environments from the following aspects: high performance, transparent verification, and high security. To achieve these goals, we first propose a verification framework for multi-cloud storage along with two fundamental techniques: homomorphic verifiable response (HVR) and hash index hierarchy (HIH). We then demonstrate that the possibility of constructing a Cooperative DDR (CDDR) technique without compromising data privacy based on modern cryptographic techniques, such as interactive proof system (IPS). We further introduce an effective construction of CDDR technique using above-mentioned structure. Moreover, we give a security analysis of our CDDR technique from the IPS model. We prove that this construction is a multi-prover zero-knowledge proof system (MP-ZKPS) [11], which has zero-knowledge properties, completeness and knowledge soundness. These properties ensure that CDDR technique can implement the security against data leakage attack and tag forgery attack. To improve the system performance with respect to our technique, we analyze the performance of probabilistic queries fordetecting abnormal situations. This probabilistic method also has an inherent benefit in reducing computation and communication overheads. Then, we present an efficient method for the selection of optimal parameter values to minimize the computation overheads of CSPs and the clients' operations. Inaddition, we analyze that our technique is suitable for existing distributed cloud storage systems. Finally, our experiments show that our solution introduces very limited computation and communication overheads.

Organization: The rest of this paper is organized as follows. In Section 2, we describe a formal definition of CDDR and the underlying techniques, which are utilized in the construction of our technique. We introduce the details of Cooperative DDR technique for multicloud storage in Section 3. We describe the security and performance evaluation of our technique in Section 4 and 5, respectively. We discuss the related work in Section and Section 6 concludes this paper.

2. STRUCTURE AND TECHNIQUES

In this section, we present our verification framework for multi-cloud storage and a formal definition of CDDR. We introduce two fundamental techniques for constructing our CDDR technique: hash index hierarchy (HIH) on which the responses of the clients' challenges computed from multiple CSPs can be combined into a single response as the final result; and homomorphic verifiable response (HVR) which supports distributed cloud storage in a multi-cloud storage and implements an efficient construction of collision resistant hash function, which can be viewed as a random oracle model in the verification protocol.

Fig 1: Verification architecture for data integrity.



2.1 Verification Framework for Multi-Cloud:

Although existing DDR techniques offer a publicly accessible remote interface for checking and managing the tremendous amount of data, the majority of existing DDR techniques is incapable to satisfy the inherent requirements from multiple clouds in terms of communication and computation costs. To address this problem, we consider amulti-cloud storage service as illustrated in Figure 1. In this architecture, a data storage service involves three different entities: Clients who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data; Cloud Service Providers (CSPs) who work together to provide data storage services and have enough storages and computation resources; and Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In this architecture, we consider the existence of multiple CSPs to Cooperative store and maintain the clients' data. Moreover, a Cooperative DDR is used to verify the integrity and availability of their stored data in all CSPs. The verificationprocedure is described as follows: Firstly, a client (data owner) uses the secret key to pre-process a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP, transmits the file and some verification tagsto CSPs, and may delete its local copy; Then, by using a verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP. We neither assume that CSP is trust to guarantee the security of the stored data, nor assume that data owner has the ability to collect the evidence of the CSP's fault after errors have been found. To achieve this goal, a TTP server is constructed as a core trust base on the cloud for the sake of security We assume the TTP is reliable and independent through the following functions [12]: to setup and maintain the CDDR cryptosystem; to generate and store data owner's public key; and to store the public parameters used to execute the verification protocol in the CDDR technique. Note that the TTP is not directly involved in the CDDR technique in order to reduce the complexity of cryptosystem.

2.2 Definition of Cooperative DDR:

In order to prove the integrity of data stored in a multi-cloud environment, we define a framework for CDDR based on interactive proof system (IPS) and multi-prover zero-knowledge proof system (MPZKPS), as follows:**Definition 1 (Cooperative-DDR):** A Cooperative demonstrable data retention $\mathcal{S} = (KeyGen, TagGen, Proof)$ is a collection of twoalgorithms $(KeyGen, TagGen)$ and an interactive proof system $Proof$, as follows: (1^k): takes a security parameter k as input, and returns a secret key sk or a public-secret key-pair (pk, sk); $TagGen(sk, F, \mathcal{P})$: takes as inputs a secret key sk, a file F, and a set of cloud storage providers $\mathcal{P} = \{Pk\}$, and returns the triples (ζ, ψ, σ), where ζ isthe secret in tags, $\psi = (u, \mathcal{H})$ is a set of verification parameters u and an index hierarchy$\mathcal{H}$ for F, $\sigma = \{\sigma^{(k)}\}p_k \in \mathcal{P}$ denotes a set of all tags,$\sigma^{(k)}$ is the tag of the fraction $F^{(k)}$ of F in P_k; **$(\mathcal{P}$, V):** is a protocol of proof of

data retention between CSPs ($\mathcal{P} = \{P_k\}$) and a verifier (V), that is, $\langle \sum_{P_k \in p} P_k(F^{(k)}, \sigma^{(k)}) \leftrightarrow V \rangle (pk, \psi) = \begin{cases} 1, & F = \{F^{(k)}\} is intact \\ 0, & F = \{F^{(k)}\} is changed \end{cases}$ Where each P_k takes as input a file $F^{(k)}$ and a set of tags $\sigma^{(k)}$, and a public key pk and a set of public parameters ψ are the common input between P and V. At the end of the protocol run, V returns a bit {1|0} denoting true and false. Where, $\sum P_k \in p$ denotes Cooperative computing in $P_k \in \mathcal{P}$. A trivial way to realize the CDDR is to check the data stored in each cloud one by one, i.e. $\bigwedge_{P_k \in p} \langle P_k(F^{(k)}, \sigma^{(k)} \leftrightarrow V \rangle (\mathrm{pk}, \psi)$ Where $\bigwedge$ denotes the logical AND operations among the Boolean outputs of all protocols $\langle P_k, V \rangle$ for all $P_k \in \mathcal{P}$. However, it would cause significant communication and computation overheads for the verifier, as well as a loss of location-transparent. Such a primitive approach obviously diminishes the advantages of cloud storage: scaling arbitrarily up and down on demand [13]. To solve this problem, we extend above definition by adding an organizer (O), which is one of CSPs that directly contacts with the verifier, as follows: $\langle \sum_{P_k \in p} P_k(F^{(k)}, \sigma^{(k)}) \leftrightarrow O \leftrightarrow V \rangle$ (pk, ψ), Where the action of organizer is to initiate and organize the verification process. This definition is consistent with aforementioned architecture, e.g., a client (or an authorized application) is considered as, the CSPs are as $\mathcal{P} = \{P_i\} i \in [1, c]$, and the Zoho cloud is as the organizer in Figure 1. Often, the organizer is an independent server or a certain CSP in $\mathcal{P}$. The advantage of this new multi-prover proof system is that it does not make any difference for the clients between multi-prover verification process and single-prover verification process in the way of collaboration. Also, this kind of transparent verification is able to conceal the details of data storage to reduce the burden on clients. For the sake of clarity, we list some used signals in Table 2.

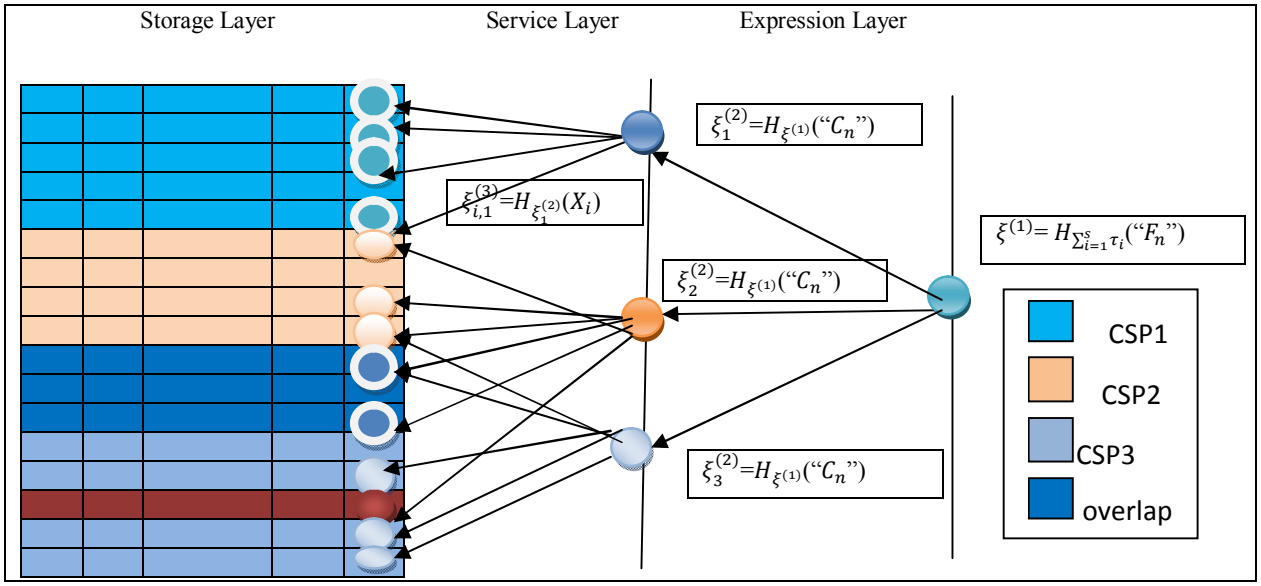
TABLE 2: The signal and its explanation.

