International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 6- 15, 2013

Risk-Aware Response Mechanism with Extended D-S theory

G.Nirmala
Erode Sengunthar Engineering College
Thudupathi,Erode,Tamil Nadu

T. Kalai selvi
Erode Sengunthar Engineering College
Thudupathi,Erode,Tamil Nadu

Abstract: Mobile Ad hoc Networks (MANET) are having dynamic nature of its network infrastructure and it is vulnerable to all types of attacks. Among these attacks, the routing attacks getting more attention because its changing the whole topology itself and it causes more damage to MANET. Even there are lot of intrusion detection Systems available to diminish those critical attacks, existing causesunexpected network partition, and causes additional damages to the infrastructure of the network , and it leads to uncertainty in finding routing attacks in MANET. In this paper, we propose a adaptive risk-aware response mechanism with extended Dempster-Shafer theory in MANET to identify the routing attacks and malicious node. Our techniques find the malicious node with degree of evidence from the expert knowledge and detect the important factors for each node.It creates black list and all those malicious nodes so that it may not enter the network again

Keywords: Mobile Adhoc Network, Black list, Aodv, Dempster Shafer theory;

1.INTRODUCTION

MOBILE Ad hoc Networks (MANET) introducing a communication in all environments without any predefined infrastructure or centralized administration Therefore, MANET is suitable for adverse and hostile environments where central authority point is not necessary. The important characteristic of MANET is the dynamic nature of its network topology which is frequently changing due to the unpredict- able mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

In Existing Wang proposed a na¨ıve fuzzy cost sensitive intrusion response solution for MANET. Their cost model took subjective knowledge, objective evidence, and logical reasoning. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation

In this paper, we seek a way to bridge this gap by using Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty .D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields , where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. First, it enables us to represent both subjective and objective evidences with basic probability assignment and belief function. Second, it supports Dempster's rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in, Dempster's rule of combination has several limitations, such as treating evidences equally without differentiating each evidence and considering priorities among them.

To address these limitations in MANET intrusion response scenario, we introduce a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model. In this paper, we propose a risk-aware responsemechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation meth- od. Our risk-aware approach is based on the extended D-S evidence model. In order to evaluate our mechanism, we perform a series of simulated experiments with proactive MANET routing protocol, Adhoc On Demand Distance Vector Routing Protocol (AODV).In addition, we attempt to demonstrate the effectiveness of our solution.

The major contributions of this paper are summarizedas follows:

We formally propose an extended D-S evidence model with importance factors and articulate ex- pected properties for Dempster's rule of combina- tion with importance factors (DRCIF). Our Dempster's rule of combination with importance factors is no associative and weighted, which has not been addressed in the literature.

We propose an adaptive risk-aware response me- chanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechan- ism allows us to systematically cope with MANET routing attacks.

2.Background

2.1 AODV Protocol

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources AODV builds routes using a route request / route reply query cycle.

When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hopcount, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

2.2.Routing Attacks:

In AODV, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. first, it changes the contents of a discovered route, modifies a route reply message, and causes the packet to be dropped as an invalid packet; then, it validates the route cache in other nodes by advertising incorrect paths, and refuses to participate in the route discovery process; and finally, it modifies the contents of a data packet or the route via which the data packet is supposed to travel or behave normally during the route discovery process but is dropped. Thus all types of fabrication attacks can occurs.

3. EXTENDED DEMPSTER SHAFER THEORY OF EVIDENCE

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. However, previous research efforts identify several limitations of the Dempster's rule of combination

1. Associative. For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in , a nonassociative combination rule is necessary for many cases.

2. Nonweighted. DRC implies that we trust all evidences equally. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence.

We proposed rules to combine several evidences presented sequentially for the first limitation and suggested a weighted combination rule to handle the second limitation. We evaluate our response mechanism against representative attack scenarios . The weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations. The DRC technique will be taken for finding the attacks and its counter measures and thus will be putting the attacker in a black list to avoid the same attacker while entering the network later.

3.1 Importance Factors and Belief Function

In D-S theory, propositions are represented as subsets of a given set. Suppose e is a finite set of states, and let 2e denote the set of all subsets of e. D-S theory calls e, a frame of discernment. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.

Definition 1. Importance factor (IF) is a positive real number associated with the importance of evidence. IF s are derived from historical observations or expert experiences.

Definition 2. An evidence E is a 2-tuple (m, I F), where m describes the basic probability assignment . Basic prob- ability assignment function m is defined as follows:

$$m(\phi)=0 \text{ ---------------> (1)}$$

and

$$\Sigma\ m(A)=1 \text{ ----------------->(2)}$$

The Belief Function is as follows

$$Bel(A)= \ \Sigma\ m(B) \text{ ------------->(3)}$$

3.2 Expected Properties for Our Dempster's Rule of Combination

The proposed rule of combination with importance factors should be a superset of Dempster's rule of combination. In this section, we describe four properties that a candidate Dempster's rule of combination with importance factors should follow. Properties 1 and 2 ensure that the combined result is a valid evidence. Property 3 guarantees that the original Dempster's Rule of Combination is a special case of Dempster's Rule of Combination with importance factors, where the combined evidences have the same priority. Property 4 ensures that importance factors of the evidences are also independent from each other.

Property 1. No belief ought to be committed to q in the result of our combination rule

$$m'(\phi)=0 \text{ ---------->(4)}$$

Property 2. The total belief ought to be equal to 1 in the result of our combination rule

$$\Sigma m'(A)=1 \text{ ---------->(5)}$$

Property 3. If the importance factors of each evidence are equal, our Dempster's rule of combination should be equal to Dempster's rule of combination without importance factors

$$m'(A,IF1,IF2)=m(A) \text{ if } IF1 =I\ F2$$

Property 4. Importance factors of each evidence must not be exchangeable.

$$m'(A,IF1,IF2)=m'(A,IF1,IF2) \text{ If } (IF1=IF2)$$

we propose a Dempster's rule of combinationwith importance factors. We prove our combination rule

$$m'(A,IF1,IF2)= m(A\ )\text{if } IF1 =I\ F2$$

4. Theorem Dempster's rule of combination

Belief to either of these evidences is less than 1. This is straightforward since if our belief to one evidence is 1 or 0.

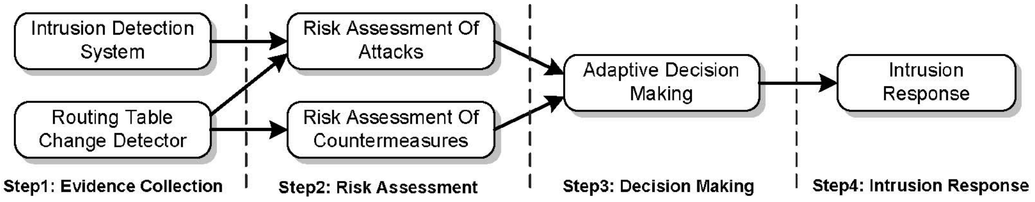

Intrusion Detection System
Routing Table Change Detector
Risk Assessment Of Attacks
Risk Assessment Of Countermeasures
Adaptive Decision Making
Intrusion Response
Step1: Evidence Collection
Step2: Risk Assessment
Step3: Decision Making
Step4: Intrusion Response

Figure. 1. Risk-aware response mechanism

Proof. It is obvious that our proposed DRCIF holds Properties . We prove that our proposed DRCIF also holds Properties

Property:

Our evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We propose a unified analysis approach for evaluating the risks of both attack (RiskA) and countermeasure (RiskC).We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective evidence, we analyze different routing table modification cases. There are three basic items in AODV routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be missed, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Two independent evidences named E1 and E2 , respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, in same time, our belief to either of these evidences is less than 1. This is straightforward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes.

4.1 Evidence Collection

Our proposed DRCIF is nonassociative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm sup- ports this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naïve fuzzy-based method. The algorithm for combination of multiple evi- dences is constructed as follows:

Algorithm 1.MUL-EDS-CMB

OUTPUT: One evidence

```
jEpj j sizeof(Ep);
While jEpj > l do
Pick two evidences with the least 1F in
Ep, named El and E2 ;
Combine these two evidences,
E j hml m2 , (1Fl + 1F2 )/2);
Remove El and E2 from Ep;
Add E to Ep;
end
```

The Evidences are collected from the IDS and priorities assigned to each of them,thus by adding together we get the total evidences. Risk Assessment is made with attacks and its effects. Adaptive decision is taken that the node is attacker or not by comparing with with the threshold values namely upper risk tolerance and lower risk tolerance and finally Intrusion response will send a alert to other nodes.

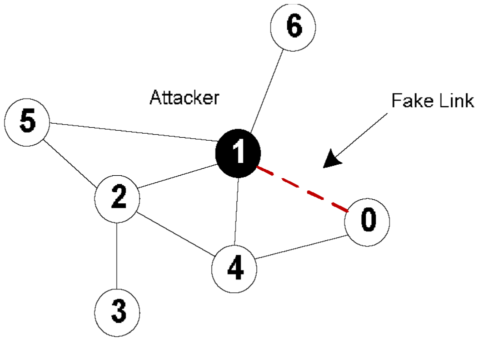


Figure. 2. Example scenario.

Intrusion response. With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isola- tion, are carried out to mitigate attack damages in a distributed manner.

4.2 Response to Routing Attacks

In our approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation. Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In AODV routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

For example, in Fig. 2, Node 1 behaves like a malicious node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are required. In our risk-aware response mechanism, we adopt two types of time-wise isolation responses: temporary isolation and permanent isolation

4.3 Risk Assessment

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence.

Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table. Link with- holding attack or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node possible for this.

Evidence 4: Changing entry II. This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. We believe the impacts on the node communication should be very minimal in this case

Evidence 5: Changing entry III. This evidence points out the proportion of changing entries in the case of different next hop(not the malicious node and the different distance.

The probability assignments of evidences 2 to 5 1-d means the maximul value of the belief that means the status of the MANET is secure.

m(1nsecure) j c, c is confidence given by 1DS

m(Secure) j 1 — c (

(Secure, 1nsecure) j O

4.3.1 Combination of Evidences

For simplicity, we call the combined evidence for an attack, EA and the combined evidence for a countermeasure, EC Thus, BelA (1nsecure) and BelC (1nsecure) represent risks of attack (RiskA) and countermeasure (RiskC), respectively. The combined evidences, EA and EC are defined The entire risk value derived from RiskA and RiskC is given as

E_A jE_1 E_2 E_3 E_4 E_5 ,

E_C j E_2 E_4 E_5 ,

where is Dempster's rule of combination with important factors defined in Theorem 1

Risk j RiskA — RiskC j BelA (1nsecure)— BelC (1nsecure).

After attack. Specific nodes were set as attackers which conducted malicious activities for their own profits. However, any detection or response is not available in this stage. This simulation process can present the traffic patterns under the circumstance with malicious activities

4.4 Adaptive Decision

Making

Our adaptive decision-making module is based on quanti- tative risk estimation and risk tolerance, which is shown in Fig. 3. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action.

We recommend the value of lower risk tolerance threshold be 0 initially if no additional information is available. It implies when the risk of attack is greater than the risk of isolation response, the isolation is needed. If other information is available, it could be used to adjust thresholds. For example, node reputation is one of important factors in MANET security, our adaptive decision-making module could take this factor into account as well. That is, if the compromised node has a high or low reputation level, the response module can intuitively adjust the risk tolerance thresholds accordingly. In the case that LT is less than 0, even if the risk of attack is not greater than the risk of isolation, the response could also perform an isolation task to the malicious nodes.

The risk tolerance thresholds could also be dynamicallyadjusted by another factors, such as attack frequency. If the attack frequency is high, more severe response action should be taken to counter this attack. Our risk-aware response module could achieve this objective by reducing the values of risk tolerance threshold

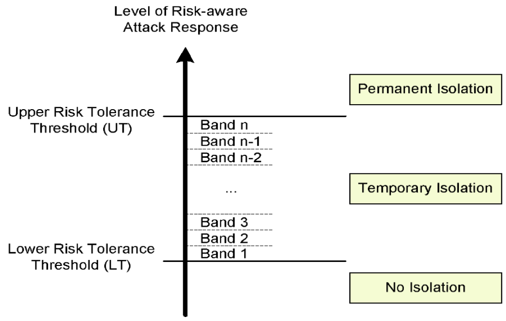

Level of Risk-aware Attack Response
Upper Risk Tolerance Threshold (UT)
Lower Risk Tolerance Threshold (LT)
Band n
Band n-1
Band n-2
...
Band 3
Band 2
Band 1
Permanent Isolation
Temporary Isolation
No Isolation

Fig 3 Decision making

5. Case Study And Evaluation

In this section, we first explain the methodology of our experiments and the metrics considered to evaluate the effectiveness of our approach. Then, we demonstrate the detailed process of our solution with a case study and also compare our risk-aware approach with binary isolation. In addition, we evaluate our solution with five random network topologies considering different size of nodes. The results show the effectiveness and scalability of our approach.

5.1 Methodology and Metrics

The experiments were carried out using Java with the eclipse tool Eclipse is an Integrated Development Tool which provides a detailed model of the physical and link layer behavior of a wireless network and allows arbitrary movement of nodes within the network.

In order to evaluate the effectiveness of our adaptiverisk-aware response solution, we divided the simulation process into three stages and compared the network performance in terms of several metrics. The following describes the activities associated with each stage:

Stage 1—Before attack. Random packets were generated and transmitted among nodes without activating any of them as attackers. This simulation can present the traffic patterns under the normal circumstance.

Stage 2—After attack. Specific nodes were set as attackers. which conducted malicious activities for their own profits. However, any detection or response is not available in this stage. This simulation process can present the traffic patterns under the circumstance with malicious activities.

Stage 3—After response. Response decisions for each node were made and carried out based on three different mechanisms. We computed six metrics for each simulation run:

. Packet delivery radio. The ratio between the number of packe ts originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.

. Routing cost. The ratio between the total bytes of routing packets transmitted during the simulation and the total bytes of packets received by the CBR sink at the final destination.

. Packet overhead. The number of transmitted routing packets; for example, a HELLO or TC message sent over four hops would be counted as four packets in this metric.

. Byte overhead. The number of transmitted bytes by routing packets, counting each hop similar to Packet Overhead.

- Average path length. This is the average length of the paths discovered by AODV. It was calculated by averaging the number of hops taken by each data packet to reach the destination

- Mean latency. The average time elapsed from “when a data packet is first sent” to “when it is first received at its destination.”

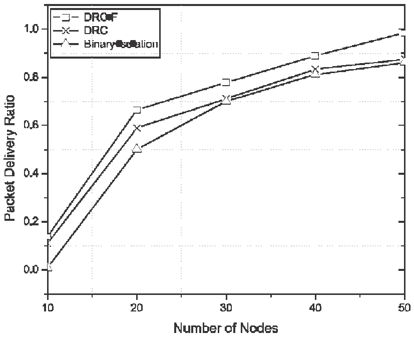
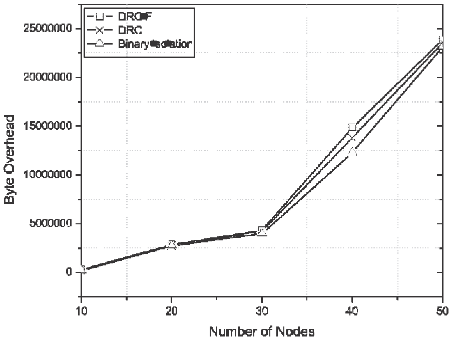


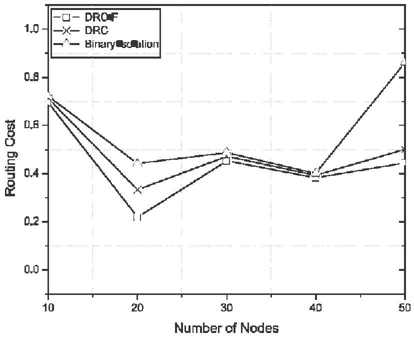
Fig 4 a Packet delivery ratio



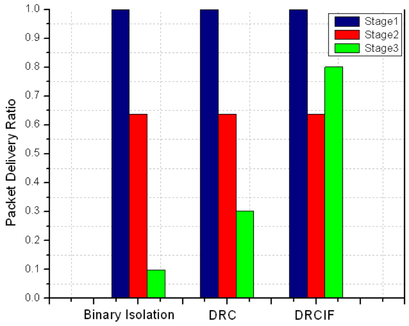
c. Byte Overhead

In Fig. 4a, as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Among these three response mechanisms, we also notice the packets delivery ratio of our DRCIF risk-aware response is higher than those of the other two approaches.

In Fig. 4b, we can observe that the routing cost of our DRCIF risk-aware response is lower than those of the other two approaches. Note that the fluctuations of routing cost shown in Fig. 4b are caused by the random traffic generation and random placement of nodes in our realistic simulation



b. Routing cost



d. Packet delivery

Fig. 4c show the packet and byte overhead, respectively. Since the routing attacks do not change the network topology further in the given case, the packet overhead and byte overhead remain almost the same . In next Stage , however, they are higher when our DRCIF risk-aware response mechanism is applied. This result meet our expectation, because the number of nodes which isolate malicious node using binary isolation and DRC risk-aware response are greater than those of our DRCIF risk-aware response mechanism.

In Fig. 4d, due to routing attacks, the packet delivery ratio decreases in Stage 2. After performing binary isolation and DRC risk-aware response in Stage 3, the packet delivery ratio even decreases more. But in DRCIF mechanism the delivery is more.

7 CONCLUSION

We have proposed a risk-aware response solution for mitigating MANET routing attacks. Especially, our approach considered the potential damages of attacks and counter- measures. In order to measure the risk of both attacks and countermeasures, we extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, we also investigated the performance and practi- cality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk- aware approach. Based on the promising results obtained through these experiments, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

8 REFERENCES

[1] Cheng.P, Rohatgi.P, Keser.C, Karger.P, Wagner.G, and Reninger.A, 2007, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy.

[2] Deng.H, Li.W, and Agrawal.D, 2002 ,"Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct..

[3] Mu.C, Li.X, Huang.H, and Tian.S, , 2008. "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08),pp. 35-48

[4] Perkins.C, Belding-Royer.E, and Das.S, 2003, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561.

[5] Refaei.M, DaSilva.L, Eltoweissy.M, and Nadeem.T, 2010 "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719.

[6] Sentz.K and Ferson.S, , 1984 “Combination of Evidence in Dempster-Shafer Theory,” technical report, Sandia Nat’l Laboratories, 2002.[9] L. Zadeh, “Review of a Mathematical Theory of Evidence,” AIMagazine, vol. 5, no. 3, p. 81.

[7] Agrawal, Sanjeev Jain, Sanjeev Sharma, January 2011, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, Journal of Computing, Volume 3, Issue 1, 41-48.

[8] Sun.L, Srivastava.R, and Mock.T, , 2006 “An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions,” Management Information Systems, vol. 22, no. 4, pp. 109-142.

[9] Sun.Y, Yu.W, Han.Z, and Liu.K, , 2002 “Information Theoretic Framework of Trust Modeling and Evaluation for Ad [8] K. Sentz and S. Ferson, “Combination of Evidence in Dempster-Shafer Theory,” technical report, Sandia Nat’l Laboratories.

[10] L. Zadeh, 1984 “Review of a Mathematical Theory of Evidence,” AI Magazine, vol. 5, no. 3, p. 81.

[11] R. Yager, , 1987, “On the Dempster-Shafer Framework and New Combination Rules* 1,” Information Sciences, vol. 41, no. 2, pp. 93-137.

[12] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, , 2002, “Sensor Fusion Using Dempster-Shafer Theory,” Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 16-17, 2013

Security for Effective Data Storage in Multi Clouds

T.NEETHA
Kommuri Pratap Reddy Institute of Technology
Hyderabad, India

CH.SUSHMA
Kommuri Pratap Reddy Institute of Technology
Hyderabad, India

ABSTRACT: Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multicloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

KeyWords: Cloud Computing, Behaviour Trust, Data integrity, Evaluation Strategy.

1. Introduction:

Currently, the cloud computing is welcome in scholars and enterprise, because of its good features such as low Investment, easy maintenance, flexibility and fast deployment, reliable service. At the same time, cloud computing can also reduce operating costs, improve operational efficiency. So many countries put the financial and material for the cloud computing.

Software as a service (SaaS): In this model, software applications are offered as services on the Internet rather than as software packages to be purchased by individual customers. One of the pioneering providers in this category is Salesforce.com offering its CRM application as a service. Other examples include Google web-based office applications.

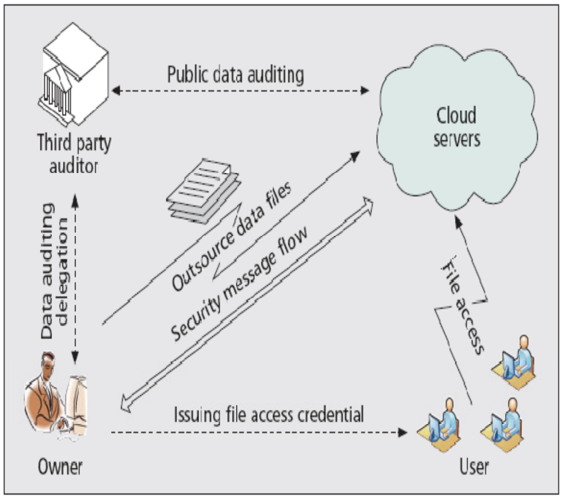
Infrastructure as a service (IaaS): Hardware resources (such as storage) and computing power (CPU and memory) are offered as services to customers. This enables businesses to rent these resources rather than spending money to buy dedicated servers and networking equipment.. As examples in this category, Amazon1 offers S3 for storage, EC2 for computing power, and SQS for network communication for small businesses and individual consumers.

Database as a service (DaaS): A more specialized type of storage is offering database capability as a service. Examples of service providers are Amazon SimpleDB, Google BigTable3, Force.com database platform and Microsoft SSDS4. DaaS on the cloud often adopts a multi-tenant architecture, where the data of many users is kept in the same physical table.

Platform as a service (PaaS): This refers to providing facilities to support the entire application development lifecycle including design, implementation, debugging, testing, deployment, operation and support of rich Web applications and services on the Internet. Most often Internet browsers are used as the development environment. Examples of platforms in this category are Microsoft Azure Services platform6, Google App Engine7, Salesforce.com Internet Application Development platform8 and Bungee Connect platform9. PaaS enables SaaS users to develop add-ons, and also develop standalone Web based applications, reuse other services and develop collaboratively in a team.

2. Ensuring Cloud Data Storage

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks.



The architecture of cloud data storage service.

To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function , chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded server failures. Lightweight: to enable users to perform storage correctness checks with minimum overhead data .Subsequently, it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure correcting code is also outlined. Finally, we describe how to extend our scheme to third party auditing with only slight modification of the main design.

3. SECURITY:

Data Integrity

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinetal.Claim that using the Byzantine faulttolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

Service Availability

Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers . Both Google Mail and Hotmail experienced service downtime recently . If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider .

Data Intrusion

According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

4. Future Work:

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers. This fact has been discovered from this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers.

5. Conclusion

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiclouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

6. References

[1] H. Shacham, B. Waters (Dec 2008), "Compact proofs of retrievability", in Proc. of Asiacrypt 2008, vol. 5350, pp. 90–107

[2] M.A.Shah, R.Swaminathan, M. Baker (2008), "Privacy preserving audit and extraction of digital contents", Cryptology ePrint Archive.

[3] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou (2009), "Enabling public verifiability and data dynamics for storage security in cloud computing", in Proc. of ESORICS'09, Saint Malo.

[4] Wang, K. Ren, W. Lou (2010), "Achieving secure, scalable, and fine-grained access control in cloud computing", in Proc. of IEEE INFOCOM'10, San Diego, CA, USA.

[5] [Online] Available : Amazon.com, "Amazon s3 availability event: (2008)," Online at http://status.aws.amazon.com/ s3- 20080720.html.

[6] Cloud Security Alliance, (2009) "Security guidance for critical areas of focus in cloud computing," 9, [Online]

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 19-21, 2013

A Generic Model for Student Data Analytic Web Service (SDAWS)

J. Shana
Coimbatore Institute of Technology
Coimbatore, India
shana@cit.edu.in

T. Venkatachalam
Coimbatore Institute of Technology
Coimbatore, India
tvenkatachalam.phy@cit.edu.in

Abstract: Any university management system accumulates a cartload of data and analytics can be applied on it to gather useful information to aid the academic decision making process. This paper is a novel attempt to demonstrate the significance of a data analytic web service in the education domain. This can be integrated with the University Management System or any other application of the university easily. Analytics as a web service offers much benefits over the traditional analysis methods. The web service can be hosted on a web server and accessed over the internet or on to the private cloud of the campus. The data from various courses from different departments can be uploaded and analyzed easily. In this paper we design a web service framework to be used in educational data mining that provide analysis as a service.

Keywords: educational data mining, web service, data analytics, association rule mining, classification

1. INTRODUCTION

Analytics is a fast emerging area of technology because there is flooding of data due to the advancement in internet. There is huge amount of data everywhere and organizations need to invest into technologies and infrastructure to analyze this data and derive meaningful knowledge out of it for effective decision making process. Education domain also generate lot of academic data that can be mined to gain useful information using which lot of remedial measures can be taken. Of late cloud computing has taken a centre stage for it is able to deliver everything as a service and the organization need no longer buy expensive hardwares or softwares to build the infrastructure needed. And web service is one of the many technologies that is helping cloud computing to achieve its objective. Data analytics involves lot of machine learning and statistical techniques to mine out useful decision making information. Data mining algorithms such as association rule mining, classification clustering and outlier analysis try to bring out hidden meaningful information from huge academic data sets. The web services approach uses standards-based interfaces for connecting data providers with data users. The network strives to go beyond searching and visualizing data to include data processing and analysis services to allow users to create new content. From a technical perspective, the web service technologies consist of a collection of standard protocols that enable the creation, distribution, discovery and integration of software components over the internet. Central to the web service technologies are the concepts of “software as service” and “platform independence” [4].

Analysis software for the education domain differs from mining the financial data or the business data in general. So the traditional commercial analysis softwares cannot satisfy the needs of the institution. This paper suggests a model that implements the analysis techniques as a service based architecture. This would enable the faculty to access the service from a any browser based client application, irrespective of the language in which the service is built. It can be invoked by any kind of application over the network. This would provide a greater flexibility to integrate even with the legacy client application or the latest kind of mobile application. Also the model can be extended to work on the private cloud of the institution there by leveraging the power of cloud computing.

2. THE BACKGROUND

There exists many commercial data analytics service for different domains offering little support for complete data analysis. There is no service for the educational domain to the best of our knowledge. This paper takes the inspiration from such existing attempts. Data analytics as a service is fast catching up after the success of cloud computing. Table 1 gives an overview of companies that have adopted to offer data storage and effective retrieval service commercially. Except ADABA all other products provide only data storage and query support to the clients.

Table 1:Commercial data analysis softwares

Company	Service	Features
Google	BigQuery	Data analysis for the uploaded data in the cloud.
HP	Vertica Analytic DB	A RDBMS for building data warehouse and database for BI in the cloud
Amazon	SimpleDB	Data storage and

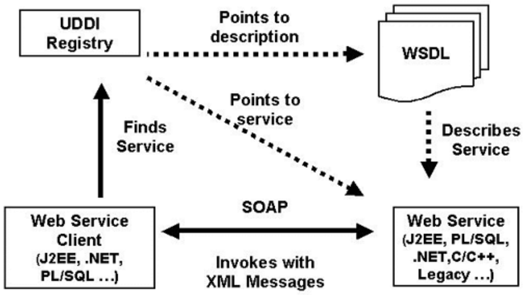
		retrieval in cloud

Literature survey of the web service analytics gives some interesting information.[6] provides a automatic advice for scientists in their data analysis using data analysis web service.[5] describes the development and application of web service for comparing US and global emission inventories.[8]specifies an on demand BI architecture on cloud for the healthcare sector. [7] offers a wide range of techniques that support the transformation of Data Analysis including web service technology.[9] propose a novel infrastructure that offers complex and optimized query facilities for web services through combined invocation of different web services. Academic analytics is used to derived intelligent information from academic data and used in higher education in decision making. Many notable works have been done in the field of educational data mining. [1] Compares different data mining methods for classifying students based on the Moodle usage data.[3] elaborates on the challenges in educational data mining. [11] uses data mining techniques for identifying the factors that affect the student drop out. In [2] different classification algorithms are implemented to identify the factors that affect the performance of students in a particular course.

3. THE PROPOSED SYSTEM

3.1 Web Service Architecture

Fig 1 Web service

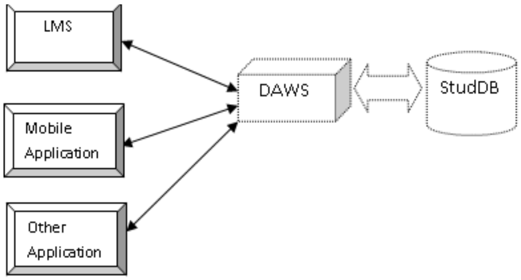

UDDI Registry
Points to description
WSDL
Points to service
Finds Service
Describes Service
SOAP
Web Service Client (J2EE, .NET, PL/SQL ...)
Invokes with XML Messages
Web Service (J2EE, PL/SQL, .NET,C/C++, Legacy ...)

The SOAP-based Web service architecture comprises three entities:

- A service provider, which creates a SOAP based Web service and publishes the service description in the service registry
- A service registry, which enables online service discovery and
- A service requestor, which finds the service by querying the service registry. The requestor then retrieves the service description, uses it to bind to the service implementation, and begins interacting with it

3.2 Architecture of SDAWS

Fig 2: Components of SDAWS



Server Side:

Database: This holds the entire student data that is represented after efficient preprocessing. The attributes relevant for analysis is selected and stored here.