Sig.	Repression
n	the number of blocks in a file;
s	the number of sectors in each block;
t	the number of index coefficient pairs in a query;
c	the number of clouds to store a file;
F	the file with $n \times s$ sectors, i.e., $F = \{mi,j\} i \in [1,n]$,$j \in [1,s]$;
σ	the set of tags, i.e., $\sigma = \{\sigma i\} i \in [1,n]$;
Q	the set of index-coefficient pairs, i.e., $Q = \{(i, vi)\}$;
θ	the response for the challenge Q.

2.3 Hash Index Hierarchy for CDDR: To support distributed cloud storage, we illustrate a representative architecture used in our Cooperative DDR technique as shown in Figure 2. Our architecture has a hierarchy structure which resembles a natural representation of file storage. This hierarchical structure $\mathcal{H}$ consists of three layers to represent relationships among all blocks for stored resources. They are described as follows: 1) **Express Layer:** offers an abstract representation of the stored resources; 2) **Service Layer:** offers and manages cloud storage services; and 3) **Storage Layer:** realizes data storage on many physical devices. We make use of this simple hierarchy to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems. For example, in Figure 2 the resources in Express Layer are split and stored into three CSPs, which are indicated by different colors, in Service Layer. In turn, each CSP fragments and stores the assigned data into the storage servers in Storage Layer. We also make use of colors to distinguish different CSPs. Moreover, we follow the logical order of the data blocks to organize the Storage Layer. This architecture also provides special functions for data storage and management, e.g., there may exist overlaps among data blocks (as shown in dashed boxes) and discontinuous blocks but these functions may increase the complexity of storage management. In storage layer, we define a common fragment structure that provides probabilistic verification of data integrity for outsourced storage. The fragment structure is a data structure that maintains a set of block-tag pairs, allowing searches, checks and updates in (1) time. An instance of this structure is shown in storage layer of Figure 2: an outsourced file F is split into n blocks {m1, m2, ⋯,}, and each block mi is split into s sectors {mi,1,mi,2, ⋯ ,mi,s}. The fragment structure consists of n block-tag pair (m_i,σ_i), where σ_i is a signature tag of block m_i generated by a set of secrets $\tau = (\tau_1, \tau_2, \cdots, \tau_s)$. In order to check the data integrity, the fragment structure implements probabilistic verification as follows: given a random chosen challenge (or query) $Q = \{(i,v_i)\}$ $i \in RI$, where I is a subset of the block indices and v_i is a random coefficient. There exists an efficient algorithm to produce a constant-size response ($\mu_1, \mu_2, \cdots, \mu_s, \sigma'$), where μ_i comes from all {m_k,i,v_k} k∈I and σ′ is from all {σ_k, v_k} k∈ I. Given a collision-resistant hash function H_k (·), we make use of this architecture to construct a Hash Index Hierarchy $\mathcal{H}$ (viewed as a random oracle), which is used to replace the common hash function in prior DDR techniques, as follows:**1) Express layer:** given s random $\{\tau_i\}_{i=1}^{s}$ and the file name F_n, sets $\xi^{(1)} = H_{\sum_i^s \tau_i F_n}$=1 and makes it public for verification but makes $\{\tau_i\}_{i=1}^{s}$ secret;**2) Service layer**: given the $\xi^{(1)}$ and the cloud name C_k, sets $\xi^{(2)} = H_{\xi^{(1)}}(C_k)$;**3) Storage layer:** given the $\xi^{(2)}$, a blocknumber i, and its index record X_i = "$B_i||V_i||R_i$", sets $\xi_{i,k}^{(3)} = H_{\xi_{i,k}^{(2)}}(X_i)$, where B_i is the sequence number of a block, V_i is the updated version number, and R_i is a random integer to avoid collision. As a virtualization approach, we introduce a simple index-hash table X = {X_i}

to record the changes of file blocks as well as to generate the hash value of each block in the verification process. The structure of X is similar to the structure of file block allocation table in file systems. The index-hash table consists of serial number, block number, version number, random integer, and so on. Different from the common index table, we assure that all records in our index table to differ from one another prevent forgery of data blocks and tags. By using this structure, especially the index records

Fig 2:Index-hash hierarchy of CDDR model.



and each block (s sectors) corresponds to a tag, so that the storage of signature tags can be reduced by the increase of s; 2) a verifier can verify the integrity of file in random sampling approach, which is of utmost importance for large files; 3) these techniques rely on homomorphic properties to aggregate data and tags into a constant size response, which minimizes the overhead of network communication; and 4) the hierarchy structure provides a virtualization approach to conceal the storage details of multiple CSPs.

2.4 Homomorphic Verifiable Response for CDDR:

A homomorphism is a map $f: \mathbb{P} \rightarrow \mathbb{Q}$between two groups such that $f(g_{1\oplus}g_2) = f(g_1) \otimes f(g_2)$ for all g_1, $g_2 \in \mathbb{P}$, where $\oplus$ denotes the operation in P and $\otimes$ denotes the operation in $\mathbb{Q}$. This notation has been used to define Homomorphic Verifiable Tags (HVTs) in [1]: Given two values σ_i and σ_j for two messages m_i andm_j , anyone can combine them into a value σ_i' corresponding to the sum of the messages $m_i + m_j$. When demonstrable data retention is considered as a challenge-response protocol, we extend this notation to the concept of Homomorphic Verifiable

$\{X_i\}$, our CDDR technique can also support dynamic data operations [8].The proposed structure can be readily incorporated into MAC-based, ECC or RSA techniques [1], [6]. These techniques, built from collision-resistance signatures (see Section 3.1) and the random oracle model, have the shortest query and response with publicverifiability.They share several common characters for theimplementation of the CDDR framework in the multiple clouds: 1) a file is split into $n \times s$ sectors

Responses (HVR), which is used to integrate multiple responses from the different CSPs in CDDR

technique as follows: ***Definition* 2** (HVR): A response is called homomorphic verifiable response in a DDR protocol, if given two responses Θ_i and Θ_j for two challenges Q_i andQ_j from two CSPs, there exists an efficient algorithm to combine them into a response Θcorresponding to the sum of the challenges $Q_i \cup Q_j$. Homomorphic verifiable response is the key technique of CDDR because it not only reduces the communication bandwidth, but alsoconceals the location of outsourced data in the distributed cloud storage environment.

3 COOPERATIVE DDR TECHNIQUES

In this section, we propose a CDDR technique for multi-cloud system based on the above-mentioned structure and techniques. This technique is constructed on collision-resistant hash, bilinear map group, aggregation algorithm, and homomorphic responses.

3.1 Notations and Preliminaries: Let $\mathbb{H} = \{H_k\}$ be a family of hash functions $H_k : \{0,1\}^n \rightarrow \{0,1\}^*$ index by $k \in \mathcal{K}$. We say that algorithm $\mathcal{A}$ has advantage ϵ in breaking collision resistance of $\mathbb{H}$ if $\Pr[\mathcal{A}(k) = (m_0, m_1) : m_0 \neq m_1, H_k(m_0) = H_k(m_0)] \geq \epsilon$, where the probability is over the random choices of $k \in \mathcal{K}$ and the random bits of $\mathcal{A}$. So that, we have the following definition: **Definition 3** (Collision-Resistant Hash): A hash family $\mathbb{H}$ is (t, ϵ)-collision-resistant if no t-time adversary has advantage at least ϵ in breaking collision resistance of $\mathbb{H}$. We set up our system using bilinear pairings proposed by Boneh and Franklin [12]. Let $\mathbb{G}$ and $\mathbb{G}T$ be two multiplicative groups using elliptic curve conventions with a large prime order p. The function e is a computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}T$ with the following properties: for any $G, H \in \mathbb{G}$ and all a, $b \in \mathbb{Z}p$, we have 1) Bilinearity: $e([a]G, [b]H) = e(G,H)ab$; 2) Non-degeneracy: $e(G,H) \neq 1$ unless G or $H = 1$; and 3) Computability: $e(G,H)$ is efficiently computable.**Definition 4** (Bilinear Map Group System): A bilinear map group system is a tuple $\mathbb{S} = \langle p,,, e \rangle$ composed of the objects as described above.

3.2 Our CDDR Technique: In our technique (see Fig 3), the manager first runs algorithm $KeyGen$ to obtain the public/private key pairs for CSPs and users. Then, the clients generate the tags of outsourced data by using $TagGen$. Anytime, the protocol $Proof$ is performed by a 5-move interactive Proof protocol between a verifier and more than one CSP, in which CSPs need not to interact with each other during the verification process, but an organizer, is used to organize and manage all CSPs. This protocol can be described as follows: 1) The organizer initiates the protocol and sends a commitment to the verifier; 2) The verifier returns a challenge set of random index-coefficient pair's Q to the organizer; 3) The organizer relays them into each lock; 4) Each Pi returns its response of challenge to the organizer; and 5) The organizer synthesizes aPi in $\mathcal{P}$ according to the exact position of each data final response from received responses and sends it to theverifier. The above process would guarantee that the verifier accesses files without knowing on which CSPs or in what geographical locations their files reside. In contrast to a single CSP environment, our technique differs from the common DDR technique in two aspects:1) Tag aggregation algorithm: In stage of commitment, the organizer generates a random $\gamma \in R\mathbb{Z}p$ and returns its commitment H'$_1$ to the verifier. This assures that the verifier and CSPs do not obtain the value of γ. Therefore, our approach guarantees only the organizer can compute the final σ' by using γ and σ' k received from CSPs. After σ' is computed, we need to transfer it to the organizer in stage of "Response1". In order to ensure the security of transmission of data tags, our technique employs a new method, similar to the ElGamal encryption, to encrypt the combination of tags $\prod_{(i,v_i)\in Q_k} \sigma_i^{v_i}$, that is, for $sk = s \in \mathbb{Z}p$ and $P_k = (g, S = g^s) \in \mathbb{G}^2$, the cipher of message m is $\mathcal{C} = (\mathcal{C}_1 = gr, \mathcal{C}_2 = m \cdot s^r)$ and its decryption is performed by $m = C_2 \,.\, C_1^{-s}$ .2) Homomorphic responses: Because of the homomorphic property, the responses computed from CSPs in a multi-cloud can be combined into a single final response. It is obvious that the final response θ received by the verifiers from multiple CSPs is same as that in one simple CSP. This means that our CDDR technique is able to provide a transparent verification for the verifiers. Two response algorithms, Response1 and Response2, comprise an HVR: Given two responses θi and θj for two challenges Qi and Qj from two CSPs, i.e., $\theta i = Response1\ (Qi, \{mk\}\ k \in Ii, \{\sigma k\}\ k \in Ii)$, there exists an efficient algorithm to combine them into a final response θ corresponding to the sum of the challenges $Qi \cup$, that is, $= Response1\ (Qi \cup, \{mk\}\ k \in Ii \cup Ij, \{\sigma k\}\ k \in Ii \cup Ij) = Response2\ (\theta_i, \theta_j)$. For multiple CSPs, the above equation can be extended to $\theta = Response2\ (\{\theta k\}\ \in \mathcal{P})$. More importantly, the HVR is a pair of values $\theta = (\pi, \sigma, \mu)$, which has a constant-size even for different challenges.

4.1 Collision resistant for index-hash hierarchy: In our CDDR technique, the collision resistant of index hash hierarchy is the basis and prerequisite for the security of whole technique, which is described as being secure in the random oracle model. Although the hash function is collision resistant, a

4 SECURITY ANALYSES

We give a brief security analysis of our CDDR construction. This construction is directly derived from multi-prover zero-knowledge proof system (MPZKPS), which satisfies following properties for a given assertion, L: **1) Completeness:** whenever $x \in L$, there exists a strategy for the provers that convinces the verifier that this is the case; **2) Soundness:** whenever $x \notin L$, whatever strategy the provers employ, they will not convince the verifier that $x \in L$; **3) Zero-knowledge:** no cheating verifier can learn anything other than the veracity of the statement. According to existing IPS research [11], these properties can protect our construction from various attacks, such as data leakage attack (privacy leakage), tag forgery attack (ownership cheating), etc. In details, the security of our technique can be analyzed as follow successful hash collision can still be used to produce a forged tag when the same hash value is reused multiple times, e.g., a legitimate client modifies the data or repeats to insert and delete data blocks of outsourced data. To avoid the hash collision, the hash value $\xi(3)$ i,k, which is used to generate the tag σi in CDDR technique, is computed from the set of values $\{\tau i\}$, Fn, Ck, $\{\chi i\}$. As

long as there exists one bit difference in these data, we can avoid the hash collision. As a consequence, we have the following theorem (see Appendix B): Theorem 1 (Collision Resistant): The index-hash hierarchy in CDDR technique is collision resistant, even if the client generates $\sqrt{2p.ln\frac{1}{1-\varepsilon}}$ files with the same file name and cloud name, and the client repeats $\sqrt{2^{L+1}.ln\frac{1}{1-\varepsilon}}$ times to modify, insert and delete data blocks, where the collision probability is at least ε, $\tau i \in \mathbb{Z}p$, and $|Ri| = L$ for $Ri \in \chi i$.

4.2 Completeness property of verification: In our technique, the completeness property implies public verifiability property, which allows anyone, not just the client (data owner), to challenge the cloud server for data integrity and data ownership without the need for any secret information. First, for every available data-tag pair $(F, \sigma) \in (sk, F)$ and a random challenge $Q = (i, vi)\ i \in I$, the verification protocol should be completed with success probability according to the Equation (3), that is, Pr $\left[\langle \sum_{P_k \in p} P_k(F^{(k)}, \sigma^{(k)}) \leftrightarrow O \leftrightarrow V \rangle(pk, \psi) = 1\right] = 1$. In this process, anyone can obtain the owner's public key $pk = (g, h, H_1 = h^{\alpha}, H_2 = h^{\beta})$ and the corresponding file parameter $\psi = (u, \xi^{(1)}, \chi)$ from TTP to execute the verification protocol, hence this is a public verifiable protocol. Moreover, for different owners, the secrets α and β hidden in their public key pk are also different, determining that success verification can only be implemented by the real owner's public key. In addition, the parameter ψ is used to store the file-related information, so an owner can employ a unique public key to deal with a large number of outsourced files.

4.3 Zero-knowledge property of verification: The CDDR construction is in essence a Multi-Prover Zero-knowledge Proof (MP-ZKP) system [11], which can be considered as an extension of the notion of an interactive proof system (IPS). Roughly speaking, in the scenario of MP-ZKP, a polynomial-time bounded verifier interacts with several provers whose computational powers are unlimited. According to a Simulator model, in which every cheating verifier has a simulator that can produce a transcript that "looks like" an interaction between an honest prover and a cheating verifier, we can prove our CDDR construction has Zero-knowledge property.

Theorem 2 (Zero-Knowledge Property): The verification protocol $Proof(\mathcal{P}, V)$ in CDDR technique is a computational zero-knowledge system under a simulator model, that is, for every probabilistic polynomial-time interactive machine $V*$, there exists a probabilistic polynomial-time algorithm $S*$ such that the ensembles $View(\langle \Sigma\ Pk \in \mathcal{P}Pk(F(k), \sigma(k)) \leftrightarrow O \leftrightarrow V* \rangle(pk, \psi))$ and $S*(pk, \psi)$ are computationally indistinguishable. Zero-knowledge is a property that achieves the CSPs' robustness against attempts to gain knowledge by interacting with them. For our construction, we make use of the zero-knowledge property to preserve the privacy of data blocks and signature tags. Firstly, randomness is adopted into the CSPs' responses in order to resist the data leakage attacks (see Attacks 1 and 3 in Appendix A). That is, the random integer λj, is introduced into the response μj, i.e., $\mu j,\ k = \lambda j,\ k + \Sigma\ (i, vi) \in Qkvi \cdot mi,\ j$. This means that the cheating verifier cannot obtain mi, from μj, because he does not know the random integer λj. At the same time, a random integer γ is also introduced to randomize the verification tag σ, i.e., $\sigma' \leftarrow (\Pi\ Pk \in \mathcal{P}\sigma'\ k \cdot R - s\ k)^{\gamma}$. Thus, the tag σ cannot reveal to the cheating verifier in terms of randomness.