Web server: It here that the data analytical web service resides. This exposes the analysis functionalities to the client application over the network.

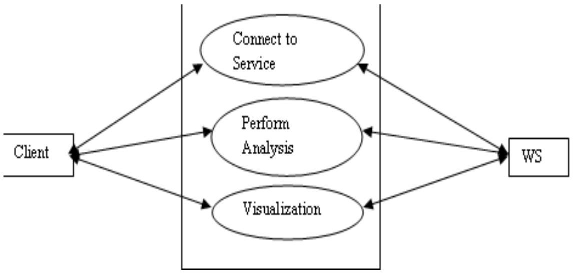
Client Side:

This can be any of kind of thin client application that can access the service by connecting to it. The client application can be a part of the Learning Management System (LMS) or any other application running in any of the department of the institution. It can also be a mobile application to be used from anywhere in the campus.

3.3 Web Service Implementation

The web service can be implemented in any language that supports a web service development framework. The client application can be any web based application developed in any language irrespective of the language in which the service is developed. The major functionalities of the data analytic web service are shown as a Use-Case model in Fig 3.

Fig 3: Use case diagram for the proposed system



3.4 Analysis Techniques

The web service can implement any of the data mining functionalities on the student data. The most common mining algorithms that can generate useful information are Association rule mining, Clustering and Prediction techniques as given in [12].

Association Rule mining

Association analysis discovers association between the attributes of a relation and specifies it in the form X=> Y. Such rules are called as association rules. This technique when applied on the student data can reveal useful associations between attributes such as test marks and final result, class attendance and final result and so on. Many algorithms exist for mining association rules and the most noted one is the Apriori algorithm.

Clustering Technique

Cluster analysis allows objects to be grouped into clusters or groups such that objects within a cluster have high similarity in comparison to one another but very dissimilar to objects in other clusters. This analysis on the student data could help us with information like what kind of students tend to score well in exams and which group of students deviates from the usual. Cluster analysis is helpful for identifying the outliers easily. Algorithms such as K-Means, K-medoids and K nearest neighbor can be used for cluster analysis.

Prediction Methods

Prediction in data mining involves classification technique to predict the class label of the data objects whose class label in unknown. This method can be applied on the student dataset to predict the performance of the students. [2]

It can also be used to predict the prospective students for a course and to would help in improving the course in general. Decision tree based algorithms such as ID3 or Neural network based algorithms or Bayesian Belief Networks can be used for classification.

4. CONCLUSION

This paper has given a general model for building a data analytic web service. Analytics as a service provides lot of benefits and can be implemented by any educational institution easily. Once the web service is hosted in the campus server it can be accessed from any browser based application. Academic analysis would help the faculty to determine lot of information about the performance of students in courses and take timely action whenever necessary. This system can be easily incorporated as a cloud based application in the private cloud of the campus also.

5. REFERENCES

[1] Romero, C Ventura, S, Espejo, P,G and Hervas, C. 2008. Data Mining Algorithms to Classify Students. 1st International Conference on Educational Data Mining, Proceedings. Montreal, Canada.

[2] Shana, J and Venkatachalam, T 2011. Identifying Key Performance Indicators from Student Course Data, IJCA.

[3] Baker, R, J, D and Yacef ,K. 2009 The state of educational data mining in 2009: A review and future visions”, Journal of Educational Data Mining.

[4] Hsing, K , Cheng, Qian and Q, T, Leon ,Z.2006. Web Services and Service-Oriented Application Provisioning: An Analytical Study of Application Service Strategies, IEEE Transactions on engineering Management.

[5] Falke, S, Stella, G and Keating, T. 2007. Web Services for Comparative Data Analysis of Emission Inventories.

[6] Kollingbaum, M, J, Cai, K and Norman ,T, J 2004.Web Service Support for Scientific Data Analysis.

[7] Farber, M, Cameron, M , Ellis, C and Sullivan, J.2000. Massive Data Anlaytics and the Cloud, A whitepaper, Booz Allen Hamilton Publications.

[8] Indrajit, B and Anandhi, R 2011.Healthcare Data Analytics on the cloud, Online Journal of Health and Allied Sciences..

[9] Quzzani, M and Bouguettaya ,A 2004. Efficient Access to Web Service, IEEE Computer Society.

[10] Zheng, G and Bouguettaya, A 2009. Service Mining on the Web, IEEE Transactions on Services Compting,

[11] Ho Yu, C and DiGangi, S. 2010. A Data Mining Approach for Identifying Predictors of Student Retention from Sophomore to Junior Year, Journal of Data Science.

[12] Han, J and Kamber, M 2006.Data Mining – Concepts and Techniques, Morgan Kaufmann Publishers.

[13] http://www. axis.apache.org/axis2/java/core.htm

Identifying the Number of Visitors to improve Website Usability from Educational Institution Web Log Data

Arvind K. Sharma
Dept. of CSE
Jaipur National University, Jaipur,
Rajasthan,India

P.C. Gupta
Dept. of CSI
University of Kota
Kota, Rajasthan-India

Abstract: Web usage mining deals with understanding the Visitor’s behaviour with a Website. It helps in understanding the concerns such as present and future probability of every website user, relationship between behaviour and website usability. It has different branches such as web content mining, web structure and web usage mining. The focus of this paper is on web mining usage patterns of an educational institution web log data. There are three types of web related log data namely web access log, error log and proxy log data. In this paper web access log data has been used as dataset because the web access log data is the typical source of navigational behaviour of the website visitor. The study of web server log analysis is helpful in applying the web mining techniques.

Keywords: Web Usage Mining, Web Log Data, WebLog Expert Lite7.8

1. INTRODUCTION

Website is an important tool for web users to obtain information such as education, entertainment, health, e-commerce, etc. Today, the Internet is most emerging technology in the world. The terms Internet and World Wide Web are often used in everyday speech without much distinction. The World Wide Web is also known as ‘Information Superhighway’. It is a system of interlinked hypertext documents accessed via Internet. However, the Internet and the World Wide Web are not one and the same. The Internet is a global system of interconnected computer networks. In other hand, the World Wide Web is one of the services that run on the Internet[1]. It is a collection of text documents and other resources, linked by hyperlinks and URLs, usually accessed by Web browsers from web servers. In short, the World Wide Web is also considered as an application ‘running’ on the Internet[2]. It is a large and dynamic domain of knowledge and discovery. It has become the most popular services among other services that the Internet provides. The number of users as well as the number of website has been increasing dramatically in the recent years. A huge amount of data is constantly being accessed and shared among several types of users, both humans and intelligent machines.

Paper is organized in different sections: Section-II explains Web usage mining. Proposed methodology is shown in Section-III. Section-IV contains Experimental results. Conclusion is shown in section-V while references are mentioned in the last section.

2. WEB USAGE MINING

Web Usage Mining is a part of Web Mining, which, in turn, is a part of data mining. As data mining has been used to extract meaningful and valuable information from large volume of data, the web usage mining has been used to mine the usage characteristics of the Website users. Web mining refers to overall process of discovering potentially useful and previously unknown information from the web document and services[3]. This extracted information can be used in a variety of ways such as improvement of the Web application, identifying the visitor’s behaviour, checking of fraudulent elements etc. Web access patterns mined from Web log data have been interesting and useful knowledge in practice. Examples of applications of such knowledge include improving design of the websites, analyzing system performance to understand user's reaction and motivation, build adaptive websites[4]. The aim in web usage mining is to discover and retrieve useful and interesting patterns from a large dataset.

2.1 Phases of Web Usage Mining Process

Web usage mining process consists of three phases such as Preprocessing of web data, Pattern discovery, and Pattern analysis [5]. Preprocessing is a primary work in web mining process. The main phases in Web usage mining process are shown in fig.1 below.

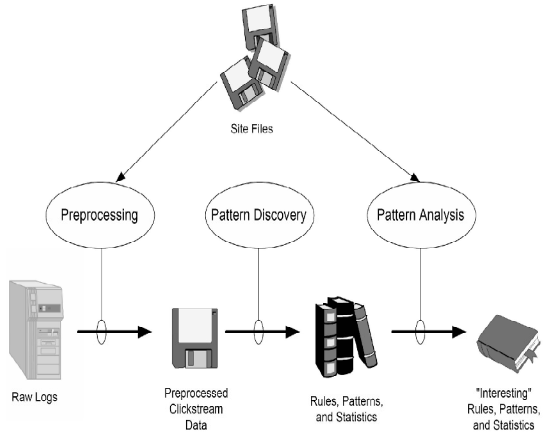

Site Files
Preprocessing
Pattern Discovery
Pattern Analysis
Raw Logs
Preprocessed Clickstream Data
Rules, Patterns, and Statistics
"Interesting" Rules, Patterns, and Statistics

Fig.1: Phases of Web Usage Mining Process

2.1.1 Preprocessing: Data preprocessing describes any type of processing performed on raw data to prepare it for another processing procedure. Commonly used as a preliminary data mining practice, data preprocessing transforms the data into a format that will be more easily and effectively processed for the purpose of the user.

2.1.2 Pattern Discovery: Web usage mining can be used to uncover patterns in web server log data but is often carried out only on samples of data. The mining process will be ineffective if the samples are not a good representation of the larger body of data.

2.1.3 Pattern Analysis: This is the final step in the Web Usage Mining process. After the preprocessing and pattern discovery, the obtained usage patterns are analyzed to filter uninteresting information and extract the useful information.

3. PROPOSED METHODOLOGY

As those trends become stronger and stronger, there is much need to study web user behaviour to better serve the users and increase the value of institutions or enterprises. Website design is currently based on thorough investigations about the interests of website visitors and investigated assumptions about their exact behaviour. Today, understanding the interests of users is becoming a fundamental need for Websites owners in order to better serve their users by making adaptive the content and usage, structure of the website to their preferences. The analysis of web log data permits to identify useful patterns of the browsing behavior of users, which exploited in the process of navigational behavior. Web log data captures web-browsing behaviour of users from a Website. Academic institutions are good examples that develop website. One such institution of the education sector has been considered in our work. This paper presents visitor pattern analysis performed through educational institution web log data. We have been performed different analysis on a sample of Web log data to–

➢ Determine the usability of the Website, including the-

- Visitor Pattern Analysis
- Page View Analysis
- Time Analysis
- Origin of the Website Visitors
- Portions of the Website that are accessed
- Number of document downloads(both hits & accesses)

In this work, WebLog Expert reports undergo a time analysis and page view analysis. The time analysis looks at the different times of day, days of week, and days of month that the Website receives the most visitors. The page view analysis provides which website pages are most viewed by the visitors. The combination of these statistics will help us to predict the attributes of the Website user and the Website usability.

3.1 Data Collection

In this study, the user access web log data has been collected from the Educational Institution Website's 0server www.davkota.org which stores normally secondary data source in view of the fact that web log keeps every activity of the user regarding to visit of the Website. The web log data contains the information from 31 October 2012 to 30 November 2012 of one month period. During this period, 1.01 GB data had been transferred for the complete work.

3.2 Data Selection

At present, towards Web Usage Mining technique, the main data origin has three kinds: Server-side data, Client-side data, and Proxy-side data (middle data). In this work, we use the case of the Web server.

3.2.1 Web Log Data

A Web log data is a listing of page reference data sometimes it is referred to as click stream data[6]. The web plays an important role and medium for extracting useful information. There is a need for data log to track any transaction of the communications. This data can offer valuable information insight into website usage. It characterizes the activity of many users over a potentially long period of time. The web server log data contains several attributes. These attributes are as follows:

Date-The date from Greenwich Mean Time(GMTx100) is recorded for each hit. The date format is YYYY/MM/DD. The example above shows that the transaction was recorded at 2012/11/01.

Time-It refers Time of transactions. The time format is HH:MM:SS.

Client IP Address-It is the number of computer who access or request the website.

User Authentication-Some websites are set up with a security feature that requires a user to enter username and password. Once a user logs on to a website, that user's 'username' is logged in the log file.

Server IP Address-It is a static IP provided by Internet Service Provider. This IP will be a reference for access the information from the server.

Server Port-It is a port used for data transmission. Usually, the port used is port 80.

Server Method(HTTP Request)-The term request refers to an image, pdf, .txt, HTML file, movie, sound, and more.

URL-It is a path from the host. It represents the structure of the websites.

Agent Log-It provides data on a user's browser, browser version, and operating system. This is the significant information, as the type of browser and operating system determines what a user is able to access on a website.

3.3 Tool for Experiment

There are various commercial and freely available tools exists for web mining purposes. WebLog Expert Lite7.8 is one of the fast and powerful Web log analyzer tool[7]. This tool helps to reveal important statistics regarding a web site's usage such as activity of visitors, access statistics, paths through the website, visitors' browsers, etc. It supports W3C extended log format that is the default log format of Microsoft IIS 4.0/.05/6.0/7.0 and also the combined and common log formats of Apache web server. It reads compressed log files (.gz, .bz2 and .zip) and can automatically detect the log file format. If necessary, log files can also be downloaded via FTP or HTTP. We have been used a web log analyzer WebLog Expert Lite7.8 web mining tool. It is one such program and used to produce highly detailed, easily configurable usage reports in Hypertext Markup Language (HTML) format, for viewing with a standard web browser[7]. Using this web mining tool we have been identified Hits statistics like Total Hits, Visitors Hits, Average Hits per Day, Average Hits per Visitor, etc., Page View Analysis like Total Page views, Average Page Views per Day, Average Page Views per Visitor, total Visitors, Total Visitors, Average Visitors per Day, Total Unique IPs, Bandwidth, Total Bandwidth, Visitor Bandwidth, Average Bandwidth per Day, Average Bandwidth per Hit, and Average Bandwidth per Visitor of the Website on monthly and day of the week basis.

4. EXPERIMENTAL RESULTS

In this work, we have been used web log data from October 31, 2012 to November 30, 2012 collected from the web server of the website *www.davkota.org* have been analyzed by using WebLog Expert Lite7.8 web mining tool[7]. The complete experiment has been done on the basis of web log data of an educational institution's website. The design and execution of such work is restricted and time consuming. The results had limited in time and space so only a limited period of time is taken to perform the results. The general activity statistics of the website usage is shown in Table-1.

Table-1: General Activity Statistics of the Website Usage

Hits	
Total Hits	23669
Visitor Hits	21744
Spider Hits	1925
Average Hits per Day	763
Average Hits per Visitor	25.46
Cached Requests	2753
Failed Requests	2177
Page Views	
Total Page Views	1517
Average Page Views per Day	48
Average Page Views per Visitor	1.78
Visitors	
Total Visitors	854
Average Visitors per Day	27
Total Unique IPs	935
Bandwidth	
Total Bandwidth	1.01 GB
Visitor Bandwidth	993.44 MB
Spider Bandwidth	42.93 MB
Average Bandwidth per Day	33.43 MB
Average Bandwidth per Hit	44.84 KB
Average Bandwidth per Visitor	1.16 MB

By using the WebLog Expert Lite7.8 web mining tool, we had been found 23669 hits, 854 visitors, 935 IPs, 1517 page views, 1.01 GB data had been transferred and so on. Based on the analyzer report, we have been found several unnecessary records like image files, failed requests and incomplete records and are eliminated and useful information like total hits, total cached hits, average hits per day, average hits per hour, average hits per visitor, average data transfer per hits, total visitors, average visitors per day, average time spent, average page views per visitors, average downloads per visitors, average data transfer per visitor, visitors who visit once, visitors who visit more than once, average page views per day, total files downloads, average files downloads per day, total data transferred and average data transfer rates have been found. Fig.2 shows the daily visit report of the website visitors.

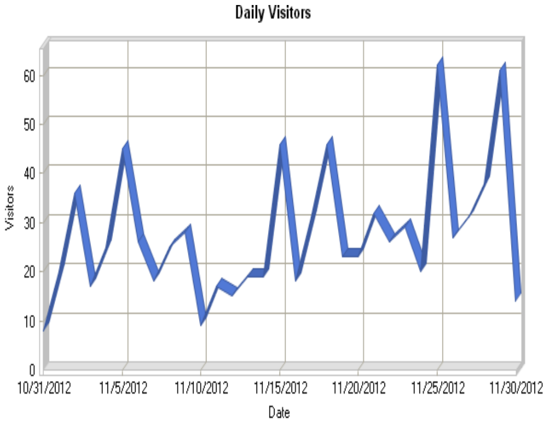


Fig.2: Daily Website Visitors Report

Table-2 shows the accurate daily visitor's activity statistics of the website usage. This summary report produced daily usage activity such as total hits of website visitors, hits per day, total page views, page views per day, total visitors, visitors per day, total time spent, data transfer per day and total data transfer on the Website.

Table-2: Daily Activity Statistics of the Website Usage

Date	Hits	Page Views	Visitors	Band width (in KB)
Wed 31/10/2012	94	6	8	4,691
Thu 1/11/2012	560	28	20	33,309
Fri 2/11/2012	338	44	36	13,894
Sat 3/11/2012	596	25	17	20,454
Sun 4/11/2012	863	105	25	41,395
Mon 5/11/2012	890	71	45	40,398
Tue 6/11/2012	511	27	26	25,445
Wed 7/11/2012	664	29	18	38,742
Thu 8/11/2012	938	44	25	42,123
Fri 9/11/2012	1,044	100	28	60,350
Sat 10/11/2012	611	40	9	28,218
Sun 11/11/2012	860	52	17	35,736
Mon 12/11/2012	935	43	15	17,630
Tue 13/11/2012	1,097	53	19	35,406
Wed 14/11/2012	855	52	19	38,358

Thu 15/11/2012	470	35	46	22,275
Fri 16/11/2012	568	40	18	29,770
Sat 17/11/2012	738	40	31	37,462
Sun 18/11/2012	1,001	76	46	52,991
Mon 19/11/2012	485	26	23	25,025
Tue 20/11/2012	1,261	66	23	24,944
Wed 21/11/2012	822	77	32	38,954
Thu 22/11/2012	1,047	50	26	54,000
Fri 23/11/2012	1,096	61	29	60,547
Sat 24/11/2012	562	42	20	25,553
Sun 25/11/2012	693	41	62	30,171
Mon 26/11/2012	524	35	27	25,890
Tue 27/11/2012	666	44	31	37,516
Wed 28/11/2012	1,417	66	38	57,966
Thu 29/11/2012	1,044	74	61	41,815
Fri 30/11/2012	419	25	14	20,198
Total	**23,669**	**1,517**	**854**	**1,061,241**

The following report produced, total number of hits 23669, total page views 1517, total visitors 854, and total bandwidth 1061241 Kilobytes were found which summarized in table-2. Every day 28 average number of visitors are visited the website. This report shows day wise total number of visitors or users who are visited the Website. From this statistics, it will be helpful to identify the number of visitors of the Website and improve the overall structure of the Website. Fig.3 shows the report of hourly website visitors.

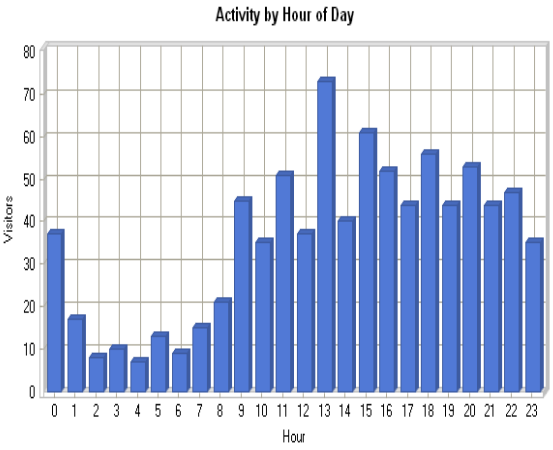


Fig.3: Hourly Website Visitors Report

Table-3 displays the accurate hourly visitor's activity statistics of the website usage. This summary report produced hourly usage activity such as total hits of website visitors, hits per hour, total page views, page views per hour, total visitors, visitors per hour, total time spent, data transfer per visitor per hour and total data transfer on the Website.

Table-3: Hourly Activity Statistics of the Website Usage

Hour	Hits	Page Views	Visitors	Bandwidth (in KB)
00:00-00:59	997	47	37	28,533
01:00-01:59	221	9	17	11,147
02:00-02:59	225	44	8	9,399
03:00-03:59	129	20	10	6,647
04:00-04:59	74	3	7	1,895
05:00-05:59	110	6	13	3,942
06:00-06:59	169	15	9	3,488
07:00-07:59	287	14	15	11,372
08:00-08:59	803	62	21	35,070
09:00-09:59	1,375	89	45	65,435
10:00-10:59	1,132	55	35	47,489
11:00-11:59	1,322	87	51	72,202
12:00-12:59	1,433	111	37	78,902
13:00-13:59	1,387	140	73	71,503
14:00-14:59	1,201	62	40	59,039
15:00-15:59	1,141	83	61	54,597
16:00-16:59	1,431	100	52	70,286
17:00-17:59	1,670	107	44	52,309
18:00-18:59	1,405	80	56	73,534
19:00-19:59	1,551	86	44	72,728
20:00-20:59	1,848	83	53	84,602
21:00-21:59	1,554	73	44	70,027
22:00-22:59	859	57	47	42,005
23:00-23:59	1,345	84	35	35,078
Total	**23,669**	**1,517**	**854**	**1,061,241**

Total number of visitors found 854 that are shown in table-3. Every day 28 average number of visitors are visited the website. This summary report shows hourly usage of the website and predicts total number of visitors who are accessed the Website. From this, it is concluded that the output of this phase plays a major role in predicting the best frequent patterns, which are the foremost information for improving the Website usability and identifying the number of visitors of the Website.

5. CONCLUSION

Web is one of the most used interface to access remote data, commercial and non-commercial services. Web mining is a growing area with the growth of web based applications to find web usage patterns. By using web mining we could found website user's interest and behavior through which we can make our website valuable and easily accessible. The complete work has accomplished by analyzing educational institution web log data for one month period. Our experimental results help to predict and identify the number of visitors for the Website and improve the Website usability.

6. REFERENCES

[1] Piatetsky Shapiro G. et al., “Advances in Knowledge Discovery and Data Mining”, AAAI/MIT Press, 1996.

[2] The W3C Technology Stack; “World Wide Web Consortium”, Retrieved April 21, 2012.

[3] Arvind K. Sharma, P.C. Gupta, “Enhancing the Performance of the Website through Web Log Analysis and Improvement”, International Journal of Computer Science and Technology (IJCST) Vol.3, Issue 4, Oct-Dec 2012.

[4] Huiping Peng, “Discovery of Interesting Association Rules Based on Web Usage Mining”, International Conference 2010.

[5] Cooley, R., “Web Usage Mining: Discovery and Application of Interesting Patterns from Web data”, 2000, http://citeseer.nj.nec.com/426030.html.

[6] Castellano.G et al., “Log Data Preparation for Mining Web Usage Patterns”, International Conference Applied Computing, 2007, pp.371-378.

[7] [Online] http://www.weblogexpert.com

7. ACKNOWLEDGMENT

Our thanks to DAV Organization, Department of Computer Science and IT, DAV Kota for providing Web server log data.

An Efficient Reconfigurable Filter Design for Reducing Dynamic Power

Mohammed Harris.S
Sri Ramakrishna Engineering College,
Coimbatore, Tamil Nadu, India

Manikanda Babu C.S.
Sri Ramakrishna Engineering College,
Coimbatore, Tamil Nadu, India

Abstract - This paper presents an architectural view of designing a digital filter. The main idea is to design a reconfigurable filter for reducing dynamic power consumption. By considering the input variation's we reduce the order of the filter considering the coefficient are fixed. The filter is implemented using mentor graphics using TSMC .18um technology. The power consumption is decreased in the rate of 16% from the conventional model with a slight increase in area overhead. If the filter coefficients are fixed then the power can be reduced up to 18% and the area overhead can also be reduced from the reconfigurable architecture.

Key words— Low power digital filter, Reconfigurable filter**.**

1.INTRODUCTION

THE explosive growth in mobile computing and portable multimedia applications has increased the demand for low power digital signal processing (DSP) systems.

One of the most widely used operations performed in DSP is finite impulse response (FIR) filtering. The input-output relationship of the linear time invariant (LTI) FIR filter can be expressed as the following equation:

$$y(n) = \sum_{k=0}^{N-1} c_k \, x(n-k) \qquad (1)$$

Where N represents the length of FIR filter, the kth coefficient, and the x(n-k) input data at time instant. In many applications, in order to achieve high spectral containment and/or noise attenuation, FIR filters with fairly large number of taps are necessary.

Many previous efforts for reducing power consumption of FIR filter generally focus on the optimization of the filter coefficients while maintaining a fixed filter order. In those approaches, FIR filter structures are simplified to add and shift operations, and minimizing the number of additions/subtractions is one of the main goals of the research. However, one of the drawbacks in those approaches is that once the filter architecture is decided, the coefficients cannot be changed, those techniques are not applicable to the FIR filter with programmable coefficients.

Approximate signal processing techniques are also used for the design of low power digital filters. In [1], filter order dynamically varies according to the stop-band energy of the input signal. However, the approach suffers from slow filter-order adaptation time due to energy computations in the feedback mechanism. Previous studies in [2] show that sorting both the data samples and filter coefficients before the convolution operation has a desirable energy-quality characteristic of FIR filter. However, the overhead associated with the real-time sorting of incoming samples is too large.

In this paper, we propose a simple yet efficient low power reconfigurable FIR filter architecture, where the filter order can be dynamically changed depending on the amplitude of the filter inputs. In other words, when the data sample multiplied to the coefficient is so small as to mitigate the effect of partial sum in FIR filter, the multiplication operation can be simply cancelled. The filter performance degradation can be minimized by controlling the error bound as small as the quantization error or signal to noise power ratio (SNR) of given system. The primary goal of this work is to reduce the dynamic power of the FIR filter, and the main contributions are (1) A new reconfigurable FIR filter architecture with real-time input monitoring circuits is presented. Since the basic filter structure is not changed, it is applicable to the FIR filter with fixed coefficients or adaptive filters

The rest of the paper is organized as follows. In Section II, the basic idea of the proposed reconfigurable filter is described. Section III presents the reconfigurable fixed coefficient architecture and circuit techniques used to implement the filter.

2. RECONFIGURABLE FIR FILTERING TO TRADE OFF FILTER PERFORMANCE

In this section, we present direct form (DF) architecture of the reconfigurable FIR filter, which is shown in Fig. 1(a). In order to monitor the amplitudes of input samples and cancel the right multiplication operations, amplitude detector (AD) in Fig. 1(b) is used. When the absolute value of is smaller than the threshold *xth*, the output of AD is set to "1". The design of AD is dependent on the input threshold *xth*, where the fan in's of AND and OR gate are decided by *xth*. If *xth* and *cth* have to be changed adaptively due to designer's considerations, AD can be implemented using a simple comparator. Dynamic power consumption of CMOS logic gates is a strong function of the switching activities on the internal node capacitances.

In the proposed reconfigurable filter, if we turn off the multiplier by considering each of the input amplitude only, then, if the amplitude of input abruptly changes for every cycle, the multiplier will be turned on and off continuously, which incurs considerable switching activities. Multiplier control signal decision window (MCSD) in Fig. 1(a) is used to solve the switching problem. Using *ctrl* signal generator inside MCSD, the number of input samples consecutively smaller than are counted and the multipliers are turned off only when consecutive input samples are smaller than. Here, means the size of MCSD [in Fig. 1(a), is equal to 2].

Fig. 2(a) shows the *ctrl* signal generator design. As an input smaller than *xth* comes in and AD output is set to "1", the counter is counting up. When the counter reaches m, the *ctrl* signal in the figure changes to "1", which indicates that consecutive small inputs are monitored and the multipliers are ready to turn off. One additional m bit, in Fig. 2(a), is added and it is controlled by *ctrl*. The accompanies with input data all the way in the following flip-flops to indicate that the input sample is smaller than *xth* and the multiplication can be cancelled when the *cth* coefficient of the corresponding multiplier is also smaller than . Once the $\text{in}_{\text{cnt\_in}}$ signal is set inside MCSD, the signal does not change outside MCSD and holds the amplitude information of the input.

A delay component is added in front of the first tap for the synchronization between x*(n) and in Fig. 3(a) since one clock latency is needed due to the counter in MCSD. However, in the FIR filter with fixed or programmable coefficients, since we knowthe amplitude of coefficients ahead, extra AD modules for coefficient monitoring are not needed.

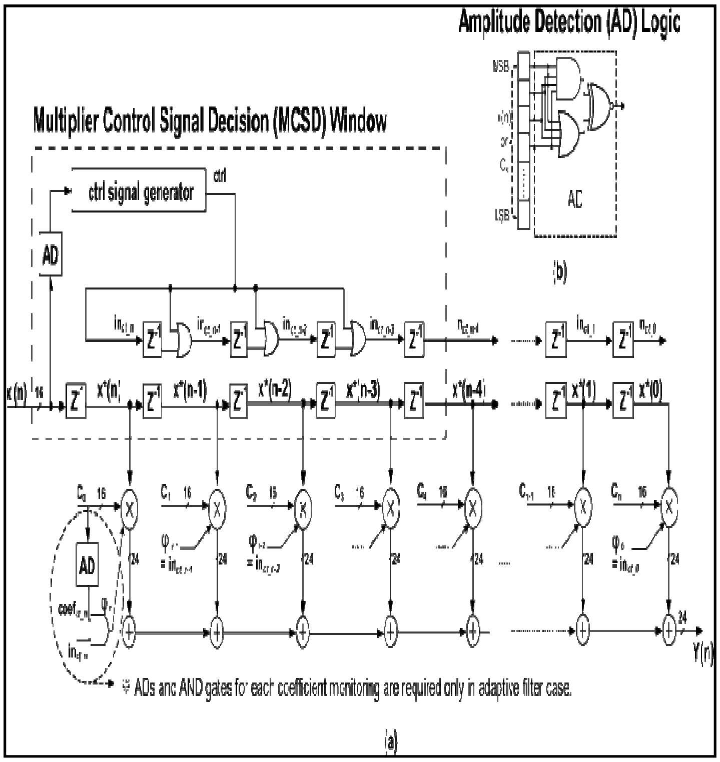


Figure. 1(a)MCSD window (b)Amplitude Detector

When the amplitudes of input and coefficient are smaller than *xth* and *cth* respectively, the multiplier is turned off by setting signal [Fig. 3(a)] to "1". Based on the simple circuit technique [11] in Fig. 4(b), the multiplier can be easily turned off and the output is forced to "0". As shown in the figure, when the control signal *ctrl* is "1", since PMOS turns off and NMOS turns on, the gate output is forced to "0" regardless of input.