4.4 Knowledge soundness of verification: For every data-tag pairs $(F*, \sigma*) \not\in (sk, F)$, in order to prove nonexistence of fraudulent $\mathcal{P}*$ and $O*$, we require that the technique satisfies the knowledge soundness property, that is, Pr $\left[\langle \sum_{P_k \in p^*} P_k(F^{(k)*}, \sigma^{(k)*}) \leftrightarrow O^* \leftrightarrow V \rangle(pk, \psi) = 1\right] \leq \epsilon$, where ϵ is a negligible error. We prove that our technique has the knowledge soundness property by using reduction to absurdity 1: we make use of $\mathcal{P}*$ to construct a knowledge extractor $\mathcal{M}$ [7,13], which gets the common input (pk, ψ) and rewindable blackbox accesses to the prover $P*$, and then attempts to break the computational Diffie-Hellman (CDH) problem in $\mathbb{G}$: given $G, G_1 = G^{a}, G_2 = G^{b} \in R\mathbb{G}$, output $Gab \in \mathbb{G}$. But it is unacceptable because the problem in polynomial-time.

Theorem 3 (Knowledge Soundness Property): Our technique has (t, ϵ') knowledge soundness in random oracle and rewindable knowledge extractor model assuming the (t, ϵ)-computational Diffie-Hellman (CDH) assumption holds in the group $\mathbb{G}$ for $\epsilon' \geq \epsilon$. Essentially, the soundness means that it is infeasible to fool the verifier to accept false statements. Often, the soundness can also be regarded as a stricter notion of unforgeability for file tags to avoid cheating the ownership. This means that the CSPs, even if collusion is attempted, cannot be tampered with the data or forge the data tags if the soundness property holds. Thus, the Theorem 3 denotes that the CDDR technique can resist the tag forgery attacks.

5 PERFORMANCE EVALUATIONS

In this section, to detect abnormality in a low overhead and timely manner, we analyze and optimize the performance of CDDR technique based on the above technique from two aspects: evaluation of probabilistic queries and optimization of length of blocks. To validate the effects of

technique, we introduce a prototype of CDDR-based audit system and present the experimental results.

5.1 Performance Analysis for CDDR Technique: We present the computation cost of our CDDR technique in Table 3. We use $[E]$ to denote the computation cost of an exponent operation in $\mathbb{G}$, namely, gx, where x is a positive integer in $\mathbb{Z}p$ and $g \in \mathbb{G}$ or $\mathbb{G}T$. We neglect the computation cost of algebraic operations and simple modular arithmetic operations because they run fast enough [12]. The most complex operation is the computation of a bilinear map $(\cdot, \cdot)$ between two elliptic points (denoted as $[B]$). Then, we analyze the storage and communication costs of our technique. We define the bilinear pairing takes the form: $(\mathbb{F}pm) \times (\mathbb{F}pkm) \rightarrow \mathbb{F}*pkm$ (The definition given here is from [13], [8]), where p is a prime, m is a positive integer, and k is the embedding degree (or security multiplier). In this case, we utilize an asymmetric pairing: $\mathbb{G}1 \times \mathbb{G}2 \rightarrow \mathbb{G}T$ to replace the symmetric pairing in the original techniques. In Table 3, it is easy to find that client's computation overheads are entirely irrelevant for the number of CSPs. Further, our technique has better performance compared with non-Cooperative numberof CSPs.Further, our technique has better

TABLE 3: Comparison of computation overheads between our CDDR scheme and non-cooperative (trivial) scheme.

	CDDR Scheme	Trivial Scheme
Commitment	$l2$	$cl2$
Challenge1	$2tl0$	$2tl0$
Challenge2	$2tl0/c$	$2tl0$
Response1	$sl0 + 2l1 + lT$	$(sl0 + l1 + lT)c$
Response2	$sl0 + l1 + lT$	$(sl0 + l1 + lT)c$

performance compared with non-Cooperative approach due to the total of computation overheads decrease $3(c-1)$ times bilinear map operations, where c is the number of clouds in a multi-cloud. The reason is that, before the responses are sent to the verifier from c clouds, the organizer has aggregate these responses into a response by using aggregation algorithm, so the verifier only need to verify this response once to obtain the final result. Without loss of generality, let the security parameter κ be 80 bits, we need the elliptic curve domain parameters over $\mathbb{F}p$ with $|p|$ = 160 bits and $m = 1$ in our experiments. This means that the length of integer is $l0 = 2\kappa$ in $\mathbb{Z}p$. Similarly, we have $l1 = 4\kappa$ in $\mathbb{G}1$, $l2 = 24\kappa$ in $\mathbb{G}2$, and $lT = 24\kappa$ in $\mathbb{G}\mathbb{T}$ for the embedding degree $k = 6$. The storage and communication cost of our technique is shown in Table 4. The storage overhead of a file with $(f) = 1M$-bytes is $(f) = n \cdot s \cdot l0 + n \cdot l1 = 1.04M$-bytes for $n = 103$ and $s = 50$. The storage overhead of its index table χ is $n \cdot l0 = 20K$-bytes. We define the overhead rate as $\lambda = (f)\ (f) - 1 = l1\ s \cdot l0$ and it should therefore be kept as low as possible in order to minimize the storage in cloud storage providers. It is obvious that a higher s means much lower storage. Furthermore, in the verification protocol, the communication overhead of challenge is $2t \cdot l0 = 40 \cdot t$-Bytes in terms of the number of challenged blocks t, but its response (response1 or response2) has a constant-size communication overhead $s \cdot l0 + l1 + lT \approx 1.3K$-bytes for different file sizes. Also, it implies that client's communication overheads are of a fixed size, which is entirely irrelevant for the number of CSPs.

TABLE 4: Comparison of communication overheads between our CDDR and non-cooperative scheme

	CDDR Scheme	Trivial Scheme
KeyGen	$3[E]$	$2[E]$
TagGen	$(2n + s)[E]$	$(2n + s)[E]$
Proof(p)	$c[B] + (t + cs+1)[E]$	$c[B] + (t + cs - c)[E]$
Proof(V)	$3[B] + (t + s)[E]$	$3c[B] + (t + cs)[E]$

5.2 Probabilistic Verification: We recall the probabilistic verification of common DDR technique (which only involves one CSP), in which the verification process achieves the detection of CSP server misbehavior in a random sampling mode in order to reduce the workload on the server. The detection probability of disrupted blocks P is an important parameter to guarantee that these blocks can be detected in time. Assume the CSP modifies $e$blocks out of the n-block file, that is, the probabilityof disruptedblocks is $\rho b = en$. Let t be the number of queriedblocks for a challenge in the verification protocol. We have detection probability[2] $(\rho b, t) \geq 1 - \left(\frac{n-e}{n}\right)^t = 1-(1 - \rho b)^t$, Where, $(\rho b, t)$ denotes that the probability P is a function over ρb and t. Hence, the number of queried blocks is $t \approx \frac{\log(1-P)}{\log(1-\rho b)} \approx \frac{P \cdot n}{e}$ for a sufficiently large n and $t \ll n^3$. This means that the number of queried blocks t is directly proportional to the total number of file blocks n for the constant P and e. Therefore, for a uniform random verification in aDDR technique with fragment structure, given a file with $sz = n \cdot s$ sectors and the probability of sector corruption ρ, the detection probability of verification protocol has $P \geq 1 - (1 - \rho)^{sz \cdot \omega}$, where ω denotes the sampling probability in the verification protocol. We can obtain this result as follows: because $\rho b \geq 1 - (1 - \rho)^s$ is the probability of block corruption with s sectors in common DDR technique, the verifier can detect block errors with probability $P \geq 1 - (1 - p_b)^t \geq 1 - ((1 - \rho)^s)^{z \cdot \omega} = 1 - (1 - \rho)^{sz \cdot \omega}$ for a challenge with $t = n \cdot \omega$ index-coefficient pairs. In the same way, given a multi-

cloud $\mathcal{P} = \{Pi\} \in [1, c]$, the detection probability of CDDR technique has $(sz, \{\rho k, rk\} \in \mathcal{P}, \omega) \geq 1 - \prod_{Pk\in\mathcal{P}}((1 - \rho k)^{s})r_k^{.\omega} = 1 - \prod_{Pk\in\mathcal{P}}(1 - \rho k)^{sz.r_{k\cdot\omega}}$, where r_k denotes the proportion of data blocks in the k-th CSP, ρk denotes the probability of file corruption 2. Exactly, we have $P = 1-(1-\frac{e}{n}) \cdot (1-\frac{e}{n-1}) \cdots (1-\frac{e}{n-t+1})$.