When x_n is "0", the gate operates like standard gate. Only the first gate of the multiplier is modified and once this set to "1", there is no switching activity in the following nodes and multiplier output is set to "0". The area overheads of the proposed reconfigurable filter are flip-flops for signals, AD and *ctrl* signal generator inside MCSD and the modified gates in Fig. 2(b) for turning off multipliers.

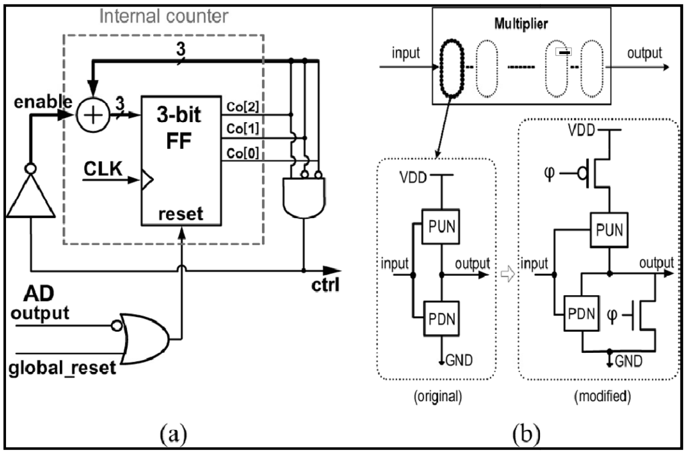


Figure. 2(a) Schematic of *ctrl* signal generator. Internal counter sets *ctrl* signal to "1" when all input samples inside MCSD are smaller than *xth* (m=4 case).(b) Modified gate schematic to turn off multiplier.

Those overheads can be implemented using simple logic gates, and a single AD is needed for input monitoring as specified in Fig. 1(a).

3. FIXED COEFFICIENT RECONFIGURABLE DIGITAL FILTER

The proposed reconfigurable digital filter uses the fixed coefficient. If we maintain a fixed coefficient then the power consumed by the multiplier for the various inputs are reduced by half literally. For example the C0=1100011 and the C11=1100011 then we can replace the coefficient of C11 with the C0. Thus the multiplication result of the C11 and C0 remains the same. This will reduce the multipliers switching activity.

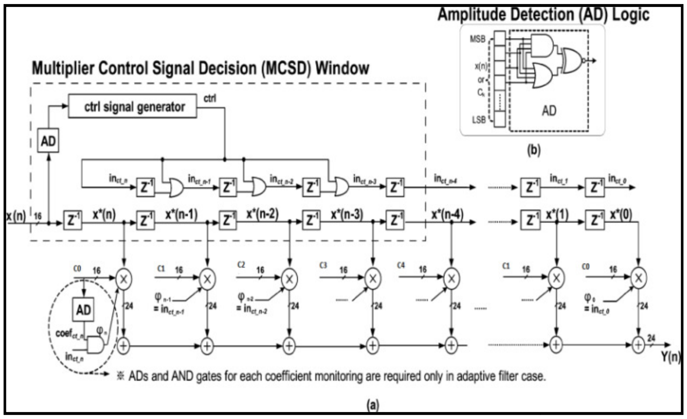

Amplitude Detection (AD) Logic
Multiplier Control Signal Decision (MCSD) Window
ctrl signal generator
ctrl
AD
MSB
LSB
AD
(b)
x(n)
16
x*(n)
x*(n-1)
x*(n-2)
x*(n-3)
x*(n-4)
x*(1)
x*(0)
C0
C1
C2
C3
C4
24
Y(n)
※ ADs and AND gates for each coefficient monitoring are required only in adaptive filter case.
(a)

Figure. 3 Proposed FIR filter with fixed co-efficient

This will enhance the power reduction. The power reduction achieved by the conventional, reconfigurable and fixed coefficient filter will reduce the power of the enormously. If the coefficients are fixed then significant reduction in area can be achieved. This can overcome one of the drawback of the filter as such area overhead. The results are shown in section IV.

4. RESULT

The reconfigurable digital filter is designed using the mentor graphics using TSMC .18um. The MCSD window which reduces the computation complexity by grouping the mitigate values. This in turn reduces the power by the 16% than that of conventional model.

TABLE 1 POWER AND AREA COMPARISON BETWEEN CONVENTIONAL, RECONFIGURABLE AND FIXED COEFFICIENT FIR FILTER

Parameter	Conventional	Reconfigurable	Fixed Coefficient Filter
Power (mW)	309	257	253
No. of Gate counts	2,702	2,017	1,993

There is a slight increase in area if the taps increases the area will be minimized. The simulation result of fixed coefficient filter is shown in fig.4 and the corresponding RTL schematic is shown in the fig.5. The result that we have obtained in the proposed method is shown in the table.1.

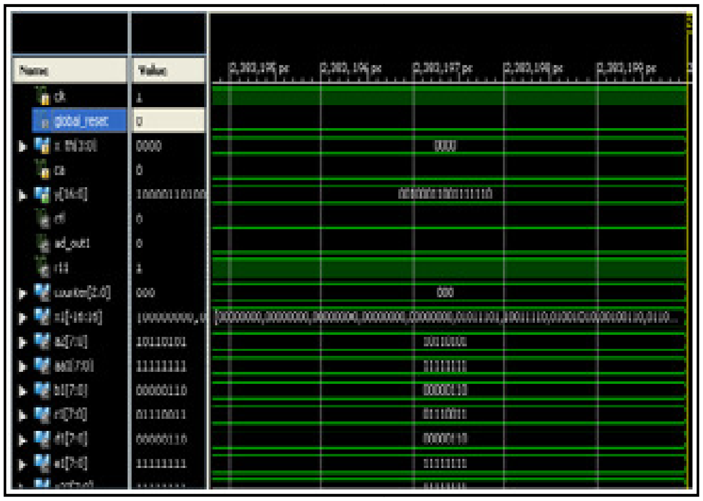


Figure. 4 Simulation result of fixed co-efficient filter

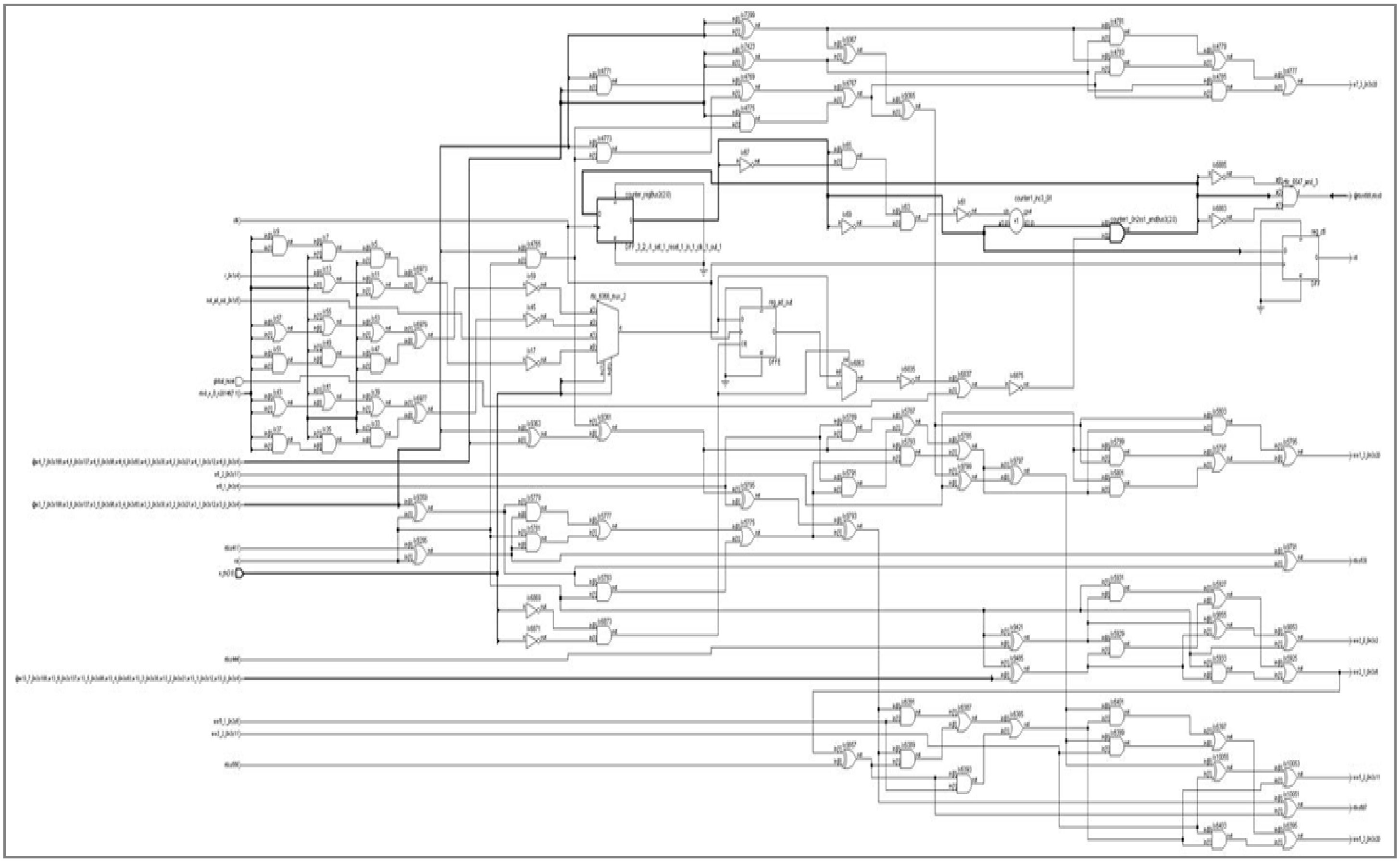


Figure. 5 RTL schematic of proposed fixed coefficient filter using TSMC .18 um technology

5. CONCLUSION

In this paper, we propose low power reconfigurable digital filter architecture. In the proposed reconfigurable filter, the input data are monitored and the multipliers in the filter are turned off when the coefficients inputs are small enough to mitigate the effect on the filter output. The power can be further reduced if the coefficients are fixed. The power reduced will be of 18%. The fixed coefficient can enhance the filters performance by reducing the power and the area.

The filter is designed using the using the VHDL code using the HDL designer from mentor graphics using TSMC .18um technology. We can implement the FIR filters in various fields such as general purpose computers, radars, wireless communication and audio processing applications. This This may enhance the systems performance by reducing the power.

6. ACKNOWLEDGEMENT

Our sincere thanks to the experts who contributed for the successful completion of the research.

7. REFERENCES

[1] H. Samueli, "An improved search algorithm for the design of multiplierless FIR filter with powers-of-two coefficients," IEEE Trans. Circuits Syst., vol. 36, no. 7, pp. 1044–1047, Jul. 1989.

[2] R. I. Hartley, "Subexpression sharing in filters using canonical signed digit multipliers," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 43, no. 10, pp. 677–688, Oct. 1996.

[3] O. Gustafsson, "A difference based adder graph heuristic for multiple constant multiplication

problems," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2007, pp. 1097–1100.

[4] J. Ludwig, H. Nawab, and A. P. Chandrakasan, "Low power digital filtering using approximate processing," *IEEE J. Solid-State Circuits*,vol. 31, no. 3, pp. 395–400, Mar. 1996.

[5] Sinha, A. Wang, and A. P. Chandrakasan, "Energy scalable system design," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 10, no. 2, pp. 135–145, Apr. 2002.

[6] K.-H. Chen and T.-D. Chiueh, "A low-power digit-based reconfigurable FIR filter," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 53, no. 8, pp.617-621,Dec 2006.

[7] Mahesh and A. P. Vinod, "New reconfigurable architectures for implementing filters with low complexity," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 29, no. 2, pp. 275–288, Feb. 2010.

[8] Z. Yu, M.-L. Yu, K. Azadet, and A. N. Wilson, Jr, "A low power FIR filter design technique using dynamic reduced signal representation," in *Proc. Int. Symp. VLSI Tech., Syst., Appl.*, 2001, pp. 113–116.

[9] K. Parhi, *VLSI Digital Signal Processing Systems: Design and Implementation*. New York:Wiley, 1999.

Speed Determination of Moving Vehicles using Lucas-Kanade Algorithm

Dolley Shukla
Shri Shankaracharya College of Engg. & Tech.
Junwani, Bhilai-490020
Durg,(CG), India

Ekta Patel
Shri Shankaracharya College of Engg. & Tech.
Junwani, Bhilai- 490020
Durg,(CG), India

Abstract: This paper presents a novel velocity estimation method for ground vehicles. The task here is to automatically estimate vehicle speed from video sequences acquired with a fixed mounted camera. The vehicle motion is detected and tracked along the frames using Lucas-Kanade algorithm. The distance traveled by the vehicle is calculated using the movement of the centroid over the frames and the speed of the vehicle is estimated. The average speed of cars is determined from various frames. The application is developed using MATLAB and SIMULINK.

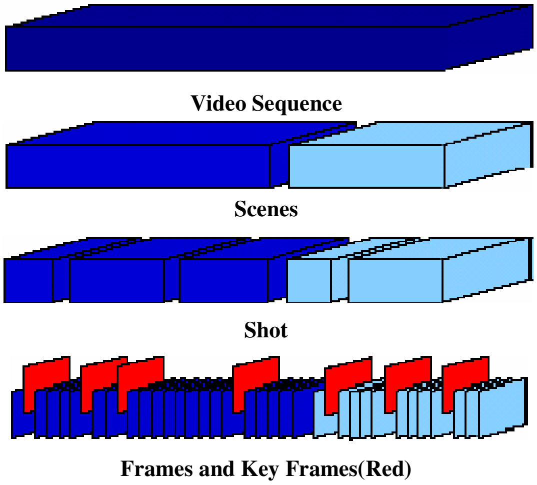
Keywords: Tracking, Optical flow, Motion estimation, Lucas-Kanade algorithm,velocity

1. INTRODUCTION

1.1 Video and Image Sequence:

Video is the technology of electronically capturing, recording, processing, storing, transmitting, and reconstructing a sequence of still images representing scenes in motion.[1] An image is a rectangular grid of pixels. It has a definite height and a definite width counted in pixels.

A video usually consists of scenes, and each scene includes one or more shots. A shot is an uninterrupted segment of video frame sequence with static or continuous camera motion, while a scene is a series of consecutive shots that are coherent from the narrative point of view.



Video Sequence

Scenes

Shot

Frames and Key Frames(Red)

Fig1: Hierarchical structure of Video Sequence

1.2 Motion estimation:

Motion estimation is an important task of video analysis. [1] It can be used to find the motion fields, to identify moving objects, calculate object trajectory and to find their velocity.

In this paper, we present an efficient method for computing direction of motion of a vehicle and estimate its speed.[1] The proposed method firstly uses optical flow algorithm to calculate changes in the intensity of the pixels of the images. These apparent velocity components are then subjected to image processing techniques to obtain centroid of the vehicle across the frames. The image coordinates of the centroid are mapped to World space. Using this information the velocity of the vehicle is estimated.

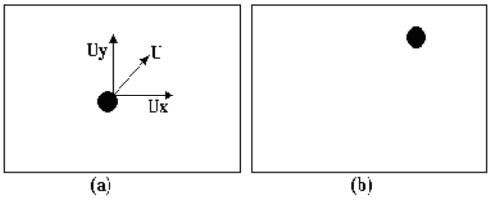


Fig2: Motion vector definition of current frame a) at time t-1 b) at time t

1.3 Methods of Motion Estimation:

1.3.1 Feature/Region Matching: Motion is estimated by correlating or matching features (e.g. edges) or regional intensities (e.g. blocks of pixels) from one frame to another. [1]

Examples include:

- Block-matching algorithm
- Phase correlation and frequency domain methods

***1.3.2 Gradient based methods*:** Gradient-based methods use spatial and temporal partial derivatives to estimate image flow at every position in the image.

- Optical flow
- Pixel recursive algorithms

2. LITERATURE REVIEW

Mehrubeoglu and McLauchlan[2] detect and count vehicles during day and night scenarios and different environmental conditions in 2006. This paper is an extension of the authors' work from detecting vehicles in still images to tracking vehicles in video.

In their paper, An *et al.* report a motion tracking algorithm that tracks different objects in motion in video.[3] The authors achieve motion tracking by segmenting key frames, and then clustering objects whose motion is close to the previously detected objects. Classification is achieved with a distance measure based on epicenter geometry.

Yu *et al.* describe an algorithm that estimates traffic density and average speed from Skycam MPEG compressed images.[4] The authors compute DCT coefficients and analyze motion vector projections across frames. Direction, magnitude and texture filters are used to eliminate redundant motion vectors. After mapping the image plane to world coordinates, the average vehicle speed is estimated over a video clip of 10 seconds, with a frame rate of 10 fps.

Anagnostopoulos *et al.* surveyed license plate recognition methods.[5] The authors broke license plate recognition into three parts, 1) license plate location, 2) license plate segmentation, and 3) character recognition. In addition, the authors have devised a database of license plate images and videos under varying lighting and environmental conditions that researchers may utilize as a common test set to enable comparisons of various algorithms.

Garibotto *et al.* utilize computer vision techniques to estimate a vehicle's speed from two images by tracking license plates and determining the distance traveled.[6] The speed is calculated by using this traveled distance and the time difference between the two images. The researchers describe both monocular as well as binocular vision systems. In our method, license plate information is not needed.

Pelegrí *et al.* developed and tested GMR magnetic sensors to determine car speeds.[7] The vehicle causes changes in the magnetic field of the sensor when it travels over the sensor. Their tracking technique did not use cameras, but is important to show the diversity of technology research for tracking and vehicle speed information.

Li *et al.* determined vehicle speeds by utilizing a CCD camera and looking at the vehicle positions in video frames.[8] The speed is determined geometrically by the two vehicle positions and their spatial relationship to the known fixed CCD camera position. In our work, the spatial relationship of a tracked vehicle across frames is determined through transformation of pixel locations from image to world coordinate system. Transformation to world coordinates and pixel calibration are achieved by using standard lane markings whose length and gap distance are standard and known.

He *et al.* developed an embedded system to take traffic measurements [9]. The authors used background subtraction to aid in vehicle detection. The researchers then used parallelograms for the regions of interest (ROI) due to the image distortion resulting from the camera position and to reduce the computational load.

3. METHODOLOGY

3.1 Implementation in Simulink:

The Simulink model for this project mainly consists of three parts, which are "Velocity Estimation", "Velocity Threshold Calculation" and "Object Boundary Box Determination".

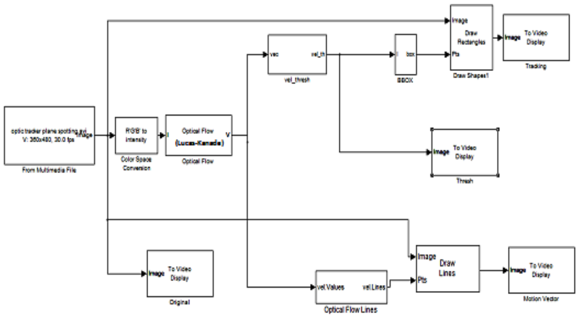


Fig3: Simulink Block Diagram for Tracking Moving Objects Using Lucas-Kanade Algorithm

3.2 Lucas-Kanade Algorithm:

The Lucas–Kanade method is a two-frame differential method for optical flow estimation developed by Bruce D. Lucas and Takeo Kanade.

It introduces an additional term to the optical flow by assuming the flow to be constant in a local neighbourhood around the central pixel under consideration at any given time.[10]

The additional constraint needed for the estimation of the flow field is introduced in this method by assuming that the flow ($V\,x$, $V\,y$) is constant in a small window of size m X m with m > 1, which is centered at Pixel x, y and numbering the pixels within as 1...n, n = m2, a set of equations can be found:

$$I_x(q_1)V_x + I_y(q_1)V_y = -I_t(q_1)$$

$$I_x(q_2)V_x + I_y(q_2)V_y = -I_t(q_2)$$

.

.

$$I_x(q_n)V_x + I_y(q_n)V_y = -I_t(q_n)$$

where $q_1, q_2, \ldots, q_n$ are the pixels inside the window, and $I_x(q_i), I_y(q_i), I_t(q_i)$ are the partial derivatives of the image I with respect to position *x*, *y* and time *t*, evaluated at the point q_i and at the current time.

These equations can be written in matrix form $Av = b$, where

$$A = \begin{bmatrix} I_x(q_1) & I_y(q_1) \\ I_x(q_2) & I_y(q_2) \\ \vdots & \vdots \\ I_x(q_n) & I_y(q_n) \end{bmatrix}, \quad v = \begin{bmatrix} V_x \\ V_y \end{bmatrix}, \quad \text{and} \quad b = \begin{bmatrix} -I_t(q_1) \\ -I_t(q_2) \\ \vdots \\ -I_t(q_n) \end{bmatrix}$$

The Lucas-Kanade method obtains a compromise solution by the least squares principle. Namely, it solves the 2×2 system

$A^TAv = A^Tb$ or

$\mathrm{v} = (A^TA)^{-1}A^Tb$ where A^T is the transpose of matrix A. That is, it computes

$$\begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} \sum_i I_x(q_i)^2 & \sum_i I_x(q_i)I_y(q_i) \\ \sum_i I_x(q_i)I_y(q_i) & \sum_i I_y(q_i)^2 \end{bmatrix}^{-1} \begin{bmatrix} -\sum_i I_x(q_i)I_t(q_i) \\ -\sum_i I_y(q_i)I_t(q_i) \end{bmatrix}$$

with the sums running from *i*=1 to *n*.

3.3 Steps Followed:

1. Input Video stream is captured.
2. Convert AVI file from RGB to Intensity.
3. The Intensity is then sent to Optical Flow block and velocity vectors in the form of matrix are obtained.
4. The matrix is then sent to 'Threshold and Region Filtering Block'.
5. Inside the block there is a Velocity Threshold block which calculates the mean threshold velocity and gives a binary threshold image.
6. This Threshold image is then divided into 2 halves using Submatrix block and processed individually. The video sequence is sent to Blob Analysis block. This block calculates statistics for labeled regions in a binary image. These labeled regions are known as blob.
7. The Blob Analysis block returns region of motion and the coordinates of centroid of the moving objects in the video sequence.
8. The Threshold Image (in Binary form), coordinates of Bounding box and centroid are sent to 'Display Results' block.
9. Centroid is superimposed on the original video using Draw Markers block.
10. The video obtained in step (9) is subtracted from original (divided) video to obtain image with centroid only.
11. The individual halves are stored in different AVI files.
12. The halves are concatenated to obtain the video sequence with superimposed centroid.
13. The video is then read and converted to frames.
14. Each image is converted from gray level to binary.
15. Reading each frame, the 2D coordinates of centroid for car are extracted and stored in a matrix with corresponding frame number.
16. The structure of the matrix is such that:

Frame Number	x - coordinate	y - coordinate

17. The calibration parameters for the fixed camera (calculated earlier) are used to convert 2D coordinates to 3D coordinates. That is, 2D Image coordinates are converted to 3D World coordinates using calibration parameters.[5]

 A new matrix is obtained:

Frame Number	X -coordinate	Y- coordinate	Z-coordinate

The Euclidean distance between each successive matrix element is calculated. Distance between 2 centroid P (xi,,yi, zi) and Q(xj,,yj, zj) in world space is calculated as

distij = √ (xi-xj)2 +(yi-yj)2+(zi-zj)2

Where n= total number of frames captured, i= 1 to n-1 and j=i+1 to n

18. The total distance traveled (in millimeters) by the object across the images is calculated. Total number of world coordinates traveled (in mm) is given by:

n-1 , n
D = Σ distij
i=1, j=i+1

19. This distance is converted to actual distance traveled (in centimeters) using pixel to distance ratio (ctod) which is calculated earlier (from preprocessing). The total distance traveled by the vehicle under consideration is calculated as:

 dtraveled = D * ctod

 Where dtraveled (in centimeters) is the total distance traveled by the vehicle.

20. The time of the motion (in seconds) is calculated using the following relation:

 ttraveled = n / fps

 Where n = number of frames for which motion of car was studied,

 fps = frame rate of the AVI (number of frames per second). This is obtained from the AVI information.

21. Estimated velocity of the vehicle in centimeters per second is calculated as:

 Vel (cm/s) = dtraveled (cm) / ttraveled (s) [11]

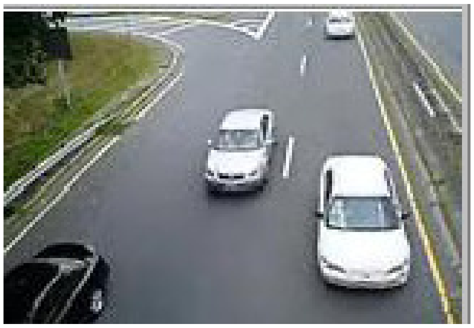


Fig 4.1: Original Video

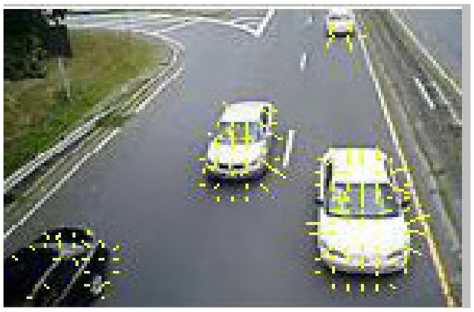


Fig 4.2: Motion Vector

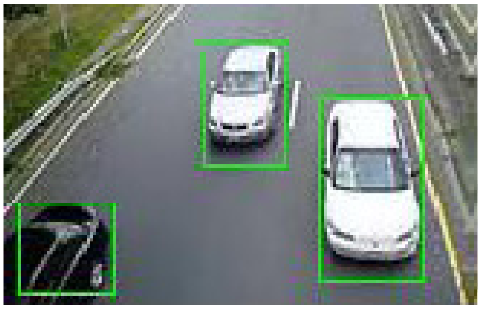


Fig 4.3: Tracking the vehicle

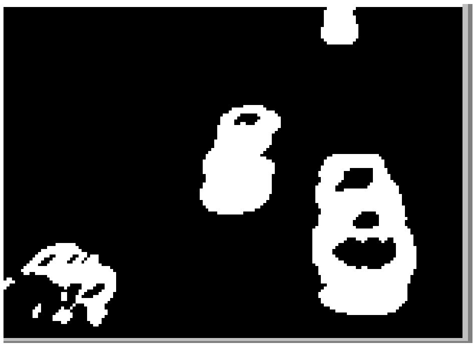


Fig 4.4: Thresholded Video

4. RESULTS

All the coding and matrix representations have been implemented in MATLAB. The proposed method was subjected to various experiments in order to check its accuracy and feasibility.

As a process of initialization, camera is calibrated and coordinate to distance ratio is calculated. Further, the video sequences were captured using a digital camera with 15 fps sample rate and resizing the images to 120 X160 pixel resolution.

The proposed method was first implemented for one vehicle.[12] A camera was mounted on a height and the video was captured. The calibration parameters were calculated using Calibration toolbox. The pixel to distance ratio was calculated and was stored for further analysis.

The experiment was repeated for multiple videos and 8 cars and the result is tabulated. Below are the output results in the form of Speeds and motion vectors of cars.[9]

Table 4.1: Average Speed of Cars

cars	1	2	3	4
Speed(km/h)	1.22	1.25	1.28	1.31

cars	5	6	7	8
Speed(km/h)	1.27	1.30	1.35	1.32

Table 4.2 : Motion Vectors of Cars

cars	1	2	3	4
Motion vector	0.3506	0.3548	0.3537	0.3586

cars	5	6	7	8
Motion vector	0.3671	0.3672	0.3753	0.3798

5. CONCLUSIONS & FUTURE WORK

The objective has been to detect moving objects and thereafter, calculate the speed of moving Vehicles and motion vector.[12] While earlier we worked with object-intrinsic properties such as the centroid of a moving object in order to make a probable prediction of its immediate future motion, methods to detect a rectangular boundary for the object, then used background subtraction Simulink models and but didn’t get fair output for multiple vehicles. Further we made an attempt using the Lucas-Kanade method. [13] Although that it does not yield a very high density of flow vectors, Lucas-Kanade Algorithm is robust in presence of Noise. Vehicle trajectory is shown in fig.5. It is window based local method. Average angular error is less in Lucas-Kanade algorithm. There exist fast and accurate optical flow algorithms which can be applied in future. Hence, in future local and global methods can be combined for requirement of dense flow estimate, preserve discontinuities and to make it robust to noise. .[14]

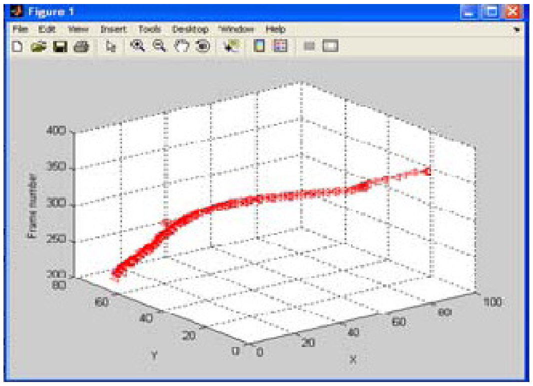


Fig 5: Vehicle Trajectory using Lucas-Kanade algorithm

6 REFERENCES

1. Y. Wang, J.Ostermann, Y.O.Zhang, E.F. (1995), “Video Processing and Communications”, Prentice Hall.

2. Mehrubeoglu, M. and McLauchlan, L., E.F. (2006), “Determination of traffic intensity from camera images using image processing and pattern recognition techniques”, Proc. SPIE-IS&T Electronic Imaging, SPIE Vol. 6063, 60630Q-1 -60630Q-12.