Since $1-\frac{e}{n} \geq 1-\frac{e}{n-i}$ for $i \in [0, t-1]$, we have $P = 1-\prod_{i=0}^{t-1}(1-\frac{e}{n-i}) \geq 1-\prod_{i=0}^{t-1}(1-\frac{e}{n}) = 1-(1-\frac{e}{n})^t$.

3. In terms of $(1-\frac{e}{n})^t \approx (1-\frac{e.t}{n})$, we have $P \approx 1-(1-\frac{e.t}{n}) = \frac{e.t}{n}$. In the k-th CSP and $rk\cdot\omega$ denotes the possible number of blocks queried by the verifier in the k-th CSP. Furthermore, we observe the ratio of queried blocks in the total file blocks w under different detection probabilities. Based on above analysis, it is easy to find that this ratio holds the

TABLE 5: The influence of s, t under the different corruption probabilities ρ and the different detection probabilities P

$\mathcal{P}$	{0.1,0.2,0.01}	{0.01,0.02,0.001}	{0.001,0.002,0.0001}	{0.0001,0.0002,0.00001}
r	{0.5,0.3,0.2}	{0.5,0.3,0.2}	{0.5,0.3,0.2}	{0.5,0.3,0.2}
0.8/ 3	4 /7	20/ 23	62/ 71	71/202
0.85 /3	5 /8	21/ 26	65/ 79	79/214
0.9 /3	6/ 10	20 /28	73 /87	87/236
0.95 /3	8/ 11	29/ 31	86/ 100	100/267
0.99 /4	10/ 13	31/ 39	105 /119	119/345
0.999 /5	11/ 16	38 /48	128/ 146	146/433

equation$w \approx \frac{\log(1-P)}{sz \cdot \Sigma Pk\in\mathcal{P}\ rk \cdot \log(1-\rho k)}$. When this probability ρk is a constant probability, the verifier can detect sever misbehavior with a certain probability P by asking proof for the number of blocks $t \approx \log(1-P)\ s.\log(1-\rho)$ for DDR or for$t \approx \frac{\log(1-P)}{s \cdot \Sigma Pk\in\mathcal{P}\ rk \cdot \log(1-\rho k)}$CDDR, where $t = n\cdot w = \frac{sz\cdot w}{s}$. Note that, the value of t is dependent on the total number of file blocks n [2], because it is increased along with the decrease of ρk and $\log(1-\rho k) < 0$ for the constant number of disrupted blocks e and the larger number n. Another advantage of probabilistic verification based on random sampling is that it is easy to identify the tampering or forging data blocks or tags. The identification function is obvious: when the verification fails, we can choose the partial set of challenge indexes as a new challenge set, and continue to execute the verification protocol. The above search process can be repeatedly executed until the bad block is found. The complexity of such a search process is $(\log n)$.

5.3 Parameter Optimization: In the fragment structure, the number of sectors per block s is an important parameter to affect the performance of storage services and audit services. Hence, we propose an optimization algorithm for the value of s in this section. Our results show that the optimal value can not only minimize the computation and communication overheads, but also reduce the size of extra storage, which is required to store the verification tags in CSPs. Assume ρ denotes the probability of sector corruption. In the fragment structure, the choosing of s is extremely important for improving the performance of the CDDR technique. Given the detection probability P and the probability of sector corruption ρ for multiple clouds $\mathcal{P} = \{Pk\}$, the optimal value of s can be computed by $\min s\in\mathbb{N}\{\frac{\log(1-P)}{\Sigma Pk\in\mathcal{P}\ rk\cdot\log(1-\rho k)}\cdot\frac{a}{s} + b\cdot s + c\}$, where $a\cdot t + b\cdot s + c$ denotes the computational cost of verification protocol in DDR technique, $a, b, c \in \mathbb{R}$, and c is a constant. This conclusion can be obtained from following process: Let $sz = n\cdot s = (f)/l_0$. According to above-mentioned results, the sampling probability holds $w \geq \frac{\log(1-P)}{sz\cdot\Sigma Pk\in\mathcal{P}\ rk\cdot\log(1-\rho k)} = \frac{\log(1-P)}{n\cdot s\cdot\Sigma Pk\in\mathcal{P}\ rk\cdot\log(1-\rho k)}$. In order to minimize the computational cost, we have $\min s\in\mathbb{N}\ \{a\cdot t + b\cdot s + c\} = \min s\in\mathbb{N}\ \{a\cdot n\cdot w + b\cdot s + c\} \geq \min s\in\mathbb{N}\{\Sigma\log(1-P)\ Pk\in\mathcal{P} rk\cdot\log(1-\rho k)\ as + b\cdot s + c\}$. Where$rk$ denotes the proportion of data blocks in the k-th CSP, ρk denotes the probability of file corruption in the k-th CSP. Since $\frac{a}{s}$ is a monotone decreasing function and $b\cdot s$ is a monotone increasing function for $s > 0$, there exists an optimal value of $s\in\mathbb{N}$ in the above equation. The optimal value of s is unrelated to a certain file from this conclusion if the probability ρ is a constant value. For instance, we assume a multi-cloud storage involves three CSPs $\mathcal{P} = \{P1, P2, P3\}$ and the probability of sector corruption is a constant value $\{\rho 1, \rho 2, \rho 3\} = \{0.01, 0.02, 0.001\}$. We set the detection probability P with the range from 0.8 to 1, e.g., $P = \{0.8, 0.85, 0.9, 0.95, 0.99, \text{and } 0.999\}$. For a file, the proportion of data blocks is 50%, 30%, and 20% in three CSPs, respectively, that is, $r1 = 0.5$, $r2 = 0.3$, and $r3 = 0.2$. In terms of Table 3, the computational cost of CSPs can be simplified to $t + 3s+9$. When s is less than the optimal value, the computational cost decreases evidently with the increase of s, and then it raises when s is more than the optimal value. More accurately, we show the influence of parameters, $sz\cdot w$, s, and t, under different detection probabilities in Table 6. It is easy to see that computational cost rises with the increase of P. Moreover, we can make sure the sampling number of challenge with followingConclusion**:** Given the detection probability P, the probability of sector corruption ρ, and the number of

sectors in each block s, the sampling number of verification protocol are a constant$t = n \cdot w \geq \frac{\log(1-P)}{s \cdot \Sigma Pk \in \mathcal{P}\ rk \cdot \log(1-\rho k)}$ for different files. Finally, we observe the change of $s$under differentρ and P. The experimental results are shown in Table 5. It is obvious that the optimal value of s rises with increase of P and with the decrease ofρ. We choose the optimal value of s on the basis ofρ. settings and system requisition. For NTFS format,

TABLE 6: The influence of parameters under different detection probabilities P ($\mathcal{P}$ = {ρ1, ρ2, ρ3} = {0.01, 0.02, 0.001}, {r1, r2, r3} = {0.5, 0.3, 0.2})

P	0.8	0.85	0.9	0.95	0.99	0.999
$sz \cdot w$	142.60	168.09	204.02	265.43	408.04	612.06
s	7	8	10	11	13	16
t	20	21	20	29	31	38

we suggest that the value of s is 200 and the size of block is 4KBytes, which is the same as the default size of cluster when the file size is less than 16TB in NTFS. In this case, the value of s ensures that the extra storage doesn't exceed 1% in storage servers.