3. An, X., Qin, X. and Bao, H., E.F.(2006), “Automatic and robust classification of independent motions in video sequences”, Proc. SPIE-IS&T Electronic Imaging, Vision Geometry XIV, SPIE 6066, 60660B-1 – 60660B-8.

4. Yu, X.-D., Duan, L.-Y., and Tian, Q., E.F.(2002), “Highway traffic information extraction from skycam MPEG Video”, Proc.IEEE 5th International Conf. on Intelligent Transportation Sys., pp.37-42.

5. Anagnostopoulos, C.-N. E., Anagnostopoulos, I. E., Psoroulas, I. D., Loumos, V., and Kayafas, E., E.F.(2008), “License Plate Recognition From Still Images and Video Sequences: A Survey”, IEEE Trans. Intelligent Transportation Systems,9(3), pp.377-391

6. Garibotto, G., Castello, P., Del Ninno, E., Pedrazzi, P, and Zan, G., E.F.(2001), “Speed-vision: speed measurement by license plate reading and tracking”, Proc. IEEE Intelligent Transportation Sys. Conf. , pp.585-590.

7. Pelegrí, J., Alberola, J., and Llario, V., E.F.(2002), “Vehicle detection and car speed monitoring systems using GMR magnetic sensors”, Proc. IEEE 2002 28th Annual Conf. Industrial Electronics Society, pp.1693-1695.

8. Li, Y., Yin, L., Jia, Y., and Wang, M., E.F.(2008), “Vehicle speed measurement based on video images”, Proc. 3rd International Conf. Innovative Computing Information and Control, pp.439-442.

9. He, Z., Liu, Y., Yu, H., and Ye, X., E.F. (2008), “Optimized algorithms for traffic information collecting in an embedded system”, Proc. Congress on Image and Signal Processing, Vol. 4, pp. 220-223.

10. S. Baker, I. Matthews, E.F.(March 2004), ”Lucas-Kanade 20 Years On: A Unifying Framework”, IJCV, Vol.56, No. 3, pp. 221-255.

11. Lazaros Grammatikopoulos, George Karras, Elli Petsa, E.F.(November 2005), “Automatic Estimation of Vehicle Speed from Uncalibrated Video Sequences”, International Symposium on Modern Technologies, Education and Professional Practice in Geodesy and related fields, Sofia,pp.03 – 04.

12. Savan Chhaniyara, Pished Bunnun, Lakmal D. Seneviratne and Kaspar Althoefer, E.F.(MARCH 2008), “Optical Flow Algorithm for Velocity Estimation of Ground Vehicles: A Feasibility Study”, International Journal on smart sensing and intelligent systems, VOL. 1, PP. 1.

13. J.L. Barron, D.J. Fleet, S.S.Beauchemin, T.A. Burkitt, E.F. (1992), “Performance of Optical Flow Techniques”, Computer Society Conference on Computer Vision and Pattern Recognition, pp. 236-242.

14. A. M Tekalp, E.F(1995), “Digital Video Processing Englewood Cliffs”, NJ: Prentice-Hall.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 37-40, 2013

GENERIC APPROACH FOR VISIBLE WATERMARKING

S. Lilly Anusha
Dept. of EEE,
S V U College of Engineering,
Tirupati-517502, India

B. AnuRadha,
Dept. of ECE,
S V U College of Engineering,
Tirupati-517502,India

ABSTRACT: In this paper generic image watermarking technique is used for the copyright protection of color images. Watermarking with monochrome and translucent images based on One-to-One compound mapping of the values of the image pixels, which provide us the recovered image without any loss. Both the translucent full color and Opaque monochrome images are used in this paper. Two-fold monotonically increasing compound mapping is used to get more typical visible watermarks in the image. Measures have been taken to protect it from hackers.

KEYWORDS: Alpha Blending, one-to-one compound mapping, parameter randomization, mapping randomization, translucent watermark, two-fold monotonically.

1. INTRODUCTION:

Digital Image watermarking methods are usually classified into two types: visible and invisible [1-7]. The invisible watermarking aims to embed copyright information into host media, in case of copyright infringements, to identify the ownership of the protected host the hidden information can be retrieved. It is important that the watermarked image must be resistant to common image operations which ensure that the hidden information after alterations is still retrievable. On the other hand, methods of the visible watermarking yield visible watermarks. These visible watermarks are generally clearly visible after applying common image operations. In addition, ownership information is conveyed directly on the media and copyright violations attempts can be deterred.

In general Embedding of watermarks, degrade the quality of the host media. The legitimate users are allowed to remove the embedded watermark and original content can be restored as needed using a group of techniques, namely reversible watermarking [8-11]. However, lossless image recovery is not guaranteed by all reversible watermarking techniques, which means that the recovered image is same as the original. Lossless recovery is important where there is serious concerns about image quality such as include forensics, military applications, historical art imaging, or medical image analysis.

The most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region [6,9,11]. Another is to rotate consecutive watermark pixels to embed watermark that is visible [11].the watermarks of arbitrary sizes can be embedded into any host image.

Only binary visible watermarks can be embedded using these approaches.

A new method for lossless visible watermarking is proposed by using compound mappings which allow mapped values to be controllable The approach is generic, leading to the possibility of embedding different types of visible watermarks into cover images. Two applications of the proposed method are demonstrated; where we can embed opaque monochrome watermarks and nonuniformly translucent full-color ones into color images.

2. One to One compound mapping:

2.1Reversible one to one compound mapping:

Here, we propose a generic one-to-one compound mapping for converting a set of numerical values P={p1,p2,…pM},Q={q1,q2,…qM}, such that the mapping pi, qi for all i=1,2,3..M is reversible. Here, all the values of pi and qi are image pixel values (grayscale or color values) which are investigated for copyright protection applications.. The compound mapping f is governed by a one-to-one function F_x with one parameter x=a or b in the following way.

$q=f\ (p) = F_b^{-1}\ (F_a(P))$ ------ (1)

Where F_x^{-1} the inverse of $F_{x,}$ the one-to-one property leads to the fact that if $F_a(p)=P'$, then $F_a^{-1}(p')=p$ for all values of a and b. On the other hand F_a (p), and $F_b(p)$ generally are set to be unequal if a≠b.

The compound mapping described by (1) is reversible, that is p can be derived exactly from q using the following formula:

$p = f^{-1}\ (q) =Fa^{-1}(\ F_b(q))$-----(2)

Lemma 1 (Reversibility of compound Mapping):

If $q= F_b^{-1}\ (F_a(p))$ for any one-to-one function F_x with a parameter x, then $p= F_a^{-1}(F_b(q))$ for any values of a, b, p and q.

Proof: substituting (1) into $F_a^{-1}\ (F_b\ (q))$, We get $F_a^{-1}\ (F_b(q)) = F_a^{-1}\ (F_b(F_b^{-1}\ (F_a(P))))$.

By regarding $F_a(p)$ as a value c, the right-hand side becomes $F_a^{-1}\ (F_b(F_b^{-1}\ (c)))$ which after F_b and F_b^{-1} are cancelled out, becomes $F_a^{-1}(c)$. But $F_a^{-1}(c)=F_a^{-1}(F_a(p))$ which is just p after F_a and F_a^{-1} are cancelled out. hence proved $p= F_a^{-1}\ (F_b(q))$

As an example, if $F_x(p) =xp+d$, then $F_x^{-1}(p') = (p'- d)/x$.

Thus
$$\begin{aligned} q &= F_b^{-1}\ (F_a(p)) \\ &=F_b^{-1}(ap+d) \\ &=(ap+d-d)/b =ap/b \end{aligned}$$

And so we have
$$\begin{aligned} F_a^{-1}\ (F_b(q)) &= F_a^{-1}\ (b(ap/b)+d) \\ &= F_a^{-1}(ap+d) \\ &= [((ap+d)-d)/a] \\ &= ap/a \\ &= p \quad \text{------ (3)} \end{aligned}$$

2.2 Lossless Visible Watermarking

The proposed generic lossless visible watermarking using one-to-one compound mappings will be derived using the lemma 1, using which a variety of visible watermarks can be embedded into images. The embedding is reversible; the original image is recovered losslessly by removing the water mark. A preliminary lemma is first described as follows.

Lemma 2(preference of compound-mapped value q): it is possible to use the compound mapping $q=F_b^{-1}(F_a(p))$ to convert a numeric value p to other value which is close to a preferred value .

Proof: Let F_x (p) = p-x where x is the parameter for F. then $F_x^{-1}(p') = p'+x$. Also, let a = p-ε and b = l where ε is a small value. Then the compound mapping $F_b^{-1}(F_a(p))$ of p yields q as

$$q \;=\; f(p) \qquad = F_b^{-1}(F_a(P))$$
$$= F_b^{-1}(p\text{-}a) = F_b^{-1}(\varepsilon)$$
$$= \varepsilon+b = \varepsilon+l \quad \text{------ (4)}$$

This means that the value q is close to the preferred value l.

The above lemma is based on two assumptions. The first 'a' is close to 'p', or equivalently, that a=p - ε. The reason why we derive the above lemma for a=p - ε instead of a = p is that in the reverse mapping we want to recover p from q without knowing p, which is a requirement in the application of reversible visible watermarking investigated in this studies. Although the value of p cannot be known in advance for such applications, it can usually be estimated, and some techniques are described for such estimations.

The second assumption is that Fx (p) yield a small value if x and p are close.

Theorem 1: (Lossless Reversible Visible Watermarking)

There exist one-to-one compound mappings for use to embed into a given image a visible watermark whose pixel values are close to those of a given watermark, such that the original image can be recovered from losslessly.

Proof:

This is a consequence of Lemmas 1 and 2 after regarding the individual pixel values in I, L and Q respectively as those of p, l and q mentioned in Lemma 2. And it is clear by Lemma 1 that the value p can be recovered losslessly from the mapped value q which is derived in Lemma 2.

Algorithm 1:
Input: original image, watermark image.
Output: watermarked image (W).
Steps:

```
1) From the image I Select a set of P pixels in the res where
   the watermark is to be embedded, call P a watermarking area.
2) Corresponding set of pixels P in W are denoted by Q.
3) For each pixel X with value p in P, corresponding pixel in
   Q is denoted as Z and corresponding pixel Y in L as l and
   the conduct the following steps:
   a) Apply an estimation technique to derive a to be a value
      close to b using the value of the neighboring pixels of X
   b) Set 'b' to be the value 'l'.
   c) Map 'p' to a new value $q=F_b^{-1} (F_a (p))$.
   d) The value of Z is set to q.
```

Now, Set each remaining pixel value in W, outside the region P, to be equal to the corresponding pixel in 'I'.

Here we do not use the information of the original image pixel value of X itself for computing the parameters a and b for X.

As an example, the purpose performed by Step:3 of the above algorithm for a pixel is illustrated by figure .Here the color of the center pixel is estimated by using west and north pixels As the pixels are unknown to the receiver and covered by the watermark the east and south pixels are not used. Following algorithm describes removal process for watermarked image.

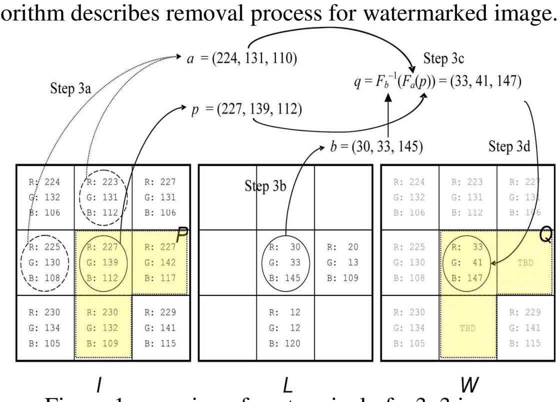


Figure 1: mapping of center pixel of a 3x3 image.

Algorithm 2:
Input: watermarked-image (W), a watermark (L).
Output: recovered image R from W.
Steps:

```
1) The watermarking area Q is selected in W as the area selected
   in Algorithm 1.
2) Value of each pixel in R is set, which is outside the region Q,
   to be equal to the corresponding pixel in W.
3) For each pixel Z with value q in Q, denote the corresponding
   pixel in the recovered image R as X and the value of the
   corresponding pixel Y in L as l, and conduct the following steps.
   a) Obtain the same value by applying the same estimation
      technique used.
   b) Set b to be the value l.
   c) Restore p from q by setting $p = F_a^{-1}(F_b (q))$.
   d) Set the value of X to be p.
```

2.3 Security considerations:

We want legitimate users to be able to recover the original image from a watermarked one; do not want an attacker to be able to do the same. Herein, we propose some security protection measures against illicit recoveries of original images. First, we make the parameters a and b in the above algorithms to be dependent on certain secret keys that are known only by the creator of the watermarked image and the intended receivers. This can be achieved by a simple technique that generate a pseudo-random sequence of numerical values using a secret key and these values are added to either or both of a and b pixels values in watermarking area and referred to as parameter randomization.

Another way of security protection is to make the choices of the positions for the pixels to be dependent on a secret key. Specifically, we propose to process two randomly chosen pixels (based on the security key) P in simultaneously as follows. Let the two pixels be denoted as X_1 and X_2 with values p_1 and P_2, respectively. The color estimates a_1 and a_2 corresponding to X_1 and X_2, respectively, are individually

derived as before using their respective neighbors. The parameters b_1 and b_2 are set to be the values l_1 and l_2 of the respective watermark pixels Y_1 and Y_2. Then, instead of setting the values of the watermarked pixels Z_1 and Z_2 to be $q_1=F_{b1}^{-1}(F_{a1}(p_1))$ and $q_2=F_{b2}^{-1}(F_{a2}(p_2))$ as before, we swap the parameters and set
$q_1=F_{b1}^{-1}(F_{a2}(p_2))$ and $q_2=F_{b2}^{-1}(F_{a1}(p_1))$.

The effectiveness of lossless recoverability does not effect by this parameter exchange, because the original pixel values can be recovered by the following compound mappings: $P_1=F_{a1}^{-1}(F_{b2}(q_2))$ & $p_2=F_{a2}^{-1}(F_{b1}(q_1))$. This technique is referred as mapping randomization..

Last, the position in the image where a watermark is embedded affects the resilience of the watermarked image against illicit image recovery attempts. In more detail, if the watermark is embedded in a smooth region of the image, an attacker can simply fill the region with the background color to remove the watermark irrespective of the watermarking technique used. The techniques such as adaptive positioning can be used to choose an appropriate position while embedding a watermark.

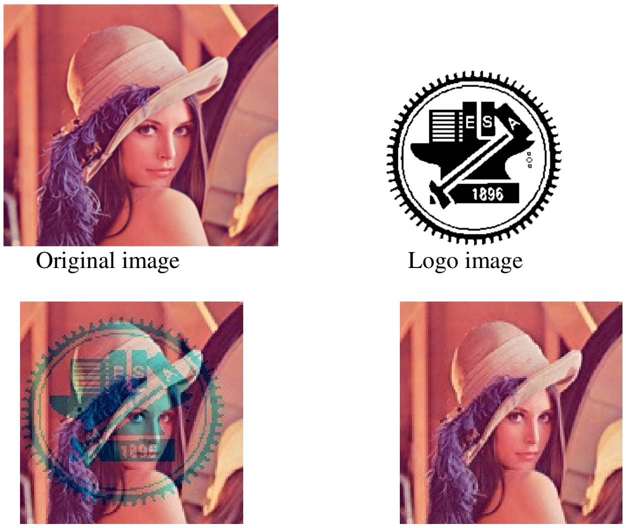
3. Experimental Results

In our experimental results for One-to-one compound mapping different color images of different sizes are used as cover images. And different logo images are used.

We measure the quality of watermarked images in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case PSNR should be infinite and MSE should be zero. But it is not possible for watermarked image. So, large PSNR and small MSE is desirable. To see that if the recovered watermark is identical to the one that is embedded we calculate only MSE. In this case it should be zero.

3.1 One to one compound mapping:

i. Lossless visible watermarking of opaque monochrome watermark:



Original image

Logo image

Watermarked image

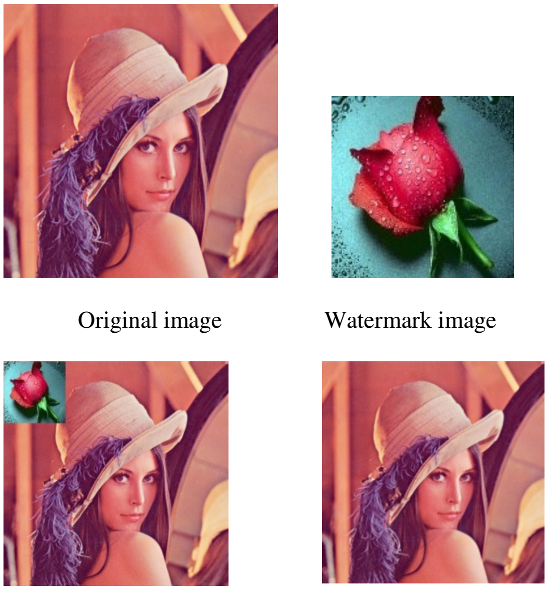
Recovered image

Figure 2: Experimental results of monochrome watermark embedding and removal.

The image has been recovered with MSE and PSNR values of MSE = 23.6935dB PSNR = 34.4185dB

ii. Lossless visible watermarking of translucent color watermarks:

For ease of discussions and comparisons, we always embed a watermark in the upper left-hand corner of an image in this study.



Original image

Watermark image

Watermarked image

Rrecovered image

Figure 3: Experimental results of translucent watermark embedding and removal.

The image has been recovered with MSE and PSNR values of MSE = 10.0308dB PSNR = 38.1515dB

3.3 Security Increase Results

In our watermarking method we used encryption. So in any case if watermarking key is leaked and attacker extracts the watermark, still he will not be able to read the watermark because it is encrypted.

In our watermarking method user need two keys for watermark extraction. If any of keys is invalid then user will not be able to extract watermark correctly. The watermark will be incorrect. It depends upon which key is invalid.

4. Conclusions:

One to one compound mapping:

A new method with a capability of lossless image recovery for reversible visible watermarking is given. one-to-one compound mappings is used which can map image pixel values to those of the desired visible watermarks. Relevant theorems and lemmas are described and proved to demonstrate the reversibility of the compound mappings for lossless reversible visible watermarking. Different types of visible watermarks are allowed to embed by compound mapping, and opaque monochrome watermarks as well as translucent full-color ones are described a as applications. A translucent watermark is clearly visible and visually appealing, thus more appropriate than traditional transparent binary watermarks in terms of advertising effect and copyright declaration. The two-fold monotonically increasing property of compound mappings was defined and an implementation proposed that can provably allow mapped values to always be close to the desired watermark if color estimates are accurate. Also described are parameter randomization and mapping randomization techniques, which can prevent illicit recoveries of original images without correct input keys. Experimental results have demonstrated the feasibility of the proposed method and the effectiveness of the proposed security protection measures.

5. Future scope:

Watermarking is an emerging research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field, spatially in the field of image watermarking. The reason might be that there are so many images available at Internet without any cost, which needs to be protected.

The watermarking technique that is given in this thesis can be further improved to increase the hiding capacity of images without affecting the imperceptibility of the images.

Future research may be applied to more applications of the proposed One to one compound mapping method and extensions of the method to other data types other than bitmap images, like DCT coefficients in JPEG images and MPEG videos.

6. REFERENCES:

[1] G. Braudaway, K. A. Magerlein, and F. Mintzer, “Protecting publicly available images with a visible image watermark,” in Proc. SPIE Int. Conf. Electronic Imaging, Feb. 1996, vol. 2659, pp. 126–133.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673– 1687, Jun. 1997.

[3] F.A.P Patitcolas, R.J.Anderson, and M.G.Kun“Information hiding- A survey”- Proc.IEEE,vol:87, no.7, jul. 1999.

[4] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, “Adaptive visible watermarking of images,” in Proc. IEEE Int. Conf. Multimedia Computing and Systems, 1999, vol. 1, pp. 568–573.

[5] S. P. Mohanty, K. R. Ramakrishnan, and M. S Kankanhalli, “A DCT domain visible watermarking technique for images,” in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding. Steganography and Watermarking Attacks and Countermeasures. Boston, MA: Kluwer, 2001.

[7] Y. Hu and S.Kwong,“Wavelet domain adaptive visiblewatermarking,” Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.

[8] Y. J. Cheng and W. H. Tsai, “A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks,” presented at the Int. Computer Symp. Workshop on Cryptology and Information Security, Hualien,Taiwan, R.O.C., Dec. 2002.

[9] P. M. Huang and W. H. Tsai, “Copyright protection and authentication of grayscale images by removable visible watermarking and invisible signal embedding techniques: A new approach,” presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan, R.O.C., Aug. 2003.

[10] Y. Hu, S. Kwong, and J. Huang, “An algorithm for removable visible watermarking,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 1, pp. 129–133, Jan.2006.

[11] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, “Lossless visible watermarking,” in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2006, pp. 853–856.

HANDLING CROSS-LAYER ATTACKS USING NEIGHBORS MONITORING SCHEME AND SWARM INTELLIGENCE IN MANET

G. Indirani
Department of CSE
Annamalai University
Annamalai nagar- 608002,
India

K.Selvakumar
Department of CSE,
Annamalai University,
Annamalai nagar- 608002,
India

ABSTRACT: The standard MAC protocol widely used for Mobile Adhoc Networks (MANETs) is IEEE 802.11. When attacks in MAC layer are left as such without paying attention, it could possibly disturb channel access and consequently may cause wastage of resources in terms of bandwidth and power. In this paper, a swarm based detection and defense technique is proposed for routing and MAC layer attacks in MANET. Using forward and backward ants, the technique obtains mean value of nodes between the first received RREQ and RREP packets. Based on this estimation, the source node decides the node as valid or malicious. Moreover the MAC layer parameters namely number of neighbors identified by the MAC layer, number of neighbors identified by the routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions are used to determine the node state. The source node uses these two node state estimation techniques to construct the reliable path to the destination. This proposed technique improves the network performance and at the same time prevents attackers intelligently.

KEYWORDS: MANET, MAC, RREQ, RREP, Neighbors monitoring scheme

1. INTRODUCTION

1.1 Mobile ad-Hoc networks (MANETs)

A Mobile ad hoc network is a collection of wireless mobile nodes that can allow people and devices to communicate with each other without the help of any existing centralized infrastructure. A MANET is a self configuring network to form an arbitrary and temporary network. Here each mobile node can function as a router or host. Often the topology of MANET changes as nodes are mobile. Here the routing protocol plays a major role in determining the routes required for communication between the source and destination through the intermediate nodes. The MANET gets new attractive applications since they offer good communication in the changing environment. The MANET can be used in the applications such as rescue operations, tactical operations, environmental monitoring, conferences, connecting soldiers in battlefields and social or business application such as Public and Personal Area Networks.[1] The weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [2].

1.2 General attacks in MANET

The MANETs are more prone to security att acks when compared to the wired networks. Due to the restricted features of the MANET such as restricted protection of every individual node, uneven behaviour of connectivity, deficit of certification authority, centralized monitoring or administration, security is difficult to maintain in these networks. In such a wireless network, attacks can enter either from inside the network or from outside. In any case, each node in MANET has to be ready for facing attacks. In particular, an attack from a compromised node inside the network is destructive and difficult to get identified. [3] Attacks in MANET are generally classified as active and passive attacks which are described below.

1.2.1 Active attacks:

An active attack causes various degrees of damage to the network depending on the type of attack. It is further classified into two categories of attacks such as internal and external attack.

- The internal attacks are performed by the compromised nodes that belong to the network.
- The external attacks are performed by the nodes that are not part of the network.

Wormhole attack, black hole attack, Byzantine attack, information disclosure and resource consumption attack are some of the examples of active attacks.

1.2.2 Passive attacks

In this attack, the attacker does not interrupt the regular behavior of the network but intrudes the data exchanged in the network without changing it. This type of attack is difficult to identify as the normal operation of the network is not affected. [3] [4]. There is an attack which is specific to the passive attack whose brief description about it is given below:

- **Snooping:**

  Snooping refers to the illicit use of another person's data. This may refer to watching e-mail informally that is displayed on another's computer screen or observing other people typing. Also more complicated snooping involves a software program to examine the process of a computer or network device. [5]

1.3 Cross layer attacks

Cross-layer attacks emerge from lack of interaction between MAC and routing layers. These attacks propagate from the MAC layer, where they are manifested as Denial of Service (DoS) attacks, to the routing layer, causing serious degradation of network performance in terms of the achieved throughput, latency and connectivity. An attacker can cause congestion in the network by either generating an excessive amount of traffic or by generating specific traffic patterns that prevent certain nodes from communicating with other nodes. [6]

1.3.1 Effects of cross layer attacks

(i) This type of attack exploits the vulnerability of a particular layer (attack point) to launch the attack, but ultimately aspires to disrupt the operations of another layer (target point) [7]

(ii) By incorporating cross-layer information and network communication into the jamming attack, a resource-constrained adversary can significantly increase the efficiency of the attack by targeting specific communication channels, helping to counteract the effect of the anti-jamming systems [9].

(iii) Reduces the attacker's probability being detected.

(iv) Reduce the cost to conduct the attack successfully

(v) Achieve the attack goals that may not be feasible through attack activities in a single layer.

1.3.2 *Issues of cross layer attacks*

(i) It is possible to modify/develop anomaly detection in each individual layer.

(ii) Cross layer defense architecture can be possible which may be based on all the layers and also individual layers.

(iii) The capability of attackers gets even more strengthened by the presence of cognitive radio. [9]

(iv) Due to the anonymization of the networks, the cross layer attackers have increased their efficiency [10].

1.4 Problem identification

The security issues in ad hoc routing have been extensively studied. However, attack strategies that target interaction between MAC layer and routing layer have not been fully addressed. A new class of attacks, cross-layer attacks, emerges from lack of interaction between MAC and routing layers. These attacks propagate from the MAC layer, where they are produced as Denial of Service (DoS) attacks, to the routing layer, causing serious degradation of network performance in terms of the achieved throughput, latency and connectivity.

In the previous works, only routing attacks considered (i.e) network layer attacks. As an extension work, cross-layer attacks are going to be considered which include both MAC and network layer and provide a detection technique using the same SWARM techniques.

2. LITERATURE REVIEW

Patrick Tague et al [8] investigate a class of coordinated jamming attacks in which multiple jammers collaboratively apply knowledge about the network layer functionality to efficiently reduce the throughput of network traffic. They show how a constrained optimization framework can be used to characterize coordinated jamming attacks and allow the impact of the attack to be quantified from the perspective of the network. Using this network-centric interpretation of jamming attacks, a network designer can attain a greater understanding of the potential threat of jamming. To illustrate their approach, they propose and evaluate a variety of metrics to model the attack impact, serving both as adversarial objective functions and as network evaluation metrics

Wenkai Wang et al [9] has proposed cross layer attacks and defending the cross layer attacks in cognitive radios. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. However, the attackers do not necessarily restrict themselves within the boundaries of network layers. In this paper, they design cross-layer attack strategies that can largely increase the attackers' power or reducing their risk of being detected. As a case study, we investigate the coordinated report-false-sensing data attack (PHY layer) and small-back-off-window attack (MAC layer). Furthermore, they propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion.

John Felix Charles Joseph et al[14] has proposed a cross-layer based routing attack detection system for ad hoc networks. Previous work that uses mostly audit trails collected from the routing protocol suffers from inadequacy of features to construct a reliable model for detecting anomalous routing behavior. On the other hand, use of linear detectors lead to very high false positives and false negatives because of the inherent on-linear nature of the feature space. In this work, these issues are addressed by collating features from multiple protocols at different layers and using a non-linear detector based on Support Vector Machine (SVM). The consequent problem of computational expense of the detection process is addressed by a combination of novel data reduction techniques. Simulation results show that the performance of the proposed CRADS is far superior than conventional protocol-specific detection systems.

Andriy Panchenko et al [10] have proposed a cross layer attack on anonymizing networks. Network layer anonymization protects only some of the user's personal identification information, namely network addresses of the communicating parties. However, even if the lower layers of communication provide perfect protection for the user's profile, information leakage on the application layer destroys the whole effort. Currently, all widespread implementations of anonymizing networks do not use a holistic approach and therefore, neither filter nor actively warn users about information leakage from the upper layers, which may look innocent to the end user. The extend existing work on security of anonymizing networks to take into account additional information leakage from the application layer. Further they show, under which conditions and how this kind of information can be used not only to build an extensive user profile at "low costs", but also to speed up traditional attacks that are targeted at the network layer identification of users' peer partners

Lei Guang et al [11] demonstrate a new class of protocol-compliant exploits that initiates at the MAC layer but targets ad hoc on-demand routing mechanisms. A misbehaved node implementing this type of attacks completely follows the specifications of IEEE802.11 standard and the existing on-demand routing protocols. However, it can cause routing shortcut attacks or detour attacks. They detail the exploits against two on-demand routing protocols: AODV and DSR. They evaluate the impact of such attacks on the network performance and propose Prevention from Shortcut Attack and Detour Attack (PSD) to mitigate their impacts.