5.4 CDDR for Integrity Audit Services: Basedon our CDDR technique, we introduce audit system architecture for outsourced data in multiple clouds by replacing the TTP with a third party auditor (TPA) in Figure 1. In this architecture, this architecture can be constructed into a visualization infrastructure of cloud-based storage service [1]. In Figure 3, we show an example of applying our CDDR technique in Hadoop distributed filesystem (HDFS)[4], with a distributed, scalable, and portable file system [9]. HDFS' architecture is composed of NameNode and DataNode, where NameNode maps a file name to a set of indexes of blocks and DataNode indeed stores data blocks. To support our CDDR technique, the index-hash hierarchy and the metadata of NameNode should be integrated together to provide an enquiry service for the hash value$\xi_{i,k}^{(3)}$, or index-hash record χi.Based on the hash value, the clients can implement the verification protocol via CDDR services. Hence, it is easy to replace the checksum methods with the CDDR technique for anomaly detection in current HDFS. To validate the effectiveness and efficiency of our proposed approach for audit services, we have implemented a prototype of an audit system. We simulated the auditservice and the storage service by using

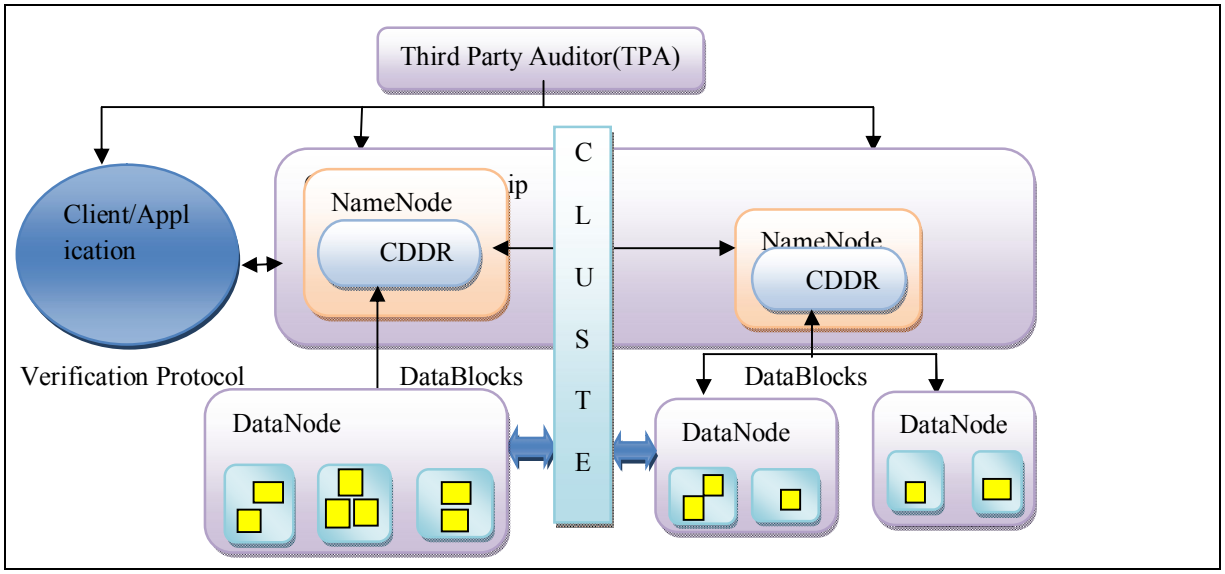


Figure 3: Applying CDDR Technique in Hadoop distributed file system (HDFS)

two local IBM servers with two Intel Core 2 processors at 2.16 GHz and 500M RAM running Windows Server 2003. These servers were connected via 250 MB/sec of network bandwidth. Using GMP and PBC libraries, we have

implemented a cryptographic library upon which our technique can be constructed. This C library contains approximately 5,200 lines of codes and has been tested on both Windows and Linux platforms. The elliptic curve utilized in the experiment is a MNT curve, with base field size of 160 bits and the embedding degree 6. The security level is chosen to be 80 bits, which means $|p| = 160$. Furthermore, the proportions of data blocks in each CSP have greater influence on the computation costs of "challenge" and "response" processes.

6 CONCLUSIONS

We make three key contributions in this paper, first we have proposed a Cooperative DDR technique to support dynamic scalability on multiple storage servers, and second we presented the construction of an efficient DDR technique for distributed cloud storage Based on homomorphic verifiable response and hash index hierarchy. Third we also showed that our technique provided all security properties required by zeroknowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds. Furthermore, we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work, we would extend our work to explore more effective CDDR constructions. For a practical point of view, we still need to address some issues about integrating our CDDR technique smoothly with existing systems, for example, how to match index structure with cluster-network model, how to match index hash hierarchy with HDFS's two-layer name space, and how to dynamically update the CDDR parameters according to HDFS' specific requirements. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such an issue to provide the support of variable-length block verification.

7 ACKNOWLEDGEMENT

The work on "**Cooperative demonstrable data retention for integrity verification in multi-cloud Storage"** was supported by many members. We are highly obliged and thankful to almighty who has provided us with the opportunity to thank all the kins who stood by us in the process of working on this project. First of all we would like to thank **Mr. Shubham Srivastava**our project guide andwho was of utmost help to us throughout the proceedings. Further, we would like to thank Head of Computer Science department of Institute of Technology and Management **Mr. Rajeev Ranjan Kumar Tripathi**, who has been a great help and an inspiration in carrying out the present work successfully. So it's our pleasure to present a cordial thanks to him.

8 REFERENCES

[1]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[2]. A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[3]. B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, "Virtual infrastructure management in private and hybrid clouds," IEEE Internet omputing, vol. 13, no. 5, pp. 14–22, 2009.

[4]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communi - cation netowrks, SecureComm, 2008, pp. 1–10.

[5]. C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, ser. Lecture Notes in ComputerScience, M. Backes and P. Ning, Eds., vol. 5789. Springer,2009, pp. 355–370.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamicaudit services for integrity verification of outsourcedstorages in clouds," in SAC, W. C. Chu, W. E. Wong, M. J.Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[9] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availabilityand integrity layer for cloud storage," in ACM Conference onComputer and Communications Security, E. Al-Shaer, S. Jha, andA. D. Keromytis, Eds. ACM, 2009, pp. 187–198.

[10] Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievabilityvia hardness amplification," in TCC, ser. Lecture Notes inComputer Science, O. Reingold, Ed., vol. 5444. Springer, 2009,pp. 109–127.

[11] L. Fortnow, J. Rompel, and M. Sipser, "On the power of multiprover interactive protocols," in Theoretical Computer Science, 1988, pp. 156–161.

[12] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, Orlando, Florida, USA, October 15-18, 2011, pp. 197–206.

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing".

International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 208 - 213, 2013, ISSN: 2319–8656

Automatic Seed Classification by Shape and Color Features using Machine Vision Technology

Naveen Pandey
CSE Department
ASET, Amity University
Noida, India

Satyanarayan Krishna
CSE Department
ASET, Amity University
Noida, India

Shanu Sharma
CSE Department
ASET, Amity University
Noida, India

Abstract: : In this paper the proposed system uses content based image retrieval (CBIR) technique for identification of seed e.g. wheat, rice, gram etc. on the basis of their features. CBIR is a technique to identify or recognize the image on the basis of features present in image. Basically features are classified in to four categories 1.color 2.Shape 3. texture 4. size .In this system we are extracting color, shape feature extraction. After that classifying images in to categories using neural network according to the weights and image displayed from the category for which neural network shows maximum weight. category1 belongs to wheat and category2 belongs to gram. Experiment was conducted on 200 images of wheat and gram by using Euclidean distance(ED) and artificial neural network techniques. From 200 images 150 are used for training purpose and 50 images are used for testing purpose. The precision rate of the system by using ED is 84.4 percent By using Artificial neural network precision rate is 95 percent.

Keywords: Features, Color, Shape, CBIR, Classification, ANN, Euclidean distance

1. INTRODUCTION

The application of machine vision is very important in agricultural industry. Seed analysis and classification can provide addaitional knowledge in their production, seeds quality control and in impurities identification. Generally these activities are performed by specialists by visually inspecting each sample, which is a very tedious and time consuming task [1]. So, automation is required in this field. Now a day, computer vision technology is applied in a large variety of fields to increase the efficiency of the work. So, This paper uses machine vison technique for the recognition aspect of the said problems[2].

In this paper a system is designed to recognize the different types of grains by their images on the basis of their features using content based image retrieval technique. Content-based image retrieval is a technique which uses visual contents to search images from large scale image databases according to users' interests. CBIR technique is further explained in next section. The proposed technique is based on color and shape features. And for classification two approaches are used and then compared. First classification is done through Artificial Neural Network(ANN) and second is done through finding the mininmum Euclidean Distance between the features of two images.

2. CONTENT BASED IMAGE RETRIEVAL

There are basically two types of image retrieval techniques 1.Text based image retrieval 2.Content based image retrieval. In the text based image retrieval technique, images are indexed on the basis of heading or topic, description, keyword. Texture based images can not be retrieved by text based query. To overcome this problem of text based image retrieval and reducing human effort in indexing process[3].
Content based image retrieval is a best technique to retrieve an image because it reduces the image indexing and texture based problems. efficiency of CBIR system can be improved by providing the feedback for a particular image which is not recognized by the system.