A.Rajaram et al [12] have developed a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, they provide link-layer security using the CBC-X mode of authentication and encryption

3. PROPOSED SOLUTION

3.1 Overview

In this paper, a swarm based detection and defense technique for cross layer attacks is proposed in MANET. The technique makes use of ant colony based optimization (ACO) technique to detect attacks in the MANET. During route discovery time, the source broadcasts RREQ message and the destination responds with RREP message. In this broadcasting, each intermediate node stores the time of first received RREQ and RREP packets. The source injects forward ant (FA) to compute the mean value between received time of RREQ and RREP packets. The backward ant (BA) updates this information and reaches the source node. While receiving the mean value of nodes, the source compares mean value with predefined threshold value and marks node as valid and malicious node. To detect MAC layer attack, each node in MANET calculates D_n using four parameters namely number of neighbors identified by the MAC layer, number of neighbors identified by the routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions. When D_n is zero the node is identified as the valid node otherwise the node is identified as the malicious node. When the source constructs path to the destination, it chooses the path such that the path contains only the valid nodes by omitting malicious nodes.

3.2 Network architecture

In MANET, IEEE 802.11 is used as a standard MAC protocol. The Distributed Coordination Function

(DCF) in IEEE 802.11 combines Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with a Request to Send/Clear to Send (RTS/CTS) handshake technique to avoid collisions. Both hidden node and exposed problems are solved using RTS/CTS handshake mechanism. At MAC layer, data transmission channel is divided by inter packet gaps, which are termed as Inter Frame Spaces (IFS). Further, channel access can be provided to the nodes based on its priority. [13]

3.3 Swarm based node monitoring strategy

The MAC and routing layer must support each other to detect attacker and adversaries during the operations in MAC layer. It is possible to have more attacks in MAC layer. The attacker may pretend the channel as busy such that no node or user transmits their data. This attack consequently leads to DoS attack in the network, which drastically reduces the network performance. To detect and prevent such kind of attacks, our technique utilizes swarm based node monitoring strategy.

When the source has data to be transmitted, it broadcasts RREQ message and the destination broadcasts back the RREP message towards the source. While receiving RREQ message, each intermediate node records the time of first RREQ packet it has received. The RREQ packet is kept tacked with its RREQ sequence number. Similarly, each intermediate node stores the time and sequence number of first RREP packet it has received. The table that contains this information is known as counter table (C- Table). The format of C-table is shown in table – 1.

To monitor the network, the source periodically injects forward ants (FA) in the network. Each FA travels towards random destination to collect mean time between received times of RREQ and RREP packets. While returning from the destination, the backward ant (BA) updates this mean time in its pheromone table. Finally, the BA reaches the destination.

Every source has mean table (MN-Table) to store the mean times of nodes collected by ants. When the BA reaches the source node, it updates the mean value of nodes in M-Table. Let Th_{rd} be the route discovery threshold value. The source compares the mean value of every node with Th_{rd}. Mean value of nodes less than or equal to Th_{rd} are noted as valid nodes. Nodes that have mean value more than Th_{rd} are noted as malicious node.

Algorithm-1

```
1. Let $Th_{rd}$ be the route discovery threshold value

2. Consider $n_i$ be the mobile node, where i=1, 2…n and $mv_i$ be the mean value of node i

3. Each node stores time of first received RREQ and RREP packet in C-Table

4. FA and BA collect and update mv values of intermediate nodes in M-Table

5. Source compares $mv_i$ with $Th_{rd}$

        5.1 If ($mv_i \leq= Th_{rd}$) then

        5.2 Node is considered as valid node

        5.3 Else if ($mv_i > Th_{rd}$) then

        5.4 Node is considered as malicious node

6. End if
```

While constructing path from source to destination, the source considers the valid nodes rather than malicious nodes.

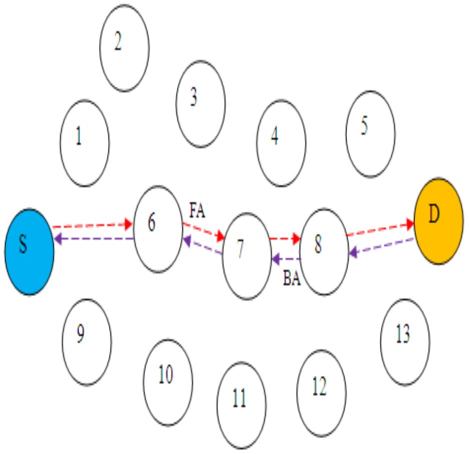


Figure-1 Mean value collection using Forward and Backward ants

Intermediate Node ID	Source ID	Destination ID	Received Time of RREQ Packet	Sequence Number of RREQ Packet	Received Time of RREP Packet	Sequence Number of RREP Packet

Table-1 Format of C-Table

3.4 Neighbors monitoring scheme

In this section, four parameters are monitored for each and every node in the MANET[14]. They are

1) Total number of neighbors found by the MAC layer which is denoted as N_{MAC}
2) Total number of neighbors found by the routing layer which is denoted as N_R
3) Total number of receptions found by the MAC layer which is denoted as R_{MAC}
4) Total number of receptions found by the routing layer which is denoted as R_R

Using these four parameters, D_N is calculated using the formula.

$$D_N \approx (|N_{MAC} - N_R|)\frac{(R_{MAC} - R_R)^2}{R_{MAc} + R_R} \qquad (1)$$

Algorithm-2

```
1. Let S and D be source and destination respectively
2. Let $D_N$ be the value calculated for every node in the network.
3. If ($D_N$ = 0) Then
        3.1 The node state is a valid node
4. Else if ($D_N$ not equal to 0) Then
        4.1 The node state is a malicious node
5. End if
```

This state of node is maintained by each node in MN-Table. The MN-Table has the following format,

Node ID	Mean Value	Node State

Table-2 Format of MN-Table

3.5 Data transmission through secure channel

While selecting path, the source uses the two node state detection techniques described in section 3.3 and 3.4. The source selects the path to the destination such that it contains only the valid nodes. Thereby, our technique provides defense against MAC layer attacks.

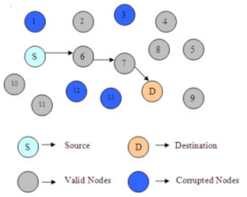


Figure-2 Secure Data transmission

4. SIMULATION RESULTS

4.1 Simulation model and parameters

Here the Network Simulator Version-2 (NS2) is used [14] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol is used. It has the functionality to notify the network layer about link breakage.

In this simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The numbers of nodes are varied as 20, 40, 60, 80 and 100. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In this simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in table 3

No. of Nodes	20, 40, 60, 80 and 100.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
No. Of Attackers	1,2,3,4 and 5.

Table 3: Simulation Settings

4.2 Performance metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average-end-to-end Delay: It is the total time delay taken by the nodes to transmit the data to the receiver.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

Here the Swarm Based Detection and Defense Technique using Neighborhood monitoring scheme for Routing and MAC layer Attacks (SBDT-NB) is compared with Cross-Layer Attack vs. Cross-Layer Defense (CACD) [9].

4.3 Results

A. Based on attackers

In the first experiment, the number of attackers are varied as 1, 2, 3, 4 and 5 in a 100 node network.

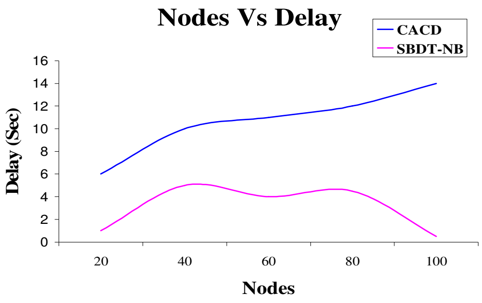


Figure 3: Nodes Vs Delay

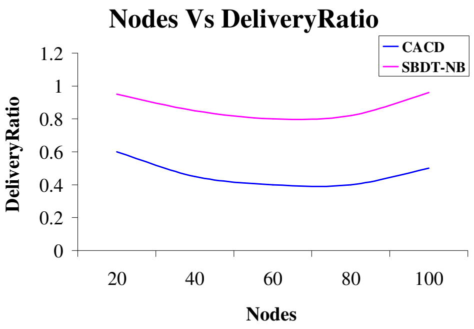


Figure 4: Nodes Vs Delivery Ratio

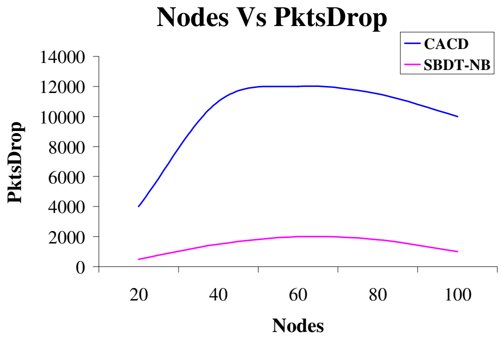


Figure 5: Nodes Vs PktsDrop

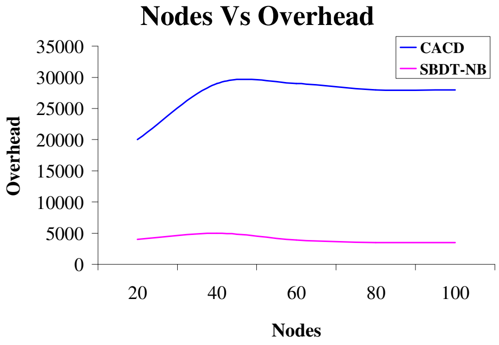


Figure 6: Nodes Vs Overhead

From figure 3, we can see that the delay of our proposed SBDT-NB is less than the existing CACD technique.

From figure 4, we can see that the delivery ratio of our proposed SBDT-NB is higher than the existing CACD technique.

From figure 5, we can see that the packet drop of our proposed SBDT-NB is less than the existing CACD technique.

From figure 6, we can see that the overhead of our proposed SBDT-NB is less than the existing CACD technique.

B. Based on nodes

In the second experiment we vary the number of nodes as 20, 40, 60, 80 and 100.

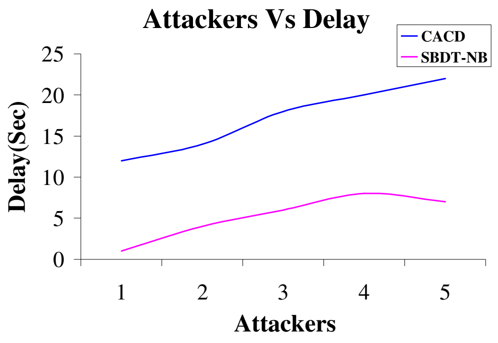


Figure 7: Attackers Vs Delay

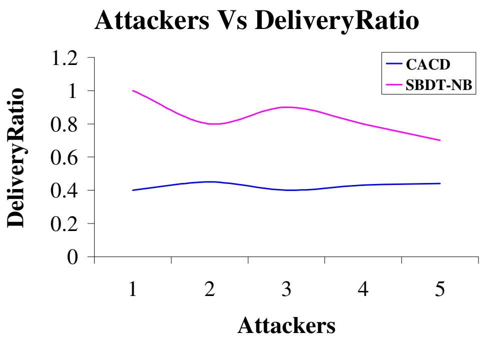


Figure 8: Attackers Vs Delivery Ratio

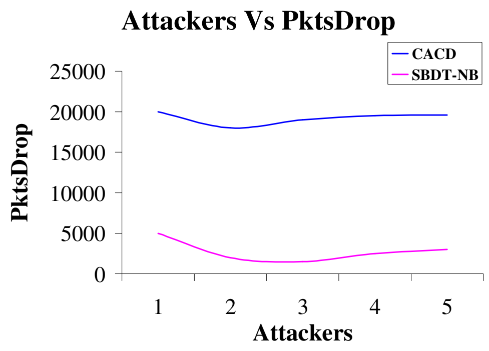


Figure 9: Attackers Vs Drop

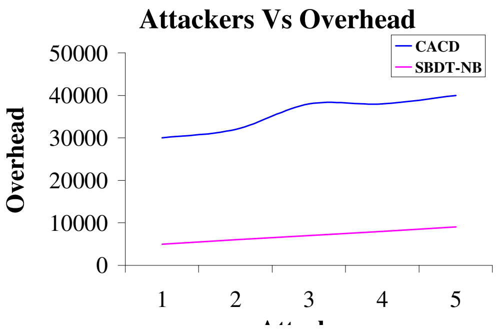


Figure 10: Attackers Vs Overhead

From figure 7, we can see that the delay of our proposed SBDT-NB is less than the existing CACD technique.

From figure 8, we can see that the delivery ratio of our proposed SBDT-NB is higher than the existing CACD technique.

From figure 9, we can see that the packet drop of our proposed SBDT-NB is less than the existing CACD technique.

From figure 10, we can see that the overhead of our proposed SBDT-NB is less than the existing CACD technique.

5. CONCLUSION

In this paper, a swarm based detection and defense technique with neighborhood monitoring scheme is proposed for cross layer attacks in MANET. Using forward and backward ants, the technique obtains mean value of nodes, which is the difference between first received RREQ and RREP packets. While receiving the mean value of nodes, the source compares mean value with predefined threshold value and marks node as valid and malicious node. Further, using the four MAC layer parameters the node state is identified. Using, these two node state estimation technique, the source constructs path to the destination by omitting the malicious nodes. The performance of our technique is proved through simulation results. This Proposed technique prevents attackers wisely and improves network performance.

6. REFERENCES

[1] Sevil ¸ Sen, John A. Clark, “A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks”, Proceedings of the second ACM conference on Wireless network security 2009

[2] Yian Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, International journal of computer applications, 2011

[3] Sureyya Mutlu, Guray Yilmaz, “A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs”, IARIA Seventh International Conference on Networking and Service, 2011

[4] N.Shanthi, DR.LGanesan and DR.K.Ramar, “Study of Different Attacks on Multicast Mobile Ad Hoc Network”, Journal of Theoretical and Applied Information Technology, 2009

[5] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security (IJCSS), 2009

[6] Svetlana Radosavac, Nassir Benammar and John S. Baras, “Cross-layer attacks in wireless ad hoc networks”, 38th Conference on Information Sciences and Systems (CISS), Princeton, March 17-19 2004

[7] Kaigui Bian, Jung-Min Park, and Ruiliang Chen, “Stasis Trap: Cross-Layer Stealthy Attacks in Wireless Ad Hoc Networks”, K. Bian, J.M. Park and R. Chen, "Stasis Trap: Cross- Layer Stealthy Attacks in Wireless Ad Hoc Networks", In Proceedings of IEEE GLOBECOM, 2006.

[8] Patrick Tague, David Slater, Guevara Noubir, and Radha Poovendran, “Quantifying the Impact of Efficient Cross-Layer Jamming Attacks via Network Traffic Flows”, Network Security Lab (NSL), University of Washington, Tech.Rep., 2009.

[9] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li, Zhu Han, “Cross-Layer Attack and Defense in Cognitive Radio Networks”, IEEE GlobeCOM, 2010

[10] Andriy Panchenko, Lexi Pimenidis, “Cross-Layer Attack on Anonymizing Networks”, IEEE International Conference on Telecommunications, (ICT 2008), pp-1-7, 2008.

[11] Lei Guang, Chadi Assi, and Abderrahim Benslimane, “Interlayer Attacks in Mobile Ad Hoc Networks”, Springer, Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science Volume 4325, pp 436-448 , 2006

[12] A.Rajaram, Dr. S. Palaniswami, “The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks”, International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010

[13] Yihong Zhou, Dapeng Wu and Scott M. Nettles, “Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems”, in proceedings of the Workshop on BWSA, BROADNETS, USA, 2004.

[14] John Felix Charles Joseph□, Amitabha Das□, Boon-Chong Seet†, Bu-Sung Lee, “CRADS: Integrated Cross Layer approach for Detecting Routing Attacks in MANETs”, WCNC proceedings,2008

[15] Network Simulator: http:///www.isi.edu/nsnam/ns

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 49-52, 2013

Functionality Based Fixing of Weight for Non-functional parameters of a web service

M.MohemmedSha
M.S University
Tirunelveli, India

C.Rajalakshmi, I.SherifBaig
Department of Computer Science
Achariya School of Business and Technology
Pondicherry, India

K.Vivekanandan
Dept of Computer Science and Engineering
Pondicherry Engineering College

Abstract: In recent years, web services open the way to global business development through B2B integration and they used with different business applications to accommodate their services. So while selecting a service, the first preference is given to the functional properties of the web service and then a best web service is selected from the list by considering the expected quality. The QoS of a web service is also depends on the variant nonfunctional parameters of its service which may subject to changes because of network and other related factors. While considering the performance of a service, the overall quality is always preferred but the actual functionality of the service is based on the weight fixed for the non functional parameters like response time, throughput, etc... So assigning functionality based weight for the non functional parameters are used to achieve the assured quality of the service. In this paper we are proposing the system that gives importance for the non functional parameters such as response time, throughput, availability, success ability, reliability for which the weight is set based on functionality and requirement of aparticular business application.

Keywords:SOA, SLA, WSLA, WSDL, UDDI, B2B, Quality of Services, QoS, Web Service

1. INTRODUCTION

The emergence of Web services make it possible to realize Business-to-Business Interoperability (B2B) by inter-connecting Web services provided by various organizations.The presence of multiple Web services with identical functionality, leads to select the best Web service based on their QoS. QoS encompasses a number of non-functional properties such as response time, throughput, availability, reliability, and reputation, etc.But setting appropriate weight for the parameters based on the user requirement paves the way to reach the actual functionality of the web service [2]. The static, dynamic attributes that are under and beyond the influence of service providers are also considered to set the weight for the non functional parameters. There are many cases that the web service cannot reach the customers requirement because the appropriate weight is not given to the non-functional parameters while selecting the web service. In this paper calculation of QoS of web service based on its functionality weight is proposed for the successful composition of multiple businesspartners according to some business process.

The framework of the proposed functionality based weight fixing for non functional parameter is discussed in section 2. Section 3 calculates the QoS of the web service for same weights of all parameters and the asserted values of weight as in the WSLA and Section 4 shows the experimental results.

2. FRAMEWORK FOR FUNCTIONALITY BASED WEIGHT

The framework consistsof the basic web service model components web service provider, web service consumer and the Web Service Level Agreement (WSLA) mutually agreed by both signing parties. In addition it has a third party broker which calculate the QoS information for every customer request into a QoS database by getting the measured values from the customer, provider application and the asserted values in the WSLA.

A measurement service implements the measurement function required both the customer and the service provider. The measurement functionality receives the measured metrics from the system's instrumentation. Instructions on how to measure a particular system parameter are defined in the measurement directives of a WSLA[8].

After getting the parametric values the third party broker receives the weight for each parameter as input from the WSLA that is mutually agreed by the signing parties while selection of the web service. The QoS can be evaluated based on this weight and compared with the assured quality [6]. If there is a violation the same can be reported to the top management of both the signing parties to take immediate action.

3. EVALUATION OF QoS BASED ON NON FUNCTIONAL PARAMETER WEIGHTS

Let WS_1,WS_2,WS_3,WS_4,WS_5 are the selected web services with the guaranteed level of quality parameters {P_1, P_2, P_3 …………..Pm} Where m ($1 \leq i \leq m$) in the WSLA.

Here the goal is to satisfy the customer requirements by assigning proper weights to all the non-functional parameters that are considered during the selection of a web service. For that a comparison between QoS for equal weight based parameter and weight based on functionality is made and the importance of fixing weight based on requirement is explained [3].

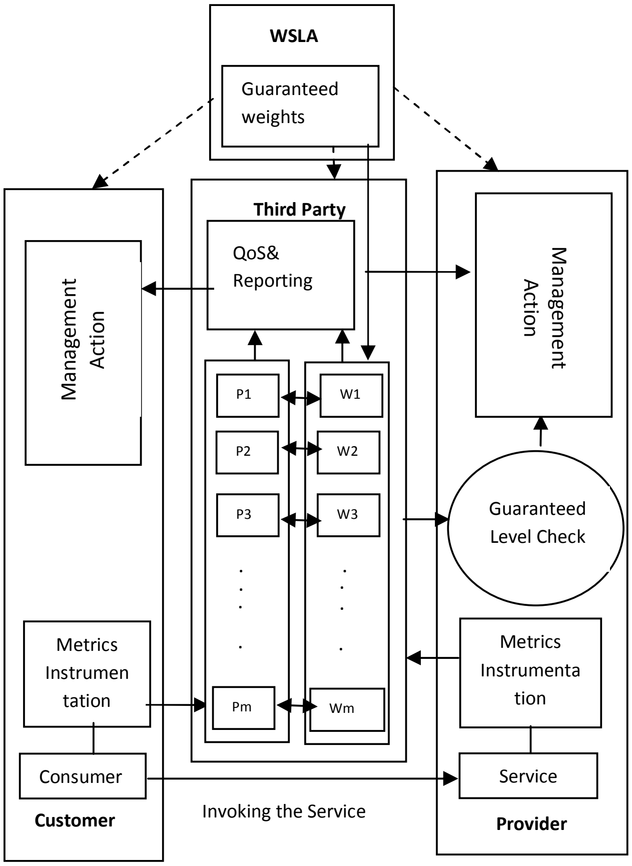


Figure 1. Framework of functionality based weight fixing

The basic metrics are measured by the customer and provider applications when the request is made. A measurement service used by the third party broker get the metrics from both the signatory parties and aggregated into composite metrics and SLA parameters which are used to calculate the actual quality of the web service [1].

Let the broker reports the management about the violation of QoS for every N requests.

These requests are equally divided into n sub requests and its average values is recorded and stored in the QoS database. The set $P_{ws\ AVG} = \{P_{1\ AVG}, P_{2\ AVG} \ldots\ldots P_{m\ AVG}\}$ is the average value for each quality parameter of the web service [1].

The parametric values are normalized as $P_{ws\ NOR} = \{P_{1\ NOR}, P_{2\ NOR}, \ldots\ldots P_{m\ NOR}\}$ and will be presented in the range of [0, 1].

The QoS for the web service can be calculated as follows

$$QoS = \frac{1}{m} \sum_{j=1}^{m} w_j . P_{j\ NOR}$$

Where $w_1, w_2, w_3, \ldots\ldots\ldots w_m$ are the weights assigned for the quality parameters.

The QoS of the web services are calculated in two phase for comparison. In the first phase an equal weight assigned for all parameters and in the second functionality based priority is given to the parameters [9]. The advantage of functionality based weight setting is studied to achieve better quality performance.

4. EXPERIMENTAL RESULTS

The average parametric values for the web services for every request 1000 is recorded for five web services under the study is as follows

Table 1. Average Non Functional Parametric Values

	P1	P2	P3	P4	P5
WS1	302.75	7.1	89	90	73
WS2	482	16	85	95	73
WS3	3321.4	1.4	89	96	73
WS4	126.17	12	98	100	67
WS5	107	1.9	87	95	73

The quality values are normalized between [0,1] as follows

Table 2. Normalized Parametric Values

	$P1_{NOR}$	$P2_{NOR}$	$P3_{NOR}$	$P4_{NOR}$	$P5_{NOR}$
WS1	0.51	0.51	0.48	0.56	0.59
WS2	0.49	0.56	0.53	0.44	0.56
WS3	0.39	0.37	0.45	0.45	0.41
WS4	0.41	0.60	0.53	0.61	0.49
WS5	0.52	0.40	0.53	0.63	0.39

4.1 QoS Based on Equal Weight Parameters

The weight = .75 is assigned for all the parameters to find the QoS of the web service

Table 3. Quality of equal weight parameters

	Q(P1)	Q(P2)	Q(P3)	Q(P4)	Q(P5)
WS1	0.38	0.38	0.36	0.42	0.44
WS2	0.37	0.42	0.40	0.33	0.42
WS3	0.29	0.28	0.34	0.34	0.31
WS4	0.31	0.45	0.40	0.46	0.37
WS5	0.39	0.30	0.40	0.47	0.29

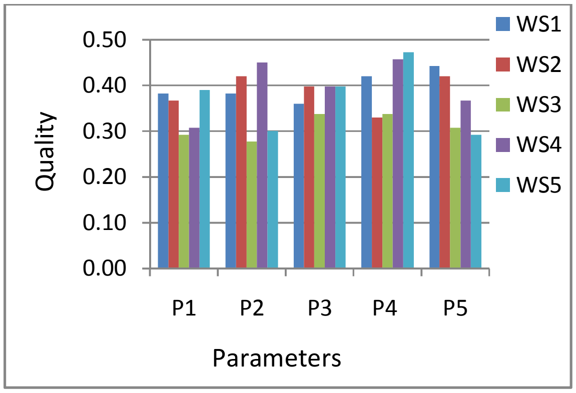


Figure 2. Performance of equal weight parameters

4.1 QoS Based on Functionality Weight Parameters

The following weights are assigned to the web services based on its functionality

Table 4. Functionality weights of web services

	W1	W2	W3	W4	W5
WS1	0.7	0.8	0.85	0.99	0.9
WS2	0.99	0.85	0.7	0.7	0.85
WS3	0.8	0.7	0.9	0.85	0.9
WS4	0.80	0.9	0.8	0.8	0.7
WS5	0.8	0.9	0.8	0.99	0.9

Table 5. Quality of functional weight parameters

	P1	P2	P3	P4	P5
WS1	0.36	0.41	0.41	0.55	0.53
WS2	0.49	0.48	0.37	0.31	0.48
WS3	0.31	0.26	0.41	0.38	0.37
WS4	0.33	0.54	0.42	0.49	0.34
WS5	0.42	0.36	0.42	0.62	0.35

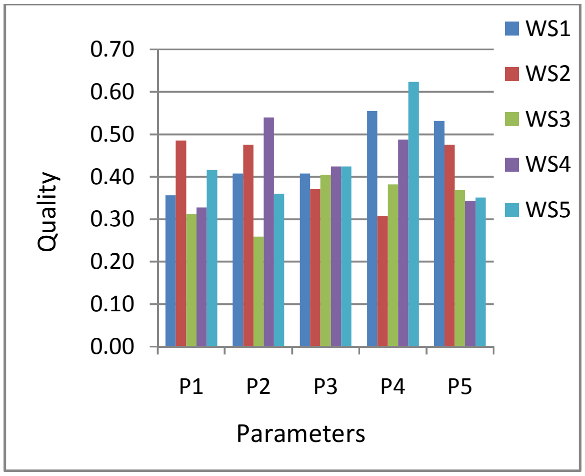


Figure 3. Performance of functional weight parameters

The overall QoS for both the phasesis shown in the table. There is a remarkable improvement in the quality of the web service that implements functionality based weight.

Table 6. QoS of equal and functional weight parameters

QoS of Web Services	WS1	WS2	WS3	WS4	WS5
Equal Weight	0.40	0.39	0.31	0.4	0.37
Functionality Weight	0.45	0.42	0.35	0.42	0.43

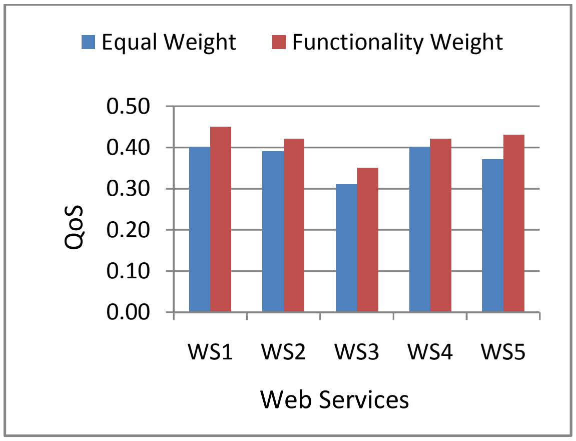


Figure 4. QoS of equal and functionality based Weights

5. CONCLUSION

For service selection non-functional QoS parameters are also considered along with the functional requirement. Fixing equal weight to all non functional parameter may result the improvement in overall quality, but considering better weigh for the parameter that improve the functionality of the of the web service. Mentioning the expected quality based on functional weight in the WSLA at the time of selection of a web service will pave the way to reach the expected functional requirement of a web service. Also the assertion in the WSLA is the mutual agreed values between the signing authorities of the web service and it forces the provider to reach the functional requirements for the success of the web service and the entire satisfaction of the customer.

6. REFERENCES

[1] M.MohemmedSha, I.SherifBaig, C.Rajalakshmi, P.Balaji and Dr. K.Vivekanandan " Automatic Pricing of Web Services Based on QoS" In: International Journal of Engineering Research and Technology Vol. 1 (02), 2012 ISSN 2278 - 0181.

[2] Al-Masr.E, Mahmoud," Discovering the Best Web Service" In: WWW 2007, Banff, Alberta, Canada, pp. 1257-2589 (2007).

[3] Ruth Lenon, John Murphy, "You can't always get what you want...-QoS in CWS", Generative Programming & Component Engineering for QOS Provisioning in Distributor System, UAB Computer & Information Science.

[4] A.Mani, A. Nagarajan, "Understanding Quality of Service for Web Services", Developer works. 01 Jan 2002. www.ibm.com/developerworks/library/ws-quality.html.

[5] DessislavaPetrova-Antonova, "Cost DependantQoS based Discovery of Web Services", Demetra EOOD (2010).

[6]MoloodMakhlughian, Seyyed Mohsen Hashemi, YousefRastegari and EmadPejman, "Web Service selection based on Ranking of QoS using Associative Classification" In: International Journal on Web Service Computing (IJWSC), Vol.3, No.1, March 2012.

[7] R. Lennon, J. Murphy, "Web Services Management and Selection": Applied Performance Mechanisms in Proceedings of ICCCN (San Diego, 2005), IEEE, 59.

[8] Kritikos K, Plexousakis D, “Requirements for QoS-Based Web Service Description and Discovery”, IEEE Transactions on Services Computing, Vol.2, Issue: 4, pp. 320-337,December 2009.

[9] P. Pabitha, J. Prabhu, A. Rajesh Kumar, R. Premadhasan, M. Rajaram, “Semantic Annotation and QoS Based Ranking of Web Services using User Preferences” European Journal of Scientific Research ISSN 1450-216X Vol.78 No.2 (2012), pp.293-303© EuroJournals Publishing, Inc. 2012.

[10] Kopecky J, Vitvar T, Bournez C, and Farrell J, “SAWSDL: Semantic Annotations for WSDL and XML Schema”, IEEE Internet Computing Journal, Vol.11, Issue: 6, pp. 60-67, December 2007.

[11] Yousefipour A, Neiat A.G., Mohsenzadeh M, Hemayati M.S., “An Ontology-based Approach for Ranking Suggested Semantic Web Services ”, 6th International Conference on Advanced Information Management and Service(IMS), pp. 17-22, December 2010.

[12] H. Kreger, Web Services Conceptual Architecture 1.0. IBM Software Group, May 2001.

[13] UDDI Version 2.0 API Specification, Universal Description, Discovery and Integration,uddi.org, June 2001.

[14] Dr. E. Kirubakaran, D. Ravindran, Dr. D. I. George Amalarathinam, “ Service Discovery Framework with Functional and Non-Functional Information (SDF)” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012 ISSN: 2277 128X

International Journal of Computer Applications Technology and Research (IJCATR)
Volume 2– Issue 1, 53-58, 2013

Formal Models for Context Aware Computing

Pooja Mohan
Department of IT, GGDSD College
Panjab University,
Chandigarh, India

Manpreet Singh
University College of Engineering,
Punjabi University,
Patiala, India

Abstract: Context-aware computing refers to a general class of mobile systems that can sense their physical environment, and adapt their behavior accordingly. In this paper we seek to develop a systematic understanding of context-aware computing by constructing a formal model and notation for expressing context-aware computations. This discussion is followed by a description and comparison of current context modeling and reasoning techniques.

Keywords: Context; Computing; Context Models; Reasoning; Ontology

1. INTRODUCTION

Context-awareness is considered as an important ingredient of today's most ubiquitous computing applications. The behavior of these applications is mostly characterized by embedding the interpretation logic of contextual information inside applications, creating problems for reusability of this information by other applications. Since ubiquitous computing is about interactive and smart environments, in order to enable such interactions, applications need a shared understanding of context to communicate and transfer contextual information effectively among them.

This study addresses the issue of how to represent and manage Context information. One approach is to model context using existing data modeling techniques from the field of information systems, and to store and manage the information using a database management system. It can be modeled by using both the Entity-Relationship model and the class diagrams of UML. According to study [1], UML constructs are more expressive than those provided by ER, but also correspondingly more cumbersome. It provides a graphical notation for modeling concepts in order to allow context models to be specified diagrammatically. This notation takes the form of a directed graph, in which entity and attribute types form the nodes, and associations are modeled as arcs connecting these nodes. Both the context toolkit [2] and the sensor architecture of Schmidt et al. [3] support the acquisition of context data from sensors, and the processing of this raw data to obtain high-level context information. The former is a programming toolkit that can be connected together to gather and process context information from sensors. The latter provides a layered model of context processing in which sensor output is transformed into one or more cues, which undergo processing to form an abstract context description comprising a set of values, each associated with a certainty measure that estimates the certainty that the value is correct.

Chan et al. [4] model (context-based) events and event's notifications in their context-aware middleware. Harper [5] proposes a context model for a web browsing; the model includes a web-specific hypertext containing user-specific context information presented within the page.

Semantics plays an important role in the interpretation of context and its changes as driving forces behind context-aware system's actions capturing the semantics of context is primarily done by using ontologies, i.e., particular models representing the nature and relationships of context. Bouquet et al. [6] propose a model for ontologies in context-aware systems. They express the model in the Web Ontology Language (OWL, [7]). Maamar and Narendra [8] takes the use of OWL further by proposing ontology-based context resolving techniques for composing of web services. Khedr and Karmouch [9] and van Kranenburg et al. [10] propose representation of context with the use of context *foundational*, *core* and *application* ontologies. Moreover, Guiling et al. [11] propose a generic ontology-based model for context query, matching and context-based policies.

Concerning semantics and context-awareness, Strang and Linnhoff-Popien [12] indicate the set of challenges, like distributed composition, partial validation, richness of quality of context information, incompleteness and ambiguity, to be tackled when modeling context. They categorize context models as a key-value, markup scheme-based, graphical (e.g. Unified Modeling Language), object-oriented, logic- and ontology-based.

They indicate the latter models as the most promising for the future.

Similarly, Razzaque et al. [13] indicate set-theory-based, directed-graph based and first-order-logic based context models, emphasizing the necessity of modeling user's preferences and profiles in comprehensive data structures exposing the dependency relations between the user's preferences and profiles.

2. CHARACTERISTICS OF CONTEXT INFORMATION

Several requirements have to be taken into account when modeling context information [14]:

2.1 Heterogeneity and mobility: Context data obtained from databases or digital libraries—like geographic map data—are often static. Many context-aware applications are also mobile or depend on mobile context information sources. This adds to the problem of heterogeneity as the context information provisioning must be adaptable to the changing environment. Also, location and spatial layout of the context information play important roles due to this requirement.

2.2 Relationships and dependencies: There exist various relationships between types of context information that have to be captured to ensure correct behavior of the applications. One such relationship is dependency whereby context information entities/facts may depend on other context information entities.

2.3 Timeliness: Context-aware applications may need access to past states and future states (prognosis). Therefore, timeliness (context histories) is another feature of context information that needs to be captured by context models.

2.4 Imperfection: Due to its dynamic and heterogeneous nature, context information may be of variable quality. In fact, it may even be incorrect. Most sensors feature an inherent inaccuracy and the sensed values age if the physical world changes, so that this inaccuracy increases over time. Thus, a good context modeling approach must take these problems into account to enable proper reasoning about context information changes to achieve appropriate adaptations for the application, and thus provide an experience for the user that is consistent with the physical world.

2.5 Reasoning: Context-aware applications use context information to evaluate whether there is a change to the user and/or to the environment situation; taking a decision whether any adaptation to that change is necessary often requires reasoning capabilities. Reasoning techniques can also be adopted to derive higher level context information.

3. CONTEXT MODELING APPROACHES

3.1 Graphical Models of context information

A very well known general purpose modeling instrument is the *Unified Modeling Language (UML)* which has a strong graphical component (UML diagrams). Due to its generic structure, UML is also appropriate to model the context. This is shown for instance by Bauer in [15], where contextual aspects relevant to air traffic management are modeled as UML extensions.

Another example is the nicely designed graphics oriented context model introduced in [16] by Henricksen et al., which is a context extension to the Object-Role Modeling (ORM) approach [17] according some contextual classification and description properties. In ORM, the basic modeling concept is the *fact*, and the modeling of a domain using ORM involves identifying appropriate fact types and the roles that entity types play in these. Henricksen extended ORM to allow fact types to be categorized, according to their persistence and source, either as *static* (facts that remain unchanged as long as the entities they describe persist) or as *dynamic*. The latter ones are further distinguished depending on the source of the facts as either *profiled*, *sensed* or *derived* types. Another quality indicator introduced by Henricksen is a history fact type to cover a time-aspect of the context. The last extension to ORM made by Henricksen for context modeling purposes are fact dependencies, which represent a special type of relationship between facts, where a change in one fact leads automatically to a change in another fact: the *dependsOn* relation. This kind of approach is particularly applicable to derive an ER-model from it, which is very useful as structuring instrument for a relational database in information system based context management architecture such as the one described in [18].

Halpin [19] describes the Rmap procedure for transforming a conceptual schema to a relational schema, and Henricksen [20] has developed an extension of Rmap that can be used to map a CML-based context model to a relational database. However, the formal semantics of ORM and CML can be leveraged to provide integration with other implementations such as fact-based reasoners (though it should be noted that some features of CML—particularly the constructs related to imperfect information—may not be supported). CML leverages the formality of ORM to support the evaluation of simple assertions as well as SQL-like queries.

3.2 Spatial context model

Space is an important context in many context-aware applications. Most context definitions mention space as a vital factor: e.g., Schilit, Adams and Want define three important aspects of context as "Where you are, who you are with and what resources are nearby" [21]. Thus, some context modeling approaches give space and location a preferential treatment. Most spatial context models are fact-based models that organize their context information by physical location. Spatial context models can be described along the tiers of spatial ontologies proposed by A. Frank [22]: Ontology based models of context information typically cover all 4 tiers. Although the tiered model of Frank is just an abstract conceptualization of different (spatial) representations of the world, it is useful to distinguish between various implementations of spatial context models.

The spatial context model developed in the Nexus project (called Augmented World Model [23]) is an object-based class hierarchy of context information that supports multi-inheritance. In contrast to the Nexus model, the Equator project context model [24] is a typical contextual ontology that represents all tiers by an OWL class model. Its location model is a hierarchical notion of inter-connected symbolic spaces, such as Buildings, Floors and Rooms. Properties define spatial relations between these spaces. Although the ontology also offers coordinate features, Millard et al. states that it is very hard to perform any inference over them using a normal reasoner, as they are usually not spatially aware.

3.3 Ontology based models of context information

Ontologies are essentially descriptions of concepts and their relationships; it is not surprising that the subset of the OWL language admitting automatic reasoning (i.e., OWL-DL) is indeed description logic. The formalism of choice in ontology-based models of context information is typically OWL-DL [25] or some of its variations, since it is becoming a de-facto standard in various application domains, and it is supported by a number of reasoning services. By means of OWL-DL it is possible to model a particular domain by defining classes, individuals, characteristics of individuals (data type properties), and relations between individuals (object properties). For instance, given two atomic classes Person and Female, the class Male can be defined as: Male ≡ Person ¬Female

Various OWL ontologies have been proposed for representing shared descriptions of context data. Among the most prominent proposals are the SOUPA [26] ontology for modelling context in pervasive environments, and the CONON [27] ontology for smart home environments. OWL-DL ontological models of context have been adopted in several architectures for context-awareness; among the others, we recall the Context Broker Architecture (CoBrA) [28] and the SOCAM [29] middleware, that adopt the SOUPA and CONON ontologies, respectively.

3.4 Logic Based Models

A logic defines the conditions on which a concluding expression or fact may be derived (a process known as reasoning or inferencing) from a set of other expressions or facts. To describe these conditions in a set of rules a formal system is applied. In a logic based context model, the context is consequently defined as facts, expressions and rules. One of the first logic based context modeling approaches has been researched and published as *Formalizing Context* in early 1993 by McCarthy and his group at Stanford [30, 31]. McCarthy introduced contexts as abstract mathematical entities with properties useful in artificial intelligence. He prevented emphatically to give a definition what context is. Instead he tried to give a formalization recipe which allows for simple axioms for common sense phenomena, e.g. axioms for static blocks worlds situations, to be *lifted* to context involving fewer assumptions, e.g. contexts in which situations change. Thus lifting rules, which relate the truth in one context to the truth in another context, are an important part of the model itself. The basic relation in this approach is *ist(c, p)*, which asserts that the it proposition p is true in the *context c*. This allows for formulas such as *c0: ist(contextof("Sherlock Holmes stories"), "Holmes is a detective")*, where c0 is considered to be an outer context. A similar approach is the *Sensed Context Model* proposed by Gray and Salber [32]. They use first-order predicate logic as a formal representation of contextual propositions and relations. Another approach within this category is the multimedia system by Bacon et al. [33]. In this system the location as one aspect of the context is expressed as facts in a rule based system. The system itself is implemented in Prolog.

3.5 Key Value Models

The model of key-value pairs is the most simple data structure for modeling contextual information. Already Schilit et al. [21] used key-value pairs to model the context by providing the value of context information (e.g. location information) to an application as an environment variable. The key-value modeling approach is frequently used in distributed service frameworks. In such frameworks, the services itself are usually described with a list of simple attributes in a key-value manner, and the employed service discovery procedure operates an exact matching algorithm on these attributes.

3.6 Markup Scheme Models

Common to all markup scheme modeling approaches is a hierarchical data structure consisting of markup tags with attributes and content. In particular, the content of the markup tags is usually recursively defined by other markup tags. Typical representatives of this kind of context modeling approach are *profiles*. They usually base upon a serialization of a derivative of *Standard Generic Markup Language (SGML)*, the superclass of all markup languages such as the popular XML. Some of them are defined as extension to the *Composite Capabilities / Preferences Profile (CC/PP)* [34] and *User Agent Profile (UAProf)* [35] standards, which have the expressiveness reachable by RDF/S and a XML serialization. An example of this approach is the *Comprehensive Structured Context Profiles (CSCP)* by Held et al. [36]. Drawback of CC/PP, the restricted overriding mechanism of default values only, replaced by a more flexible overriding and merging mechanism, allowing for instance to override and/or merge a whole profile subtree. A similar approach to CSCP is the *CC/PP Context Extension* by Indulska et al. [37]. They extended the basic CC/PP and UAProf vocabulary by a number of component-attribute trees related to some aspects of context, e.g. concerning location, network characteristics, application requirements, session information as well as certain types of relations and dependencies. Another context modeling approach in the markup scheme category – which does not bear towards CC/PP – is the *Pervasive Profile Description Language (PPDL)* [38]. This XMLbased language allows accounting for contextual information and dependencies when defining interaction patterns on a limited scale. There are several other context modeling approaches in the markup scheme category. They are oftentimes either proprietary or limited to a small set of contextual aspects, or both. Examples affected by these limitations are, among others, the *context configuration* of Capra et al.'s reflective middleware [39] the *Centaurus Capability Markup Language (CCML)* [40], *ConteXtML* [41].

3.7 Object Oriented Models

Common to object oriented context modeling approaches is the intention to employ the main benefits of any object oriented approach - namely encapsulation and reusability – to cover parts of the problems arising from the dynamics of the context in ubiquitous environments. An approach within the object category is the *Active Object Model* of the GUIDE project [42]. Again, the chosen approach has been primarily driven by the requirement of being able to manage a great variety of personal and environmental contextual information while maintaining scalability. All the details of data collection and fusing (e.g. the context adaptive composition of HTML fragments) are encapsulated within the active objects and thus hidden to other components of the system.

3.8 Hybrid models

Henricksen et al. [43] propose a hybrid approach to context modelling, combining ontologies with the fact based approach provided by the CML language. The goal is to combine the particular advantages of CML models (especially the handling of ambiguous and imperfect context information) with interoperability support and various types of reasoning provided by ontological models. The hybrid approach is based on a mapping from CML modeling constructs to OWL-DL classes and relationships. It is worth noting that, because of some expressivity limitations of OWL-DL, a complete mapping between CML and OWL-DL cannot be obtained.

With respect to interoperability issues, the advantages gained by an ontological representation of the context model are clearly recognizable. However, with respect to the derivation of new context data, experiences with the proposed hybrid model showed that ontological reasoning with OWL-DL and its SWRL extension did not bring any advantage with respect to reasoning with the CML fact-based model. For this reason, ontological reasoning is performed only for automatically checking the consistency of the context model, and for semantic mapping of different context models. [44] Presents creation of generic context ontology, and a location-based context model. The designed ontology is called COMANTO and describes general context types and interrelationships that are not domain-, application- or situation-specific. The location-based context model proposed focuses on addressing context management challenges in distributed pervasive environments, and is integrated with the COMANTO context knowledge. The combined modeling approach aims to enable efficient management of context data and allow for widely applicable context formalism.

4. CONCLUSION

In the paper we presented a set of requirements that context modeling and reasoning techniques should meet. The discussion of the requirements was followed by a description of the most prominent, approaches to context modeling. These approaches are rooted in database modeling techniques and in ontology based frameworks for knowledge representation. Spatial models provide efficient procedures for the execution of typical spatial queries; however, they do not always cope with the uncertainty of actual location readings. With regard to fact-based models, the CML language has advantages in its support for software engineering and in the good balance between expressive power and efficient reasoning procedures for that language. Indeed, the predicate logic supported by CML is well suited for expressing dynamic situations. However, in order to preserve efficiency, that language is less expressive than ontological languages like OWL-DL. Finally, ontological models have clear advantages regarding support for a) interoperability, b) heterogeneity, and c) representation of complex relationships and dependencies among context data. However, when considering the tradeoff between expressiveness and complexity, the choice of ontological models may not always be satisfactory.

5. REFERENCES

[1] Karen Henricksen, K., Jadwiga Indulska, J., "Modeling Context Information in Pervasive Computing Systems", 2002, pp. 167–180.

[2] Dey, A., Salber, D., Abowd, G., "A context-based infrastructure for smart environments", in: 1st International Workshop on Managing Interactions in Smart Environments (MANSE'99). (1999), pp. 1-15.

[3] Schmidt, A., et al. "Advanced interaction in context" In: 1st International Symposium on Handheld and Ubiquitous Computing (HUC'99), Karlsruhe (1999)

[4] Chan, A., et al., "An Event-Driven Middleware for Mobile Context Awareness", The Computer Journal, 2004, 47(3), pp. 278-288.

[5] Harper, S., "Middleware to Expand Context and Preview in Hypertext", In ACM SIGACCESS conference on Computers and accessibility. 2004. Atlanta, GA, USA: ACM Press.

[6] Bouquet, P., et al., "C-OWL: Contextualizing Ontologies", In Second Intl Semantic Web Conference (ISWC03). 2003. Las Vegas, Nevada, USA: Springer Verlag.

[7] Zuo, Z. and M. Zhou, "Web Ontology Language OWL and its description logic foundation", In 4th Intl Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT03). 2003: IEEE Press.

[8] Maamar, Z. and N.C. Narendra, "Ontology-based Context Reconciliation in a Web Services Environment: From OWL-S to OWL-C", In Workshop on Web Services and Agent-based Engineering (WSABE). 2004. New York City, USA.

[9] Khedr, M. and A. Karmouch, "ACAI: Agent-Based Context-aware Infrastructure for Spontaneous Applications", Journal of Network & Computer Applications, 2005. 28(1): pp. 19-44

[10] Kranenburg, H., et al., "Grounded Contextual Reasoning enabling Innovative Mobile Services", In 5th Workshop on Applications and Services in Wireless Networks (ASWN05). 2005. Grenoble, France, pp. 93-102

[11] Guiling, W., J. Jinlei, and S. Meilin, " A Context Model for Collaborative Environment". In 10th Intl. Conference on Computer Supported Cooperative Work in Design. 2006: IEEE Press., pp. 1-6

[12] Strang, T. and C. Linnhoff-Popien., "A Context Modeling Survey", In UbiComp 1st Intl Workshop on Advanced Context Modeling, Reasoning and Management. 2004.

[13] Razzaque, M.A., S. Dobson, and P. Nixon., "Categorization and Modeling of Quality in Context Information", In Workshop on AI and Autonomic Communications (IJCAI05). 2005.

[14] Shehzad, A., Hung Q. Ngo, Kim Anh Pham, and S. Y. Lee, "Formal Modeling in Context Aware Systems", http://*citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.131.1231*

[15] Bauer, J., "Identification and Modeling of Contexts for Different Information Scenarios in Air Traffic", Mar. 2003. Diplomarbeit.

[16] Henricksen, K., Indulska, J., and Rakotonirainy, A., "Generating Context Management Infrastructure from High-Level Context Models", In Industrial Track Proceedings of the 4th International Conference on Mobile Data Management (MDM2003) (Melbourne/Australia, January 2003), pp. 1–6.

[17] Halpin, T. A., "Information Modeling and Relational Databases: From Conceptual Analysis to Logical Design", Morgan Kaufman Publishers, San Francisco, 2001.

[18] Indulska, J., Robinsona, R., Rakotonirainy, A., and Henricksen, K., "Experiences in using cc/pp in context-aware systems", In LNCS 2574: Proceedings of the 4th International Conference on Mobile Data Management (MDM2003) (Melbourne/Australia, January 2003), M.-S. Chen, P. K. Chrysanthis, M. Sloman, and A. Zaslavsky, Eds., Lecture Notes in Computer Science (LNCS), Springer, pp. 247–261.

[19] Halpin, T. A., "Conceptual Schema and Relational Database Design", 2nd ed., Prentice Hall Australia, Sydney, 1995.

[20] Henricksen, K., "A framework for context-aware pervasive computing applications", Ph.D. thesis, School of Information Technology and Electrical Engineering, The University of Queensland (September 2003).

[21] Schilit, B, Adams, N., R. Want, et al., "Context-aware Computing Applications", Xerox Corp., Palo Alto Research Center, 1994.

[22] Frank, A., "Tiers of ontology and consistency constraints in geographical information systems", International Journal of Geographical Information Science 15 (7) (2001), pp. 667–678.

[23] Nicklas, D., Mitschang, B., “The Nexus Augmented World Model: An extensible approach for mobile, spatially aware applications”, 7th International Conference on Object-Oriented Information Systems.2001, pp. 392-401

[24] Millard, I., D. De Roure, Shadbolt, N., “The use of ontologies in contextually aware environments”, In Proceedings of First International Workshop on Advanced Context (2004), pp. 42–47.

[25] Horrocks, I., Patel-Schneider, P.F., F. van Harmelen, “From SHIQ and RDF to OWL: The making of a web ontology language”, Journal of Web Semantics 1 (1) (2003), pp. 7–26.

[26] H. Chen, F. Perich, T. W. Finin, A. Joshi, “SOUPA: Standard Ontology for Ubiquitous and Pervasive Applications”, in: 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2004), IEEE Computer Society, 2004.

[27] D. Zhang, T. Gu, X.Wang, “Enabling Context-aware Smart Home with Semantic Technology”, International Journal of Human-friendly Welfare Robotic Systems 6 (4) (2005), pp. 12–20.

[28] Chen, H., Finin, T., Joshi, A., “Semantic Web in the Context Broker Architecture”, in: Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom 2004), IEEE Computer Society, 2004.

[29] Gu, T., Wang, H. K. , Pung, H.K., Zhang, D.Q., “An ontology-based context model in intelligent environments”, in: Proceedings of Communication Networks and Distributed Systems Modeling and Simulation Conference, San Diego, California, USA, 2004.

[30] McCarthy, J., “Notes on formalizing contexts”, In Proceedings of the Thirteenth International Joint Conference on Artificial Intelligence (San Mateo, California, 1993), R. Bajcsy, Ed., Morgan Kaufmann, pp. 555–560.

[31] Mccarthy, J., and Buva., “Formalizing context”. In Working Papers of the AAAI Fall Symposium on Context in Knowledge Representation and Natural Language (Menlo Park, California, 1997), American Association for Artificial Intelligence, pp. 99–135.

[32] Gray, P., Salber, D., “Modelling and Using Sensed Context Information in the design of Interactive Applications”, In LNCS 2254: Proceedings of 8th IFIP International Conference on Engineering for Human-Computer Interaction (EHCI 2001), May 2001, M. R. Little and L. Nigay, Eds., Lecture Notes in Computer Science (LNCS), Springer, p. 317 ff.

[33] Bacon, J., Bates, J., Halls, D., “Location-oriented multimedia”, IEEE Personal Communications 4, 5 (1997).

[34] W3C. Composite Capabilities / Preferences Profile (CC/PP). http://www.w3.org/Mo- bile/CCPP.

[35] Wapforum. User Agent Profile (UAProf). http://www.wapforum.org.

[36] Held, A., Buchholz, S., Sachill, A., “Modeling of context information for pervasive computing applications”, In Proceedings of SCI 2002/ISAS 2002 (2002).

[37] Indulska, J., Robinsona, R., “Experiences in using cc/pp in context-aware systems”, In LNCS 2574: Proceedings of the 4th International Conference on Mobile Data Management (MDM2003) (Melbourne/Australia, January 2003), M.-S. Chen,P. K. Chrysanthis, M. Sloman, and A. Zaslavsky, Eds.,Lecture Notes in Computer Science (LNCS), Springer, pp. 247–261.

[38] Chtcherbina, E., Franz, M., “Peer-to-peer coordination framework (p2pc): Enabler of mobile ad-hoc networking for medicine, business, and entertainment”, In Proceedings of InternationalConference on Advances in Infrastructure for Electronic Business, Education, Science, Medicine, and Mobile Technologies on the Internet (SSGRR2003w) (L’Aquila/Italy, January 2003).

[39] Capra, L., Emmerich, W., Mascolo, C., “Reflective middleware solutions for context-aware applications”, 2001.

[40] Kagal, L., Korolev, V., Chen, H., Joshi, A., Finin, T., “Project centaurus: A framework for indoor mobile services”.

[41] Ryan, N., “ConteXtML: Exchanging Contextual Information between a Mobile Client and the FieldNote Server”, August 1999.

[42] Cheverst, K., Mitchell, K., Davies, N., “Design of an object model for a context sensitive tourist GUIDE”, Computers and Graphics 23, 6 (1999), pp. 883–891.

[43] Henricksen, K., Livingstone, S., Indulska, J., “Towards a Hybrid Approach to Context Modeling, Reasoning and Interoperation”, in: J. Indulska, D. D. Roure (eds.), Proceedings of the First International Workshop on Advanced Context Modelling, Reasoning And Management, in conjunction with UbiComp 2004, Nottingham, England: University of Southhampton, 2004.

[44] Roussaki, I., Strimpakou, M. et al, "Hybrid context modeling: A location-based scheme using ontologies," percomw, pp.2-7, Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), 2006

A survey of service Discovery Architecture of MANET with AODV-SD

Bela I. Patel
Institute of Science and
Technology for Advanced
Studies and Research
Vallabh Vidhyanagar,
India

Abstract: Mobile Adhoc Network (MANET) is network of a no. of mobile routers and associated hosts, organized in a random fashion via wireless link. MANET has been widely used for not only military purposes but for search-and- rescue operations, intelligent transportation system, data collection, virtual classrooms and ubiquitous computing. There are various Issues in MANET like Routing, MAC Layer issues, Transport protocol, QoS, Data Mgt. And Security etc. from them Service Discovery is one of the most important issues in MANET. Service discovery technologies are exploited to enable services to advertise their existence in a dynamic way, and can be discovered, configured and used by other devices with a minimum of manual efforts. Most of the service discovery protocols such as DEAPspace, UPnP, Konark, Salutation, Jini, and SLP. These protocols don't provide an appropriate route from consumer to service provider. Hence after services are discovered, a route request needs to be initiated in order to access the service. In this paper proposing an efficient, robust and flexible approach to service discovery for MANET that not only discovers a service provider, but at the same time, it also provides a route to access the service.

Keywords: Mobile Ad hoc Networks, Service Discovery and Service, Discovery Protocols, Jini, UPnP, Konark, SLP, Salutation.

1. INTRODUCTION

A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multichip radio network and maintaining connectivity in a decentralized manner. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference.

In MANET service discovery is most important issue. A service can be anything that can be useful for someone. For example when a labourer works for cleaning a house, he is giving his services for which he is paid. Similarly a professor teaches to his students providing them knowledge that is useful for students. This act of teaching is a service provided by a professor to his students. So, service can be defined as any facility provided by a device that can be useful for any other device. A service could be a software service like providing an implementation of some algorithm (for example, converting one audio file format to another) on a device so that when some device needs this service, it can contact that device and use it. A service can also be a hardware service like a printer that can be used by a mobile device to print a file. To get benefit from these services a device must be able to locate them in the network and also have the ability to invoke these services. Service Discovery Protocols (SDPs) provide such capabilities to devices.

In this paper, proposing an efficient, robust and flexible approach to service discovery in mobile ad-hoc network. First, we will provide a review of existing approaches of service discovery architecture with its advantages and disadvantages. We will then discuss our proposing approach to service discovery. Finally we will conclude the paper with future work.

2. LITERATURE REVIEW

Service Discovery Protocols can be defined as "Service Discovery Protocol is n/w protocols which allow automatic detection of devices and services offered by these devices on a computer n/w."The service discovery protocols proposed in paper that is classified as;

- Directory less architecture (DEAPspace, UPnP, Konark).
- Directory based architecture.

"A directory is an entity that stores information about services available in the network so as to enable service discovery and invocation."

The directory based architecture can be divided into two categories:

a. Centralized directory architecture (Salutation, Jini, and SLP)
"Relies on one or a few centralized directories that store the descriptions of all services available in the network."

b. Distributed directory architecture.

"Directories are further distributed and deployed dynamically."

1. infrastructure-less distributed directory architecture
2. Infrastructure-based distributed directory architecture.

JINI Architecture
Basic Jini Functions

- ✓ Allows a service (hardware, software) to make itself known to the community.
- ✓ Allows clients (browsers, OSs, hardware) within a community to discover services of interest.

- ✓ Network Communication between peers.
- ✓ Knowledge of the network terrain.
- ✓ Finding services.
- ✓ Utilizing services.

Advantages

- ✓ Scalable Implementation of architecture.
- ✓ OS and hardware independence.
- ✓ Scalable Scope (local to internet URL).
- ✓ Requires more limited apriority knowledge.
- ✓ Jini provides a more flexible and robust service discovery infrastructure for building distributed components comparing to other systems.
- ✓ The Jini object code offers direct access to the service using an interface known to the client.
- ✓ This code mobility replaces the necessity of pre-installing drivers on the client.
- ✓ The Jini specifications are open source and may be used freely.
- ✓ The code mobility appears as an efficient solution for supporting information retrieval.
- ✓ The Jini discovery infrastructure supports both unicast and multicast service discovery protocol.
- ✓ Jini systems provide mechanisms for service construction, lookup, communication, and use in a distributed system.
- ✓ Examples of services include devices such as printers, displays, or disks; software such as applications or utilities;

Disadvantages

- ✓ The problem is that the code mobility is very complex in an environment which bandwidth is a scarce resource and users' mobility makes continuous communication.
- ✓ Since code mobility gives to the users the access to other machines, security is a concern and the literature hardly addresses the security of MANET.
- ✓ The nodes should be designed to define in such a way that the peers accept the others' code.
- ✓ Since code mobility gives to the users the access to other machines, security is a concern, and the literature hardly addresses the security of Ad Hoc networks.
- ✓ Bleeding edge technology, not supported by industry yet
- ✓ Network Appliance market is very much embedded hardware based, and Java is not yet.

UPNP Architecture

Actions in UPNP (Universal Plug and Play)

- ✓ Discover devices & services
- ✓ Get a description of the device
- ✓ Control discovered devices
- ✓ Be informed of events indicating changes in the device
- ✓ Use a presentation prepared by the device to present a control

Advantages

- ✓ Universal Plug and Play is the youngest of these protocols, and it is still in an early state of development.
- ✓ Microsoft plans to implement it for all Windows platforms.
- ✓ The specifications and a sample source code are available freely.
- ✓ It is processor, operating system and communication protocol independent.