In a general CBIR system different types of features of image database is calculated and feature database is created. When the random test or input or query image is given to the system then all the defined features is extracted for that particular image and stored in feature vector.

Then image retrieval is done by comparing the similarity between the query feature vector and different feature vectors of feature database.

And then the image which has closest feature set as the query image is displayed as the result. The general architecture of CBIR system is shown in Fig 1[3].

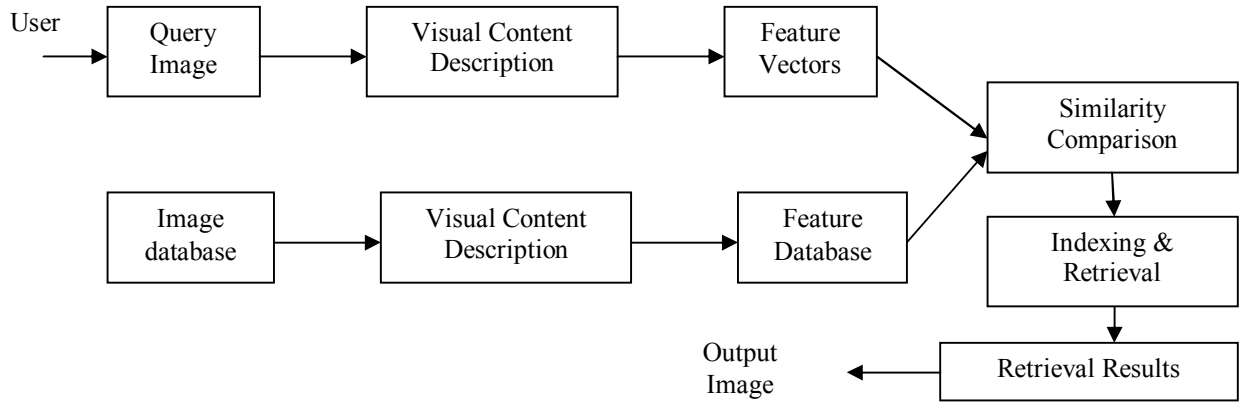


Figure 1. General architecture of CBIR

3. RELATED WORK

There are many researchers who develop a variety of seed image recognition system by applying different-different classification techniques e.g. a artificial neural network, a Euclidean distance technique, Histogram Intersection Distance etc. The details of each technique given below-

3.1 Euclidean Distance Method

Benjamaporn Lurstwut and chomtip pornpanomchai developed a method which uses shape ,size ,color , texture feature extraction with the Euclidean distance technique to classify seed Images. The system's recognition rate was 95.1 % for trained dataset and 64.0 percent for unknown in untrained dataset [4].

Dr. H.B.Kekre, Mr. Dhirendra Mishra, Ms. Stuti Narula and Ms. Vidhi Shah applied the color feature extraction to recognize different kinds of image. They applied Euclidean distance technique with The different images of the same class give results varied from 30% to 60% for a database of size 300 [5].

Poulami Haldar and Joydeep Mukherjee used Euclidean matrix method to calculate the distance vector. System provides overall accuracy 87.50 % for the images of different class [6].

3.2 Artificial Neural Network

Dayanand Savakar designed algorithms which is used to extract 18 color and 27 texture features from food grains. For the Recognition and Classification of Similar Looking

Food Grain Images this system uses artificial neural network. Recognition of Mustard is about 87% and for Soya is 78% using color feature and on the basis of texture feature extraction maximum classification rate is 84% [7].

Ai-Guo OuYang, Rong-jie Gao, Yan-de Liu,,Xu-dong Sun, Yuan-yuan Pan and Xiao-ling Dong designed a system in which color features in RGB and color space is computed. A back feed forward neural network trained to identify rice seed 86.5 % rice seeds were identified by the system [8].

3.3 Histogram Intersection Distance

Manimala Singha and K.Hemachandran used histogram intersection distance for feature similarity matching. Experiment performed on standard "Wang Database" containing 1000 image. In it texture and color feature extracted through wavelet transformation and color histogram [9].

3.4.Support vector machine

Ying Liua, Dengsheng Zhanga, Guojun Lua and Wei-Ying Mab used SVM in their system because of SVM has been used for object recognition, text classification, etc. After using SVM in that system an improvement of 10% in

retrieval accuracy is obtained compared with SVM (400 images for training) with much fewer training data [10].

b) Kantip Kiratiratanapruk and Wasin Sinthupinyo classify defects of corn seed in more than ten categories and extracted color, texture feature. They used SVM as type classifier. Accuracy of the system is 96.5 % for normal seed type and 86.5 % in the case of defect seed(group) types [1].

On the basis of above literature reviews it has been observed that ANN and Euclidean distance method of classification can provide better results with shape and color features.

4. PROPOSED METHODOLOGY

The general methodology of the proposed system is shown in Fig 2, which is further explained in subsections.

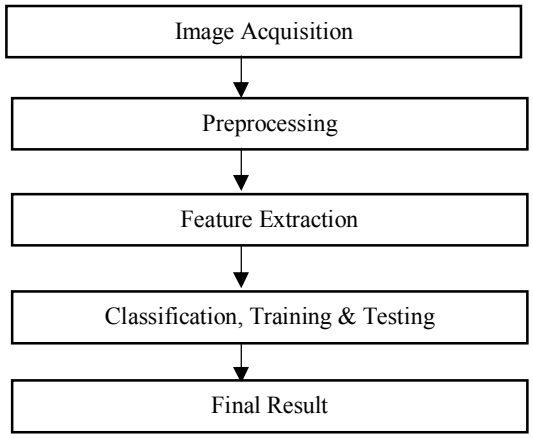


Figure 2. Algorithm of Proposed System

4.1 Image acquisition

12 mega pixel camera is used for taking the images of wheat, gram and pulse. Distance between seed and camera is almost equal to 14 centimeters.

4.2 Image preprocessing: Preprocessing operation includes the following steps-

4.2.1 Image resizing: The input images captured by different cameras may have different sizes which can affect the result, so initial resizing is necessary.

4.2.2 RGB to Gray Scale Conversion: Equation 1 is used to convert the RGB value of a pixel into its gray value.

gray=.2989*R+.5870*G*.1140*B

4.2.3 Gray to Binary Image Conversion: Binarization is done using otsu method, it can be done using graythresh function in MATLAB.

4.2.4 Morphological Processing: Closing and Filling operations are performed using a disk type structuring elements of radius 2 to fill any holes in the images.

The steps of pre-processing on an input of wheat is shown in Fig 3.

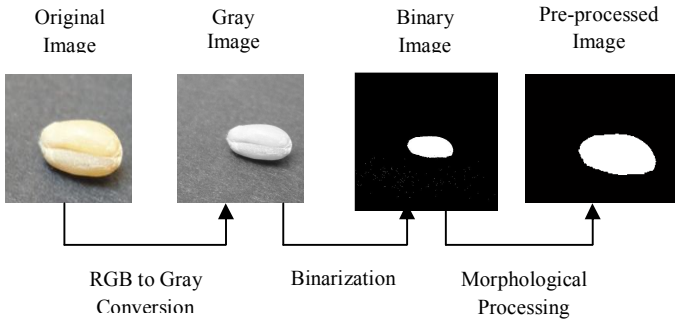


Figure 3. Pre-processing on an Input Image

4.3.Feature extraction

Following shape and color features are extracted for each Input Image.

4.3.1 Shape feature extraction: Following shape features are considered.

Seed roundness : Roundness of each seed is calculated w.r.t circle, means when the value of roundness of any particular seed is .9 then it's almost round. Roundness can be calculated by following equation.

R = 4*pi*area/P^2, where P is the perimeter of the seed.

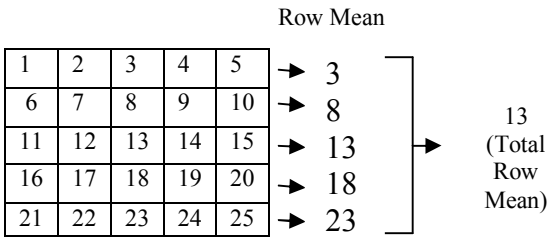
4.3.2 Color feature extraction

Row mean and column mean: For each Red, Green and Blue plane row and column mean is calculated by following step.

a)Three color planes Red, Green ,Blue are separated and step 2 to 4 is performed on each plane.

b) For each plane row mean and column mean of colors are calculated.