Disadvantages

- ✓ UPnP is designed for TCP/IP networks only.
- ✓ In its current version, it does not allow clients to search for service attributes.

SALUTATION Architecture

Salutation architecture is composed of two major components:

- Salutation Manager(SLM)
  The Salutation Manager is the core of the architecture, similar to the Lookup Service in Jini.
- Transport Manager.
  Provides reliable communication channels, regardless of the underlying network transport.

SLM can be discovered by services in a number of ways such as:

- ✓ Using a static table that stores the transport address of the remote SLM.
- ✓ Sending a broadcast discovery query using the protocol defined by the Salutation architecture.
- ✓ Inquiring the transport address of a remote SLM through a central directory server. This protocol is undefined by the Salutation architecture; however, the current specification suggests the use of SLP.
- ✓ The service specifies the transport address of a remote SLM directly.

Advantages

- ✓ Salutation is independent on the network technology and may run over multiple infrastructures, such as over TCP/IP and IrDA.
- ✓ It is not limited to HTTP over UDP over IP, as UPnP is.
- ✓ Moreover, Salutation is independent on the programming language, i.e., it is not limited to nor does it have a prerequisite for Java (as Jini).
- ✓ Its major advantage compared to UPnP and Jini is that there already exist commercial implementations.
- ✓ A Salutation Manager sits on the Transport Managers that provide reliable Communication channels, regardless of what the underlying network transports are.
- ✓ The Salutation Manager provides a transport-independent interface to Server and Client applications.
- ✓ Salutation can operate in any network, including IP, IR and, in the future, wireless. This transport independence is the strongest feature of Salutation.

Disadvantages

- ✓ The Salutation is well defined but confined to the service discovery protocol and session management.
- ✓ Salutation accordingly doesn't address features like remote event notification, which are no doubt useful in distributed environment.

SLP Architecture

SLP (service location Protocols) offers the following services:

- ✓ Obtaining service handles for User Agents.
- ✓ Maintaining the directory of advertised services.

- ✓ Discovering available service attributes.
- ✓ Discovering available Directory Agents.
- ✓ Discovering the available types of Service Agents.

Advantages

- ✓ SLP offers a flexible and scalable architecture and the utilization of service templates make service browsing and human interaction possible.
- ✓ Since SLP is able to operate with or without a DA, it is suitable for networks of different sizes, ranging from very small ad hoc connectivity to large enterprise networks.
- ✓ SLP also includes a leasing concept with a lifetime that defines how long a DA will store a service registration.
- ✓ SLP also can conduct in the distributed scenario without DAs, where UAs repeatedly multicast Attribute Request to network and receive the unicast replies from SAs directly.
- ✓ This mode provides a relative simple structure for service discovery in small network (such as home LAN).
- ✓ SLP is developed by an open and vendor independent forum and its implementation is freely available. We expect SLP to play a major role in service discovery.
- ✓ SLP is independent on the programming language.
- ✓ The SLP also supports a simple service registration leasing mechanism that handles the cases where service hardware is broken but the services continue to be advertised

Disadvantages

- ✓ Tends to increase the bandwidth usage

2.1 Existing Approach Vs Proposed Approach

After analyzing the Existing service discovery protocols it can be concluded that The Existing service discovery protocols don't provide an appropriate route from consumer to service provider. Hence, after services are discovered, a route request needs to be initiated in order to access the service. AODV, Totally different approach of service Discovery, Provided a service Discovery at network layer. As a result when a service discovery request is initiated to discover a service, a route is also established towards the service provider. Hence, when the client wants to use the service, a new route request is not required. It offers "quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, Determines unicast routes to destinations within the ad -hoc network".

3. OVERVIEW OF AODV-SD

We have extended The AODV protocol to perform service discovery; we call this extension AODV-SD.RREQ, RREP, RERR. Three message types are defined by AODV. In order to perform service discovery with AODV, we have extended the formats of the RREQ and RREP messages. Every node will be periodically broadcasting the services provided by it to its peer nodes

3.1 Service Discovery with AODV

New fields were defined, but also actions that nodes along the network perform when receiving these extended messages. whenever a node requires a service, it performs a lookup in its service table, services table maintains a information about services provided by current node as well as information about services provided by other nodes, The current node services information itself when the node in initialized, or when new service is initialized within the node while the other node services information is acquired when the current node participates in service discovery process. Each row in a services table contains the service identifier (a string that uniquely identifies the service), its IP address, a lifetime is used to keep information up to date, and a list of attributes that varies with the type of service and URL path. (Figure 1).

Service ID	Port	Protocol	IP Address	Lifetime	Attributes List	URL Path

Figure. 1 Services Table

A node can contact a service provider to use service, if the service information in its service table has a valid route to the service provider, and if the service lifetime is still valid; otherwise node has to initiate a discovery process by sending an RREQ message with extensions, known as SREQ. Recall that these extensions are fields added to regular RREQ, so it is possible to the locate the service (IP address of the service provider), as well as a route to it, simultaneously. RREQ message extension includes a Type field to identify a SREQ message, the Length of the extension, the Service ID field Length, Attributes List field length, service ID and attribute list with an optional values used to include restrictions in the useful service. (Figure 2).

1 byte	1 byte	1 byte	1 byte

Type	Length	Length Service ID	Length Attributes List
Service ID			
Atributes List			

Fig 2. Format of SREQ messages

When a node receives an SREQ it executes several following actions. First, it determines a valid association (Service name, IP address) for the required service is already available in its services table; that means if it provides the service or if it knows a valid route to a node that can provide it. If particular information is found, the node issues an RREP message with extensions for service discovery, also known as SREP, and sends it to the requesting node. SREQ and SREQ messages are transmitted through the network according to the rules at the AODV protocol, so both service provider routes will be found, as well as the reverse route, will be found. the RREP message extension includes the following fields: a Type to identify SREP messages, the extensions Length, lifetime of service, the service URL Length, and finally the URL itself (Figure 3).

1 byte	1 byte	1 byte	1 byte

Type	Length	LifeTime	
URL Length	URL		

Fig 3 . Format of SREP messages

If a node contains an association (service name, IP address) to a service, but does not have a valid route to it, then it assigns this IP address as the address to resolve issuing an SREQ. Any node receiving an SREQ with a valid destination address sends an SREP if it has a route to the destination node or if it knows an equivalent route to the service required. Otherwise, if it does not have information about the service required, or a route to the destination node, it will only forward the SREQ message. If a node receives an SREP and already has information about the service required, it compares the lifetime with the lifetime contained in its service table; if the information in the table is more recent, then it discards the message received and issues an SREP with that information. Otherwise, it will simply send the message to its destination.

4. SIMULATION PARAMETERS

We adopted the LBNL network simulator (ns) to evaluate the effects of performance of ad hoc routing protocols. The ns is a very popular software for simulating advanced TCP/IP algorithms and wireless ad hoc networks. To simulate our approach, we have developed our own simulation software. The simulator creates n nodes dynamically and links them randomly. Every node is randomly chosen to be either capable of storing or not storing advertisements. Nodes are randomly assigned a number of services.

5. CONCLUSION

In this paper we explored several architecture choices for service discovery with its advantages and disadvantages from them the proposed AODV approach is very flexible, efficient and can be adopted to work in any environment. In addition to it not only pull the service provider information on demand, but a node will also be pushing the service advertisements periodically along with route information.

6. FUTURE WORK

We can improve the current work to represent the service using better representation language like DAML etc. In addition, broadcasting of service advertisement right now done periodically. We can improve the broadcasting mechanism.

7. REFERENCES

[1] Dante Arias Torres, J. Antonio Garcia-Macias, "Service Discovery in Mobile Ad-hoc Networks by Extending the AODV Protocol", Proc. 2nd Mobile Computing Workshop (ENC' 04). Colima, Mexico. Sept. 2004. ISBN 970-692-170-2

[2] A Novel Approach to Service Discovery in Mobile Adhoc Network by Noman Islam Zubair A. Shaikh

[3] "Understanding Universal Plug and Play", White Paper, UPnP Forum (http://www.upnp.org), June 2000.

[4] Cho, C. and Lee, D., "Survey of Service Discovery Architectures for Mobile Ad hoc Networks", Term paper, Mobile Computing, CEN 5531, Department of Computer and Information Science and Engineering (CICE), University of Florida, Fall, 2005.

[5] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004, ISSN 1682-6027, © 2004 Asian Network for Scientific Information.

[6] "JiniTm Architecture Specification", Version 1.0.1, November 1999.

[7] Service Location Protocol, "RFC 2608", http://www.ietforg, June 1999.

[8] Michael Nidd, "Reducing Power Use in DEAPspace Service Discovery", IBM Research Zurich Research Laboratory, 2000.

[9] Fatma Outay, Veronique and Ridha Bouallegue, "Survey of Service Discovery Prtocols and Benefits of Comining Service and Route Discovery", International Journal of Computer Science and Network Security, VOL. 7 No 11, November, 2007.

[10] Choonhwa Lee and Sumi Helal, "Protocols For Service Discovery In Dynamic And Mobile Networks", International Journal of Computer Research, Volume 11, Number 1, pp. 1-12, © 2002 Nova Science Publishers,Inc.

[11] Survey of Service Discovery Protocols in Mobile Ad Hoc Networks by Adnan Noor Mian, Roberto Beraldi, Roberto Baldoni.

Data Transfer Security solution for Wireless Sensor Network

Bhavin Patel
Department of Computer Engineering
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.

Neha Pandya
Department of Information and Technology
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.

Abstract: WSN is a wide growth area for specific resource limited application. Factor associated with technology like, the encryption security, operating speed and power consumption for network. Here, we introduce a mechanism for secure transferring of data is WSN and various security related issues. This energy-efficient encryption is a secure communication framework in which an algorithm is used to encode the sensed data using like, RC5, AES and CAST Algorithm. The proposed scheme is most suitable for wireless sensor networks that incorporate data centric routing protocols. An algorithm in sensor network is help to designers predict security performance under a set of constraints for WSNs. This symmetric key function is used to guarantee secure communications between in-network nodes and reliable operation cost. RC5 is good on the code point of view, but the key schedule consumes more resource time for efficient security aspects.

Keywords: WSN, security mechanism, encryption, security issues, WSN algorithm.

1. INTRODUCTION

A wireless sensor networks (WSN) are one of the largest growing technology in area of data processing and communication networks today. Wireless sensor networks (WSNs) are based on physically small-sized sensor nodes exchanging mainly environment-related information with each other [2]. The wide application areas of WSN such as wildlife, real-time target tracking, transportation, entertainment, battlefield, building safety monitoring, Agriculture, etc. A WSN consists of a number of wirelessly interconnected sensor nodes that are used to gather information from the environment. In this paper Figure1 represent the model structure of wireless sensor network. The structure network consists of sensor devices which use a single integrated circuit which embeds all the electronic components required. The whole sensor is powered by a small battery which means the network's life is highly dependent on the energy consumption of the sensor. In addition to the sensors the network uses a base station which is the network's interface point to the rest of the world. However, energy consumption still remains one of the main obstacles to the diffusion of this technology, especially in application scenarios where a long network lifetime and a high quality of service are required [1].

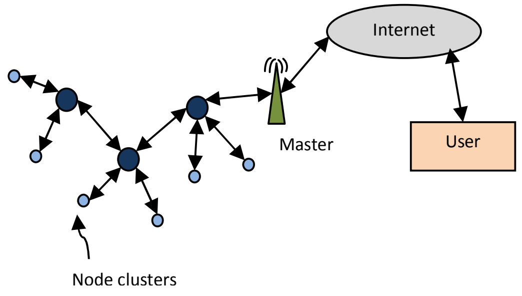


Figure 1. Model structure of WSN System

The major challenges to be addressed in WSNs are coverage and deployment, scalability, quality- of- service, size, computational power, energy efficiency and security [3]. Among these challenges, security is a major issue in wireless sensor networks. Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. Secure data transmission over unreliable medium is continuously gaining higher importance. WSN security includes Key management, providing secrecy and authentication; ensure privacy, robustness against communication denial of service attack, secure routing, energy efficiency, and resilience to node capture. It demands improvements in the performance of existing cryptographic algorithms.

Cryptographic algorithms are an essential part of the security architecture of WSNs, using the most efficient and sufficiently secure algorithm is thus an effective means of conserving resources. It is ideal to choose the most efficient cryptographic algorithm in all aspects; operation speed, storage and power consumption [1]. The cryptographic algorithms used in WSNs are generally categories into two parts: symmetric-key algorithms and Asymmetric-key algorithms. In asymmetric public key cryptosystems each node has a public key and a private key. The public key is published, while the private key is kept secret. Asymmetric public key cryptosystems such as the Diffie-Hellman key agreement or RSA signatures are typically too conservative in their security measures, adding too much complexity and protocol overhead to be usable in WSN solutions [2]. Symmetric key cryptographic mechanisms use a single shared key between the two communicating host which is used both for encryption and decryption. Symmetric key algorithms can be further divided into block ciphers for fixed transformations on plain-text data, and stream ciphers for time varying transformations. However, one major challenge for deployment of symmetric key cryptography is how to securely distribute the shared key between the two communicating hosts. Symmetric key cryptosystems such as the AES, DES, CAST, RC5 algorithm is used in WSN. It is give a comparison for those encryption algorithms at different settings such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. The popular encryption schemes RC5 can be considered as one of the best ciphers in terms of overall performance, when used in nodes with limited memory and processing capabilities.

The rest of the paper is organized as follows. Section 2 provides an overview of security issues & semantics in WSN. Section 3 presents different encryption algorithm schema for WSN. Section 4 provides security mechanism analysis. The paper then concludes in section 5, with insight to future work.

2. SECURITY ISSUES & SEMANTICS OF WSN

A sensor network is a special type of network. The whole network represented using layered architecture to represent its different level security aspect.

2.1 Security requirements

The basic functional security requirement for any WSN application listed as below:

Confidentiality: It refers to limiting information access and disclosure to authorized users. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality [1, 3].

Availability: It assures that the services of the system nodes are available to any authorized users as when they require. WSN should have mechanisms to tolerate the interference of malicious nodes. Techniques such as in-network processing, en-route filtering can be used to minimize the impact of unavailability [4].

Integrity: It guarantees that a message being transferred over network is delivered to its destination without any modification. In nature of WSN Integrity handle using MAC code data packet.

Authenticity: Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes. In WSN data authentication can be achieved through a symmetric mechanism.

Non-repudiation: It ensures that the information originator/ receiver cannot deny of performing its task. Non-repudiation is useful for detection and isolation of compromised nodes.

Robustness and Survivability: The purpose of robustness and survivability in WSN to reduce/recover effect of compromise the node performance. The attack on single node not leads to entire network breakdown.

Self Synchronization: Self- Synchronization is an important requirement for WSN because when point identification is necessary to prevent large scale attacks.

2.2 Attacks scenarios

Any Action that compromises the security of information is called Security Attack. It can be classified into two major categories, namely passive attacks and active attacks. Commonly security attacks are performing over the node of network. The most popular types of attacks are:

Denial of Service Attacks: An attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. A compromised node can send continuous messages to overflow the network and to deplete the life time of other sensor nodes. Another way is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life [5].

Injection attack: An intruder might add a node to the system that feeds false data or prevents the passage of true data [1]. The false message could lead to wrong decision for the whole network. Such messages also consume the scarce energy resources of the nodes.

Protocol- specific Attack: Routing protocol is also one of the vulnerable way in WSN to Spoofed routing information-corruption of the internal control information such as the routing tables, selective forwarding of the packets. Also perform action of forwarding packet to other network.

Wormholes Attack: The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. In this type of attack uses tunneling mechanism to establish malicious node between them by confusing the routing protocol. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages [1].

The Sybil Attack: In this attack the attacker gets illegally multiple identities on one node [7]. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage and multipath routing. Sybil attacks are generally prevented by validation techniques.

2.3 Constraints related to WSN

Some basic constraints are most commonly affected in the security mechanism for wireless sensor network:

Resource Consumption: WSN has storage, memory and Power limitations. In addition, when implementing a Cryptographic protocol within a sensor the energy impact of Security code must be considered. Energy consumption usually derives from two areas: computational costs and communication costs. Computational cost relates to the cost incurred by calculation of hash functions and primitives while communication cost derives from additional byte transfer among sensor nodes. Usually communication cost is much higher than computational cost.

Network Operability: Certainly, unreliable network is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. It can be classified in mainly three fields: Unreliable Transfer, Conflicts, and Latency**.** Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Wireless communication channel also results in damaged Packets. The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

Node reliability/ freshness: Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Its lead to exposure of physical attacks mainly of environment causes. Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues [4]. If designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

3. ENCRYPTION ALGORITHM SCHEMA FOR WSN

In this section, we provide an overview of three symmetric key cryptographic algorithms like. AES Algorithm, RC5 Algorithm and CAST Algorithm.

3.1 RC5 Algorithm

RC5 is suitable for resource-constrained sensor nodes for the following reasons [2]. RC5 is a fast symmetric block cipher with a two-word input block size plaintext and output block cipher text. The RC5 encryption algorithm is used in different modes like. Counter, feedback. RC5 is a block cipher with variable parameters: block size (32bits, 64 bits, and 128 bits), key size and encryption rounds, and it can be expressed as RC5-w/r/b [1]. The general operation performed by RC5 algorithm such as modular addition, XOR, and cyclic shift. The rotation operations depend on both the key and the data. The different combinations of values for these parameters are used to fully understand their influence on the energy consumption caused by the encryption algorithm. In normal way 18-20 round operation is enough to provide data encryption in WSN. RC5 uses an “expandable key table”, S, that is derived from the secret key K and the size t of Table S also depends on Nr, with S has t = 2(Nr + 1). RC5 does not rely on multiplication and does not require large tables. Hence, RC5 block cipher offers a computationally inexpensive way of providing secure encryption. The advantage of RC5 encryption schema in WSN is: high speed implementation, simplicity, arbitrary message length and a low rate of error propagation.

3.2 CAST Algorithm

The CAST encryption algorithm is one type of symmetric key base encryption schema for WSN. It was developed by Stafford Tavares and Carlisle Adams. Mainly two types of CAST schema consider like, CAST-128 and CAST-256. CAST-128 is a12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits [cast]. In this approach symmetric key always perform composition with substitution boxes (s) related to fewer bits. CAST-256 was derived from CAST-128. It is a 48-round Feistel network with a 128-bit block size and acceptable key sizes are 128, 160, 192, 224 or 256 bits [3]. The strength of the algorithm lies in its S-boxes. CAST does not have fixed S-boxes while new S-boxes are constructed for each application. Round function of the CAST algorithm performs faster. So it is more suitable for wireless network application which exchanges small size packets.

3.3 AES Algorithm

The Advanced Encryption Standard (AES) algorithm, also known as Rijndael, is a block cipher in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits with 4 x 4 array, while the key length can be 128, 192, or 256 bits and the number of rounds Nr is 10, 12 or 14 respectively[5]. The mail goal of this AES algorithm performed based on substitution- permutation of data block. In the encryption of the AES algorithm, each round except the final round consists of four iterative transformations: the Sub Bytes, the Shift Rows, the Mix-Columns, and the Add Round Keys, while the final round does not have the Mix Columns transformation. It is composed mainly of nonlinear components, linear components, and round keys, and though it employs an iterative structure, is does not have a Feistel network structure but an SP structure instead [1]. AES is fast in both software and hardware and is relatively easy to implement.

4. SECURITY MECHANISM ANALYSIS

Evolution of different symmetric key cryptographic algorithm based on following criteria:

4.1 Energy efficiency/consumption

Energy is the asset that has to be paid to obtain security. It is therefore generally accepted that a security mechanism will be less efficient and slower than a plain one. The energy consumed by a processor during the execution of a piece of software, such as a block cipher, corresponds to the product of the average power dissipation and the total running time. The power consumption of sensor network given each cryptographic algorithm AES, RC5 and CAST is executed on Mica2 mote of sensor node. The energy consumptions show that source node using RC5 saves about 72% of the energy Consumed by the hybrid scheme and 82% of the energy consumed ECC. Also for the CAST and AES algorithm the ratio of power consumption is about 67% and 78% respectively. The computational complexity of an algorithm translates directly to its energy consumption.

4.2 Operation time-speed

The data transfer time from sensor nodes to cluster head is computed below by including the data transmission time only for in case of the conventional data aggregation algorithm. Encryption speed is used to measure the throughput per unit time of an encryption scheme [3]. The encryption speed is calculated as the total plaintext in bytes divided by the encryption time and also calculates key setup time and decryption time for data value. For all three algorithms CAST, AES-128 and RC5 the encryption time is about 38%, 43%, and 40% of the decryption time. Encrypting data arrays handle operation speed of different size up to 8192 byte with RC5/AES.

4.3 Security strength

Security strength is referred differential cryptanalysis and linear cryptanalysis approach for the security mechanism implementation to handle bit wise operation of the key with data. The bits rotation for each random position in round of RC5 involves data dependent rotations which may help frustrate differential cryptanalysis and linear cryptanalysis since bits are rotated to random positions in each round [6].

The RC5 block cipher has built-in parameter variability that provides flexibility at all levels of security and efficiency. Also for the other symmetric key algorithm CAST and AES-128,256 the strength of security increase with no. of round is increased. The RC5 is better than DES in security strength and implementation efficiency.

4.4 Performance overhead

The measurement criteria for performance overhead consists of energy overhead, communication overhead, computational overhead and Memory space. Major performance overhead generates from the key setup operation, encryption operation and decryption. The initialization overheads are significant for all encryption algorithms like RC5, CAST and AES especially for small plaintexts. Thus they are suitable for large data size. RC5 requires that a pre-computed key schedule to be stored in memory taking up significant bytes memory for each key. RC5 is faster compared to AES-Rijndael and therefore more energy-efficient under memory constraints for both encryption and decryption, but it suffers from a relatively costly key expansion [6]. The group size, secret-key length, and the number of iterations of RC5, which can be used flexibly in systems with different resource configurations.

5. CONCLUSION & FUTURE WORK

In this paper we have describe the different security encryption mechanism for Wireless sensor network. Encryption algorithm plays a crucial role for information security due to various approach of resource constrains. Paper presented a systematic model of cryptographic algorithms complexity and in particular analyzed the suitability of RC5, CAST and AES encryption techniques to provide efficient link layer security. It provides one of the major security services namely confidentiality by the help of RC5 Encryption scheme which is based on the permutation codes on the blocks of data. One future research is to explore dynamic key assign cryptographic mechanisms to optimize energy consumption by varying cipher parameters using strong primitive arithmetic operation in WSN.

6. REFERENCES

[1] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef, “Performance Evaluation of Encryption Algorithm for Wireless Sensor Networks” International Conference on Information Technology and e-Services, 2012.

[2] Juha Kukkurainen, Mikael Soini, Lauri Sydanheimo, “RC5-Based Security in Wireless Sensor Networks: Utilization and Performance” WSEAS TRANSACTIONS on COMPUTERS, ISSN: 1109-2750, Issue 10, Volume 9, October 2010.

[3] Tingyuan Nie, Yansheng Li, Chuanwang Song, “Performance Evaluation of CAST and RC5 Encryption Algorithms” International Conference on Computing, Control and Industrial Engineering, year-2010.

[4] Abu Shohel Ahmed, “An Evaluation of Security Protocols on Wireless Sensor Network” TKK T-110.5190 Seminar on Internetworking, 2009.

[5] S.Prasanna, Srinivasa Rao, “An Overview of Wireless Sensor Networks Applications and Security” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[6] Dhanashri H. Gawali, Vijay M. Wadhai, “RC5 ALGORITHM: POTENTIAL CIPHER SOLUTION FOR SECURITY IN WBSN” International Journal of Advanced Smart Sensor Network Systems (IJASSN), Volume 2, No.3, July 2012.

[7] Abhishek Pandey, R.C. Tripathi, “A Survey on Wireless Sensor Networks Security” International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 67-71, 2013

Web Services Based Information Retrieval Agent System for Cloud Computing

Yu Mon Zaw
University of Technology,
Yatanarpon Cyber City,
Mandalay, Myanmar

Nay Min Tun
Computer University,
Kyaing Ton,
Shan State,Myanmar

Abstract: Cloud computing is Internet based system development in which large scalable computing resources are provided "as a service" over the Internet to users and has attracted more and more attention from industry and research community. However, the concept of cloud computing does not provide facilities for the knowledge discovery and information retrieval; i.e. clouds need to be intelligent and autonomous. On the other hand, Web Service plays important role in Service Oriented Computing (SOC) in cloud environment. Retrieving desired specific information from Web Services on cloud environment cannot be done by single Web Service. So, there should be a possibility to combine existing services together in order to fulfil the request. To compose Web Services, Agents can give great help. Therefore, this research mainly focus on providing a framework for retrieving information from Cloud using composite Web Services by means of Multi-Agent System.

Keywords: Cloud Computing; Multi-Agent; Web Services; Service Oriented Computing; Information Retrieval

1. INTRODUCTION

Cloud computing provide elastic services, high performance and scalable data storage to a large and everyday increasing number of users. Cloud computing enlarged the arena of distributed computing systems by providing advanced Internet services that complement and complete functionalities of distributed computing provided by the Web, Grid computing and peer-to-peer networks. In fact, Cloud computing systems provide large-scale infrastructures for high performance computing that are dynamically adapt to user and application needs. [1]

According to the current situation, most of ongoing works or researches are intended at developing the techniques and constructing cloud platforms, such as Amazon, Google AppEngine, Microsoft Azure, and manjrasoft Aneka. [2] We need more researches in information retrieval and knowledge discovery area. As Web Services play the major role in Cloud Environment since Cloud's main feature is also "as-a-service", to achieve the user desired information correctly and completely may depend on numerous Web Services' supports.

Web Services are considered as self-contained, self describing, modular applications that can be published, located, and invoked across the Web. Amount of products and services available now on the Web increases dramatically and goes beyond user's ability to analyze them efficiently. At the same time the number of potential customers available via the Internet also increases significantly and starts to be beyond service providers' ability to perform efficient targeted marketing. In particular, if no single Web service can satisfy the functionality required by a user, there should be a possibility to combine existing services together in order to fulfill the request. [3]

At the same time, multi-agent systems (MAS) represent another distributed computing paradigm based on multiple interacting agents that are capable of intelligent behavior. Multi-agent systems are often used to solve problems by using a decentralized approach where several agents contribute to the solution by cooperating one each other. One key feature of software agents is the intelligence that can be embodied into them according to some collective artificial intelligence approach that needs cooperation among several agents that can run on a parallel or distributed computer to achieve the needed high performance for solving large complex problems keeping execution time low. [1]

Therefore, for the Cloud-wide Information Retrieval system based on Web Services, it is sure that not a single Web Service can fulfill the user needs. To get the complete and desired information results, numerous related Web Services should be cooperated. In this case, we propose to get the help of multi- agents systems.

The remainder of this paper is organized as follows. In the next section, we will introduce the background knowledge and theory of Cloud Computing, Service Oriented Computing (SOC), Web Services and Agent Computing. Section 3 describes the related work. Section 4 discusses about our proposed framework. We introduce our system components, their functions and natures in Section 5. Section 6 presents proposed Algorithms for our Medical IR Multi-Agent System. The paper concludes in Section VII with titled Conclusion.

2. BACKGROUND

2.1 Cloud Computing

Cloud computing [9] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (by U.S. NIST (National Institute of Standards and Technology))

Five essential elements of cloud computing are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

Three main service model of cloud computing are:

- *Software as a Service (SaaS)*- Cloud consumers release their applications on a hosting environment, which can be accessed through networks from various clients (e.g. web browser, PDA, etc.) by application users. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth.
- *Platform as a Service (PaaS)*- PaaS is a development platform supporting the full software Lifecycle which allows cloud consumers to develop cloud services and applications(e.g. SaaS) directly on the PaaS cloud. Hence the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both completed and in-progress cloud applications. Eg. Google App Engine.
- *Infrastructure as a Service (IaaS)*-Cloud consumers directly use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers.

Four cloud deployment models have been defined in the Cloud community:

- *Private cloud*.-The cloud infrastructure is operated solely within a single organization, and managed by the organization or a third party regardless whether it is located premise or off premise. Academics often build private cloud for research and teaching purposes.
- *Community cloud*-Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community
- *Public cloud*- The public cloud is used by the general public cloud consumers and the cloud service provider has the full ownership of the public cloud with its own policy, value, and profit, costing, and charging model.
- *Hybrid cloud*.-The cloud infrastructure is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

2.2 Cloud and Service Oriented Computing (SOC)

The encapsulation, componentization, decentralization, and integration capability provided by SOC are substantial: they provide both architectural principles and software specifications to connect computers and devices using standardized protocols across the Internet. In fact, the notion of Cloud is more or less based on the evolving development on SOC, in particular the SaaS service model.

Advances in SOC can benefit Cloud Computing in several ways:

- *Service Description for Cloud Services*- Web Service Description Language (WSDL) and the REST protocol are two widely used interface languages to describe Web Services. They have been utilized to describe Cloud API specification.
- *Service Discovery for Cloud Services*- Various service discovery models can be leveraged for cloud resource discovery, selection and service-level agreement verification.
- *Service Composition for Cloud Services*- Since Web Services are born to compose business applications, a great deal of research in this area can be leveraged for cloud services integration, collaboration, composition.
- *Service Management for Cloud Service*- Research and practices in SOA governance and services management can be adapted and reused in the cloud infrastructure management.