Pictorially the row and column mean is calculated as follows [5]:



c) The row mean of all three planes are stored as 3 new features in feature vector.

Dominant color: Dominant Color is calculated for each Red, Green and Blue Plane by their histogram.

Histogram is representation of the occurrence of relative frequencies of various gray levels in an image. Dominant color is that gray level which has the maximum occurrence in the image. 3 more features are then added in the feature vector.

Median: It can be used to determine the value of intensity level of pixel which is separating high intensity value pixel from low intensity value pixel. Three median values are calculated for Red, Green and Blue Planes.

Some other statistical features are also calculated [11].

Standard Deviation: In the digital image processing it shows variation from standard or expected value. It is calculated for each plane by following function in MATLAB.

std((std(Red,0,1))',0,1);

Covariance: It is a positive number.It is the measure of change in two variable(random numbers) together.

diag(cov(diag(cov(Red)))')

Kurtosis: It tells about the shape of probability distribution function of a random number.high curtosis value is good for system because of ,it shows low noise and low resolution.

kurtosis((kurtosis(Red))')

Skewness: The value of skewness can be positive, negative, zero or may be undefined. Negative skewness shows that more values lies to the right of the mean, positive skewness means more values lies to the left of mean and zero skewness shows values are evenly distributed on both side of mean.

skewness((skewness(Red))')

Moment: The central first moment is zero and second central moment is calculated by using a divisor of N instead of N-1.
N -> length of vector or number of rows in matrix.

moment((moment(Red,3))',3)

4.4 Image Recognition

Image recognition is done using both ANN and Euclidean distance method.

Euclidean Distance Method

In this method Euclidean distance is calculated between a feature vector of test image and the feature file of all sample images stored in the database. The Euclidean distance can be calculated by using equation:

$$ED = \sqrt{\sum_{j=1}^{m}(c_j - b_j)^2}$$

Where ED is the Euclidean distance ,

m is number of features,

c_j is the value of feature j stored in the predefined database,

b_j is the value of feature

Artificial neural network

A neural network, illustrated in Fig. 4, consists of units (neurons), arranged in layers, which convert an input vector into some output. Each unit takes an input, applies a (often nonlinear) function to it and then passes the output on to the next layer. Generally the networks are defined to be feed-forward: a unit feeds its output to all the units on the next layer, but there is no feedback to the previous layer. Weightings are applied to the signals passing from one unit to another, and it is these weightings which are tuned in the training phase to adapt a neural network to the particular problem at hand. This is the learning phase.

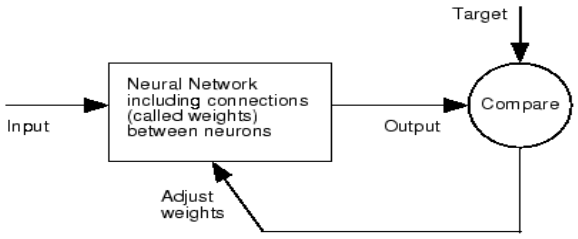


Figure 4. A typical Neural Network

Then the learned network with new weights is used for testing purpose.

5. EXPERIMENTAL RESULTS

The system is developed using MATLAB (R2011a), in this system 200 samples images of three different grains are taken by camera, from which 150 images are used for training phase and 50 for testing phase. Then the total 25 features of 150 sample images are calculated stored in a single feature file "feature_file.mat" using Matlab , this mat file stores features in a 25x150 array.

In classification using ANN method , first training of network is done using the previously generated "feature_file.mat" of 150 images , with 10 hidden neurons. Final application gives an option to user to select a test image form the rest 50 testing images and then the 25 features of this test image is calculated and stored in a 'test.mat' file, which is a 25x1 array. This "test.mat" file is then passed to the trained network. It gives 95% accuracy.

Euclidean Distance methods outputs that image from training set which has the closest features of test image. It gives 84.4 % accuracy.

Below Table 1 shows the values of different features for one test image of wheat.

Table 1. 25 Different feature values of Test Image

Roundness	.605
Red_row_mean	135.6
Green_row_mean	135.5
Blue_row_mean	133.5
Red_Dominatnt_color	144
Green_Dominat_color	144
Blue_Dominat_color	142
Red_Median	139
Green_Median	139
Blue_Median	137
Red_Std_Deviation	13.5
Green_Std_Deviation	12.0
Blue_Std_Deviaion	8.6
Red_Covariance	527920
Green_Covariance	380240
Blue_Covariance	144390
Red_Kurtosis	10.15
Green_Kurtosis	6.21
Blue_Kurtosis	1.97
Red_Skewness	1.05
Green_Skewness	1.00
Blue_Skewness	1.7
Red_Moment	57808420356433.4
Green_Moment	19499436210162.3
Blue_Moment	833492646434.140

And Fig 5. shows the final result, which has the test image and the closest matched image.

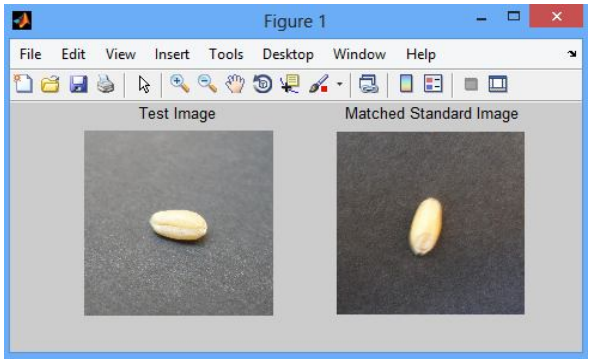


Figure 5. Final result of application with matched image

6. CONCLUSION

In the proposed system 25 shape, color and statistical features are calculated. Image recognition is done using both techniques Euclidean distance and artificial neural network. System is 95 % accurate using ANN and 84.4 % accurate using Euclidean distance method.

7. ACKNOWLEDGEMENTS

We would like to thank our guide Ms. Shanu Sharma for their guidance and feedback during the course of the project. We would also like to thank our department for giving us the resources and the freedom to pursue this project.

8. REFERENCES

[1] Kantip Kiratiratanapruk and Wasin Sinthupinyo. 2011. Color And Texture For Corn Seed Classification By Machine Vision, International Symposium on Intelligent Signal Processing & Communication Systems(ISPACS). pp 1-5.

[2] Adjemout Ouiza, Hammouche Kamal and Diaf Moussa. 2007. Automatic seed recognition by size, form and texture features, International Symposium on Signal Processing and its applications,(ISSPA). pp 1-4.

[3] (2013),"Tutorial on CBIR", [Online] Available: www.cs.bgu.ac.il/~icbv061/...2006.../CBIR_Presentation.ppt

[4] Benjamaporn Lurstwut ,Chomtip Pornpanomchai, "Plant Seed Image Recognition System(PSIRS)", IACSIT International Journal of Engineering & Technology, 2011. pp. 600-605.

[5] Dr. H.B.Kekre ,MR.Dhirendra Mishra, MS. Stuti narula and MS. Vidhi Shah , " Color Feature Extraction For Cbir", International Journal of Engineering Science & Technology(IJEST), 2011. pp. 8357-8365.

[6] Poulami Haldar and Joydeep Mukherjee, "Content based Image Retrieval using Histogram,Color and Edge", International Journal of Computer Applications, 2012. pp 25-31.

[7] Dayanand Savakar , "Recognition and Classification of Similar Looking Food Grain Images using Artificial Neural Networks", Journal of Applied Computer Science & Mathematics, 2012. pp 61-65.

[8] Ai-Guo OuYang, Rong-jie Gao, Yan-de Liu,Xu-dong Sun, Yuan-yuan Pan. 2010. An Automatic Method For Identifying Different Variety Of Rice Seeds Using Machine Vision Technology, Sixth International Conference on Natural Computation. pp 84-88.

[9] Manimala Singha and K. Hemachandran, "Content Based Image Retrieval using Color and Texture", Signal & Image processing: An International Journal, 2012. pp 39-57.

[10] Ying Liua, Dengsheng Zhanga, Guojun Lua and Wei-Ying Mab. 2007. A survey of content-based image retrieval with high-level semantics", Pattern Recognition, Elsevier. pp 262-282.

[11] Vijay Kumar, Priyanka Gupta, "Importance of Statistical Measures in Digital Image Processing", International Journal of Emerging Technology and Advanced Engineering, 2012. pp. 56-62.