2.3 Web Services

Web Service[4] is an accessible application that other applications and humans as well, can automatically discover and invoke. An application is a Web Service if it is

1) independent as much as possible from specific platforms and computing paradigms;
2) developed mainly for inter organizational situations rather than for intra-organizational situations; and
3) easily composable (i.e., its composition with other Web Services does not require the development of complex adapters).Web Services are, in practice, transient and stateless processes that exist only during service execution, which is triggered by a request coming from a consumer, or client. Services are instantiated to perform specific tasks, thus facilitating scalable, concurrent service provision. The design of a Web Service is usually defined as a clearly articulated workflow, for the sake of reliability and quality of service.

Though Web Services has many advantages, but still there are certain problems which need to be addressed. These are:

1) Provided resources and services are not in machine understandable form, these are in human understandable form.
2) The representation of resources and services on the web are unstructured and they are loosely related to each other.
3) Searching resources and services on the web at present is keyword based; no semantics of the resources are used. So by using some popular keywords, web page owner can make his page mostly retrieval with irrelevant results and
4) Interoperability between toolkits.

2.4 Agent Computing

An agent [1] is a computational entity that acts on behalf of another entity (or entities) to perform a task or achieve a given goal. Agent systems are self-contained software programs embodying domain knowledge and having ability to behave with a specific degree of independence to carry out actions needed to achieve specified goals. They are designed to operate in a dynamically changing environment**.**

Agents typically include a set of features. The main features of agents include the following:

- *Autonomy:* the capacity to act autonomously to some degree on behalf of users or other programs also by modifying the way in which they achieve their objectives.
- *Pro-activity:* the capacity to pursue their own individual set goals, including by making decisions as result of internal decisions.
- *Re-activity:* the capacity to react to external events and stimuli and consequently adapt their behavior and make decisions to carry out their tasks.
- C*ommunication and Cooperation*: the capacity to interact and communicate with other agents (in multiple agent systems), to exchange information, receive instructions and give responses and cooperate to fulfill their own goals.
- *Negotiation:* the capability to carry out organized conversations to achieve a degree of cooperation with other agents.
- *Learning:* the ability to improve performance and decision making over time when interacting with the external environment.

3. RELATED WORK

Yue-San Chang, Chao-Tung Yang and Yu-Cheng Luo presented an Ontology based Agent Generation for Information Retrieval on Cloud Environment. [2] While user submitting a flat-text based request for retrieving information on a based on predefined ontology and reasoning rule, and then be translated to a Mobile Information Retrieving Agent Description File (MIRADF) that is formatted in a proposed Mobile Agent Description Language (MADF). A generating agent, named MIRA-GA, is also implemented to generate a MIRA in accordance with MIRADF.

G.Vadivelou, E.Ilavarasan and M.S.Yasmeen presented an agent and ontology based approach that supports the semi-automatic composition of Web Services.[3] This paper provided the way to select an optimal composition of services and it also propose a framework for Semi-Automatic Web Services Composition.

Energy-Saving Information Multi-agent System with Web Services for Cloud Computing was given by Sheng-Yuan Yang, Dong-Liang Lee, Kune-Yao Chen and Chun-Liang Hsu from St. John's University in Taiwan. [5] It employs the concept of SQL IC to construct the operational interface of cloud database as a data warehouse. It presented the three-stage intelligent decision processing strategy with four agents: Interface agent, Data Mining agent, Reasoning agent and Web-Service-Based Information Agent System (WIAS).

Vishal Jain proposed the information retrieval practical model through the multi-agent system with data mining in a cloud computing environment. [6] He recommended that users should ensure that the request made to the IaaS is within the scope of integrated data warehouse and is clear and simple. In that research model/ architecture, the use of cloud computing allows the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage.

4. THE PROPOSED SYSTEM FRAMEWORK

We propose a framework for Web Services Based Information Retrieval Agent System for Cloud Computing Environment. The proposed system framework is intended to apply in Medical field. We have already assumed that a private Medical Cloud Environment was been founded. In that environment, a number of hospitals, clinics and health care services are hosted and are providing Web Services. Each Web Service of a specific hospital offers specialists (doctors) information worked at that hospital by numerous Web Methods. By using our Medical IR multi-agent System, users (patients) can easily search the desired information by day (Monday, Tuesday,...), by time (1pm-4pm,…), by doctor's name (Prof: Dr. Nay Win,…), by specific clinic (Asia Royal, SSC,..) and by disease type (Liver, Lung, OG,…).

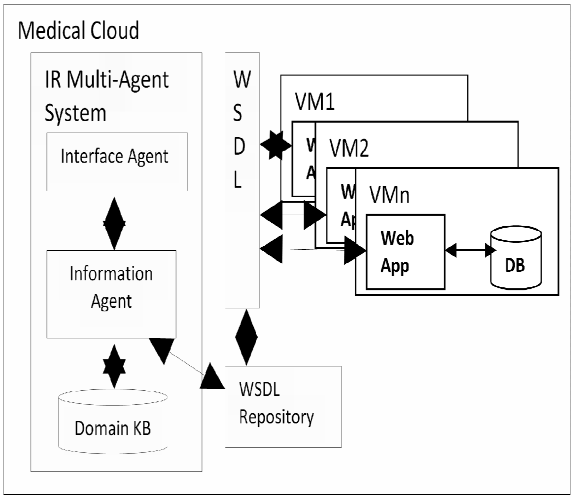


Figure 1. Medical IR Multi-Agent System Architecture

5. SYSTEM COMPONENTS AND THEIR FUNCTIONS

- The system will start from Interface Agent.
- Receiving queries from end users to search required information from Cloud databases and showing back the queries result may be done by interface agent in this proposed system.
- The duty of Interface Agent in this system is to receive queries from end users, prepare the queries into a format match for Information Agent's working style, pass the well formatted data to Information Agent and to show back the queries results.

- Information Agent will play as a major role and it uses specific Domain Knowledge Base for cloud-wide service composition and then decides which services can be a perfect match for the user queries.
- Domain Knowledge Base is a repository which stores system associated rules and conditions.
- WSDL Repository stores Web Service Description files published by various web applications hosted in the Cloud.
- Several web application systems from VMs (Virtual Machines) support services for Information Retrieval purpose**.**
- One VM represents one hospital.
- Each VM contains a web application (web site) for each hospital which desires to coordinate with our cloud-wide Medical IR Multi-agent System.

6. PROPOSED ALGORITHMS FOR MEDICAL IR MULTI-AGENT SYSTEM

- User Request is defined as Req.
- Refined Request is defined as RefineReq.
- The Returned Result from each Web Service is defined as ResWS.
- ResWS1, ResWS2,…, ResWSn □ ResWS
- Extracted Rules associated with user requests is defined as R.
- WS is the set of Web Services published in WSDL Repository.
- WS1, WS2,…, WSn □ WS
- Selection Web Services is defined as SelectedWS.
- AG is the set of all agents in the System.
- InterfaceAG, InfoAG □ AG
- Interface Agent is defined as InterfaceAG.
- Information Agent is defined as InfoAG.

```
Begin
FinResult←NULL.
User sends Req to InterfaceAG.
RefineReq←Req refined by InterfaceAG.
InterfaceAG sends RefineReq to InfoAG.
InfoAG extracts R appropriate with RefineReq.
InfoAG calls SelectWSAlgo(R).
WS←SelectedWS.
While not receiving the FinResult from InfoAG
InfoAG sends RefineReq to WS1, WS2, …, WSn
 □WS.
    For All WS1,WS2,…,WSi,…,WSn
        If WSi can solve RefineReq
            It will return ResWSi to
             InfoAG.
        Else
            Return NULL.
        End If
        FinResult←FinResult+ ResWSi.
    End For
End While
InfoAG sends back FinResult to InterfaceAG.
InterfaceAG shows the FinResult to User.
End
```

```
SelectWSAlgo(R)
Begin
SelectedWS←NULL
ForAll ItemR in R
    For All WS1,WS2,..,WSi,…,WSn in WS
        If WSi content matches ItemR
        SelectedWS←SelectedWS + WSi
        Else
        SelectedWS←SelectedWS + NULL
        End If
    End For
End For
Return SelectedWS.
End
```

7. CONCLUSION

A Web Services Based Information Retrieval Agent System for Cloud Computing is proposed. Efficiently composed cloud Web Services using multi-agents features can give new form for cloud wide information retrieval systems. The proposed system will become an intelligent way for searching or retrieving information from Cloud environment. By implementing the propose system, it can give a good hand for the public to get the desired specialists' schedule completely and perfectly at one sitting and can make the right choice with their current situations. Moreover, this framework can be applied in other domain area efficiently.

8. REFERENCES

[1] Talia, D. 2012. Cloud Computing and Software Agents : Towards Cloud Intelligent Services.

[2] Chang, Y. S., Yang, C. T., and Luo, Y. C. 2011. An ontology based agent generation for information retrieval on cloud environment, Journal of Universal Computer Science, vol. 17, no. 8, 2011.

[3] Vadivelou, G., Ilavarasan, E., and Yasmeen, M. S. 2011, QoS based semi-automatic web service composition using multi-agents systems, IJCSET, Vol 1, Issue 7, pp. 381-386, August 2011.

[4] Curbera, F., Khalaf, R., Mukhi, N., Tai, S., and Weerawarana, S. 2003, The Next Step in Web Services, Comm. ACM, vol. 46, no. 10, October 2003.

[5] Yang, S. Y., Lee, D. L., Chen, K. Y., and Hsu, C. L 2011., Energy-saving information multi-agent system with web services for cloud computing, SUComS 2011 , CCIS 223, pp. 222–233.

[6] Jain, V. 2012, Information retrieval through multi-agent system with data mining in cloud computing, J.Comp.Tech.Appl, Vol 3 (1), pp. 62-66, IJCTA.

[7] Wang, S., Zheng, Z., Sun, Q., Zou, H., and Yang, F. 2011, Cloud model for service selection, IEEE INFOCOM Workshop on Cloud Computing.

[8] Pejman, E., Rastegari, Y., .Majlesi Esfahani , P., and Salajegheh, A. 2012, Web Service Composition Methods: A Survey, IMECS 2012 Vol I.

[9] Dillon, T., Wu, C., and Chang, E. 2010, Cloud Computing Issues and Challenges, 24th IEEE International Conference on Advanced Information Networking and Applications.

Cross-domain Recommendations for Personalized Semantic Services

Hla Hla Moe
University of Technology
Yatanarpon Cyber City,
Pwin Oo Lwin, Myanmar

Win Thanda Aung
University of Computer Studies
Bahan Campus,
Yangon, Myanmar

Abstract: An increasing amount of work has been published in various areas related to the Recommender System. Among them, cross-domain recommendation is an emerging research topic and in this field, it is important to investigate how to manage personalization and how to consider customer's contextual features to keep more user satisfaction and accuracy. This paper tends to provide cross-domain recommendations for personalized semantic services using Taxonomic CCBR, directed acyclic graph by Ford-Fulkerson algorithm and TOPSIS method. Taxonomic CCBR helps the system get the accurate problem by engaging a user in a series of questions and answers from the user's partial definition of the problem. Semantic concepts between different domains are considered by using weighted directed acyclic graph to find meaningful solutions. Then TOPSIS method is used to get the results more precisely considering contextual features such as season, place, etc. which have not been addressed in the current cross-domain recommender systems.

Keywords: recommender systems; cross-domain recommendations; personalization; semantic concepts; customer's contextual features

1. INTRODUCTION

Through the Internet, different products, services and customers can now easily interact with each other because the advance of Internet and Web technologies has continuously boosted the prosperity of e-commerce [4]-[7]. On the other hand, the more continuous development of electronic commerce, the more difficult it is for customers to single out products or services and find the most suitable ones with them. To make a suitable decision, customers still spend much time in visiting a flood of online retailers, and gather valuable information by themselves. This process is very time-consuming and sometimes the contents of Web documents that customers browse have nothing to do with those that they need indeed.

To overcome the above problem, recommender system is a main solution. Recommender systems typically provide the user with a list of recommended items they might prefer, or supply guesses of how much the user might prefer each item [2]-[4]. Such systems are now popular both commercially and in the research community and even overwhelm human processing capabilities in a wide array of information seeking for decision making. So many Web sites such as Amazon, Netflix, Last.fm and many online retailers have proved that recommendation models are successful [2]-[7]. However, ample room and need for further improvements remain in the effective human decision support in a wide variety of applications.

The vast majority of these systems offer their recommendations only for items belonging to a single domain. In fact, joint recommendations in multiple domains are sometime needed for a customer. For instance, a system suggests not only a particular movie but also music CDs and books that are somehow related to that movie [2]-[7]-[5]-[12]. Such types are cross-domain recommendations. By definition, cross-domain recommendation is providing recommendations of items in one (source) domain using the preferences expressed on items in a second (target) domain [7]-[5]. Another task for cross-domain recommendation is making joint recommendations for items belonging to different domains [13].

According to [2], cross-domain recommendation models are classified into adaptive models – which exploit information directly from a source domain to make recommendations in a target domain – and collective models – which are built with data from several domains and potentially can make joint recommendations for such domains. Generally, almost all cross-domain recommendations are less accurate than single-domain recommendations but they can give more diverse recommendations leading to a higher user satisfaction and engagement addressing cold-start and sparsity problems [5]-[7]-[11]-[13]-[15].

In this paper, a framework for cross-domain recommender system is proposed. Previous cross-domain recommender systems are constructed based on music, music artists and related things [5]-[7]-[11]-[17]. The framework is used to apply the useful application area where skin care problem is solved and suitable cosmetics are recommended. The framework tends to solve customer's personalized problem and give more accurate recommendations in a particular way. To handle personalization systematically, Taxonomic CCBR is used. It allows for a partial definition of the problem by the user, identifies more clearly user's problem and gives accurate solution by conversation. Hence, it improves personalization. To extract the semantic concepts between domains, the Ford and Fulkerson algorithm is applied by directed acyclic graph. Consideration of customer's contextual features such as season, place and so on is an important role for managing personalization. And hence, to get personalized recommendations precisely and accurately. TOPSIS method is used to calculate the final results considering contextual features.

The rest of the paper is organized as follows. Section 2 describes our motivation. In section 3, related works on cross-domain recommender systems are briefly described. In section 4, system overview of the proposed system is described. Section 5 also describes detailed approach for cross-domain recommendations for personalized semantic services and section 6 describes the conclusion.

2. MOTIVATION

In the most current recommender systems, recommendations are only from a single domain. Therefore, today, cross-domain recommender systems become an interesting topic. This type of recommendations has barely been investigated because it is difficult to obtain public datasets with user preferences crossing different domains. The previous related works for cross-domain recommendations still have some weaknesses. Some are lack of personalization. Some are lack of semantic concepts and less accuracy. Our framework tends to solve these weaknesses. And then the objectives of our framework are to understand about the advantages of cross-domain recommender systems adding semantic concepts, to get more accurate, precise and personalized recommendations and to know the interesting results of cross-domain recommendations applying TOPSIS method with customer's contextual features.

3. RELATED WORK

The application of cross-domain recommendation approaches becomes of special interest in many e-commerce and retailer websites because it can increase company profits and strengthen customers' loyalty. Therefore, cross-domain recommendation is an interesting research area and applies in many application areas, and even mobile environments. In the previous works, cross-domain recommender systems have been proposed in various kinds of ways.

Gustavo González et al. described an approach for cross-domain recommender systems using Smart User Model (SUM). It was a multi-agent based system. It used incremental aggregation of information, which favored non-intrusive behavior of the user model in order to determine objective, subjective and emotional user features [12].

A generic framework to mediate the integration of data collected by several recommender systems was presented by Shlomo Berkovsky et al. They discussed four major types of mediation: cross-user, cross-item, cross-context, and cross representation. Some evaluations had shown that in certain conditions, user modeling data mediation improved the quality of recommendations, especially in the cold start of a recommender system [10].

References [17] and [5] showed that Marius Kaminskas and Francesco Ricci proposed an approach which considered contextual conditions such as the user mood or location. It retrieved music that suited the user's interested place using emotional tags attached by users' population to both music and POIs. It applied a set of similarity metrics for tagged resources to establish a match between music track and POIs.

Francesco Ricci et al. designed and developed a generic framework built upon semantic networks, which integrated and exploited knowledge on several domains to provide cross-domain adapted item recommendations. They proposed an approach that automatically extracted information about two domains available in Linked Data repositories, linked items in the two domains by means of a weighted directed acyclic graph, and performed weight spreading mechanisms on such graph to identify matching items in a target domain (music artists) from items of a source domain (places of interest) [7].

Fabian Abel et al. studied distributed form-based and tag-based user profiles, based on a large dataset aggregated from the Social Web. The performance of several cross-system user modeling strategies in the context of recommender systems is developed and evaluated to solve the cold-start problem and improve recommendation quality [13].

Jie Tang et al. proposed Cross-domain Topic Learning (CTL) approach to address three challenges: sparse connections - cross-domain collaborations were rare, complementary expertise - cross-domain collaborators often have different expertise and interest and topic skewness - cross-domain collaboration topics are focused on a subset of topics. For handling sparse connections, CTL consolidates the existing cross-domain collaborations through topic layers instead of at author layers, which alleviated the sparseness issue. For handling complementary expertise, CTL models topic distributions from source and target domains separately, as well as the correlation across domains. For handling topic skewness, CTL models only relevant topics to the cross-domain collaboration [15].

4. SYSTEM OVERVIEW OF CROSS-DOMAIN RECOMMENDATIONS FOR PERSONALIZED SEMANTIC SERVICES

To provide cross-domain recommendations for personalized semantic services, recommendation algorithm works as follows:

1. User gives the initial dialog from the system interface.
2. Taxonomic CCBR system defines the definite problem.
3. According to the problem, the concepts from the source and target domains are linked by means of weighted directed acyclic graph for semantic filtering.
4. From the results, the vectors of product and customer's contextual features are constructed and the utility value of the each product is calculated using TOPSIS method.
5. Recommendations are given to the user.

System overview of cross-domain recommendations for personalized semantic services can be seen as the following figure.

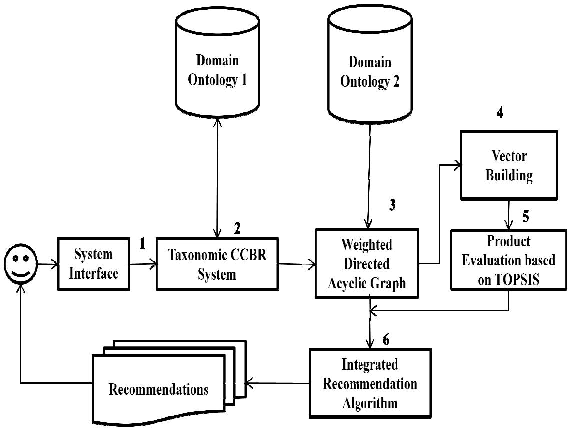


Figure. 1 System overview of cross-domain recommendations for personalized semantic services

4.1 Algorithm of cross-domain recommendations for personalized semantic services

Algorithm: Product Recommendation ( )

```
Input:          user query, customer's contextual features
                and weights of      commodities
Output:         products list
```

```
Init (Q); Load (Q); // initiate and load user query
Begin
        DefineProblem (Q, c); /*define definite problem
        with Taxonomic CCBR system*/
        for each P_i do
        {
            FindSemanticRelation (c, P_i); /* find semantic
            relation between from problem domain and
            each product from product domain*/
            ComputeWeight (P_i); /* compute weight of
            each product using Ford-Fulkerson algorithm*/
            InsertTo(ProductList); /* insert P_i into Product
            list in descending order*/
        }
        while (ProductList != Null)
        {
            GetProductUtility(P_i); /* compute the utility
            value of each product from the product list
            with customer's contextual features*/
            InsertTo(ProductList); /* insert P_i into Product
            list in descending order*/
        }
        Output (ProductList, top-k); /* output top-k
        products as the recommended product to target
        customer*/
End
```

5. CROSS-DOMAIN RECOMMENDATIONS FOR PERSONALIZED SEMANTIC SERVICES

To obtain cross-domain recommendations for personalized semantic services, the framework is considered as three stages and worked as follows.

5.1 Acquiring Definite Problem from User Query

In this stage, Taxonomic conversational case-based reasoning (Taxonomic CCBR) is applied. the user is not expected to know exactly which type of problem she has but she is required to answer a set of questions such that the system identifies more clearly what her problem is [3]-[6]. Given information related to the domain, the retrieval process is initiated whereby all questions in taxonomy relevant to that particular domain are presented to the user. Given the set of questions to choose from, the user can then decide to answer some of these questions. Depending on the answers provided, the system will try to find cases in which questions were answered in a similar manner. A similarity measure is used to rank cases. The questions which are present in the retrieved cases but which are still unanswered, yet are related to the problem, are then presented in a rank order to the user. The process continues until the system gets a case which includes a definite problem, personalizing the solution to her needs.

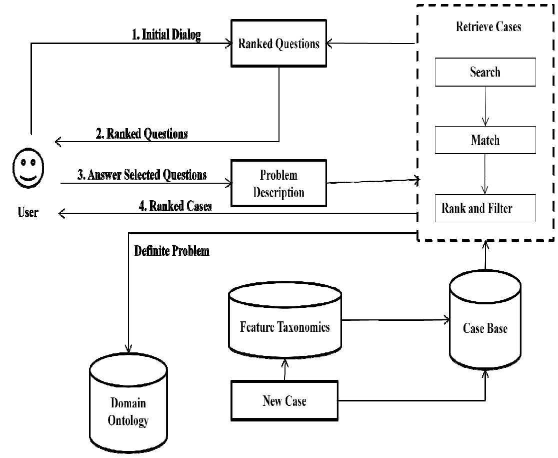


Figure. 2 User interactions with a Taxonomic CCBR system

For case retrieval, Taxonomic theory is divided into two steps taking into account that each question-answer (QA) pair is a set of triples or rather an acyclic directed graph:

(i) similarity between QA pairs

$$sim(C_{q1},C_{q2})=\begin{cases}1 & if C_{q1}\subseteq C_{q2}\\ (n+1-m)/(n+1+m) & if C_{q2}\subseteq C_{q1}\\ 0 & otherwise\end{cases} \quad (1)$$

where,

C_{q1} and C_{q2} are concepts
n = number of edges between C_{q1} and the root
m = number of edges between C_{q1} and C_{q2}

(ii) an aggregate similarity between the user query Q and a case problem description P to retrieve the most suitable cases

$$sim(Q,P)=\frac{\sum_{i\in Q,\, j\in P} sim(C_{qi},C_{qj})}{T} \quad (2)$$

where, T represents the number of taxonomies.

5.2 Finding Cross-domain Recommendations

In the second stage, the system finds the semantic relation between source and target domains according to the definite problem from the previous stage in with weighted directed acyclic graph.

Firstly, semantic relationships between domains are considered based on ontology knowledge representation which can be defined as a network (DAG) of semantic entities (concepts) of different domains interlinked by semantic relations (properties). Entities can be categorized as classes (e.g. cosmetic) and instances (e.g. Revlon Toner). Semantic relations are taken into account using the generic ontology rules such as generalization/specification ("is a" relation), aggregation/decomposition ("has a" relation), similarity (e.g. acne, pimple) and relatedness (e.g. "hydroxyl acid" makes acne "clear"). The relationships can link classes (e.g. "cosmetic" consists of "ingredients"), instances (e.g. "tea tree oil" contains "vitamin A") and both types (e.g. "Revlon Toner" is a "cosmetic").

In calculation, the weight of relations between instances is identified. [16]-[18] According to Kirchkoff's Law, "everything that leaves the source must eventually get to the sink", how much flowing into the weight of each target node with Ford-Fulkerson algorithm. It is simple and gives accurate weight of each target node. The weight of target node is calculated by

$$W(v_i) = \sum_{k=1}^{n} f_{k,i}, i > 1 \qquad (3)$$

where, n is the number of vertices and f is the weight of the flow.

The more the weight is, the better the performance of semantic relation between different domains.

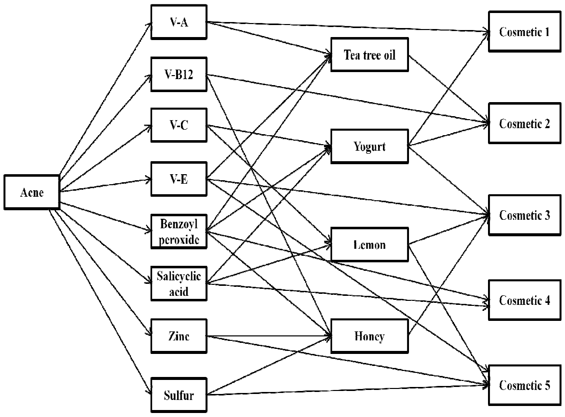


Figure.3 Example of finding semantic relationship between source and target domains by DAG

5.3 Considering Contextual Features

Finally, the system calculates the utility value of each candidate product for customer utilizing TOPSIS method, considering customer's contextual features. TOPSIS method is a multi-attribute decision making approach and stands for technique for ordering preference by similarity to ideal solution [1]-[4]-[8]. It is based on the principle that the solution should have the shortest distance to the best solution and the farthest distance to the worst one. As the mathematical model, $P = \{p_1, p_2, \ldots, p_m\}$ is defined as the vector of the product information and $F = \{f_1, f_2, \ldots, f_3\}$ is defined as the vector of the customer's contextual features. To represent the relevance performance of the product p_i in the qualitative feature i, decision matrix can be constructed as the following:

$$D = \begin{bmatrix} d_{11} & d_{12} & \ldots & d_{1n} \\ d_{21} & d_{22} & \ldots & d_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ d_{m1} & d_{m2} & \ldots & d_{mn} \end{bmatrix} \qquad (4)$$

The decision matrix should be normalized following the formula:

$$b_{ij} = d_{ij} \Big/ \sqrt{\sum_{j=1}^{n} d_{ij}^2}, i = 1,2,\ldots, m, j = 1,2,\ldots, n \qquad (5)$$

The normalized value b_{ij} is limited in [0, 1]. The utility value of the product p_i can then be calculated using the formula:

$$R_i = t_i^- / (t_i^- + t_i^+), i = 1,2,\ldots, m \qquad (6)$$

where,

$$t_i^+ = \sqrt{\sum_{j=1}^{n} (c_{ij} - c_j^+)^2}, i = 1,2,\ldots, m \qquad (7)$$

$$t_i^- = \sqrt{\sum_{j=1}^{n} (c_{ij} - c_j^-)^2}, i = 1,2,\ldots, m \qquad (8)$$

In the above equations, n is the number of customer's contextual features, c_{ij} is the weighted normalized decision matrix which is calculated by

$$c_{ij} = w_j b_{ij}, i = 1,2,\ldots, m, j = 1,2,\ldots, n \qquad (9)$$

where, w_j means the customer's relative need in this feature and c_j^+ , c_j^- are the positive and negative ideal solutions:

$$C^+ = \{c_1^+, c_2^+, \ldots, c_n^+\} = \left\{\left(\max_i c_{ij} \mid j \in I\right), \left(\min_i c_{ij} \mid j \in J\right)\right\} \qquad (10)$$

$$C^- = \{c_1^-, c_2^-, \ldots, c_n^-\} = \left\{\left(\min_i c_{ij} \mid j \in I\right), \left(\max_i c_{ij} \mid j \in J\right)\right\} \qquad (11)$$

The more increase the relative closeness R_i, the more important the utility value of the product p_i.

Finally, by performing the three stages systematically, the algorithm recommends a ranked list with the highest weighted target instances and the customer can obtain the most suitable products and services that matches her personal problem with full of satisfaction.

6. CONCLUSION

The paper presents an approach of cross-domain recommendations for personalized semantic service based on Taxonomic CCBR, Ford-Fulkerson algorithm and TOPSIS method. The system tends to build the framework for recommending cosmetics (target domain) related to customer's skin care problems (source domain) because skin care is the most interesting area for people today. The system is user-friendly and more accurate than the other related works. It gives more personalized semantic recommendations and makes more profits for commercial sites. Therefore, the system becomes an interesting and successful recommender system taking the advantages of ground-truth theory and application area.

7. ACKNOWLEDGMENTS

My Sincere thanks to my supervisor Dr. Win Thanda Aung, Lecturer, University of Computer Studies (Bahan Campus), Myanmar for providing me an opportunity to do my research work. I express my thanks to my Institution namely University of Technology (Yatanarpon Cyber City) for providing me with a good environment and facilities like internet books, computers and all that as my source to complete this research. My heart-felt thanks to my family, friends and colleagues who have helped me.

8. REFERENCES

[1] Wei J., "TOPSIS Method for Multiple Attribute Decision Making with Incomplete Weight Information in Linguistic," Journal of Convergence Information Technology, Volume 5, Number 10, December 2010, doi: 10.4156/jcit.vol5. issue 10.23

[2] Fernández-Tobías I., Cantador I., Kaminskas M. and Ricci F., "Cross-domain recommendr sysems: A servey of the State of the Art", Escuela Politécnica Superior, Universidad Autónoma de Madrid, 28049 Madrid, Spain

and Faculty of Computer Science,Free University of Bozen-Bolzano, 39100 Bolzano, Italy, 2012

[3] Abela C. and Montebello M., “PreDiCtS: A Personalised Service Discovery and Composition Framework”, Department of Computer Science and AI, University of Malta, 2006

[4] Zeng Z., “A Personalized Product Recommender System based on Semantic Similarity and TOPSIS Method”, Journal of Convergence Information Technology, Volume 6, Number 7, July 2011, doi: 10.4156/jcit.vol6.issue7.39

[5] Kaminskas M. and Ricci F., “ Location Adapted Music Recommendation Using Tags”, Free University of Bolzano, Piazza Domenicani 3, 39100 Bolzano, Italy, 2011

[6] Moy Gupta K., “Taxonomic Conversational Case-Based Reasoning”, Proc. ICCBR 2001, LNAI 2080. Pp.219-133, 2001

[7] Fernández-Tobías I., Cantador I., Kaminskas M. and Ricci F., “A Generic Semantic-based Framework for Cross-domain Recommendation”, Escuela Politécnica Superior, Universidad Autónoma de Madrid, 28049 Madrid, Spain and Faculty of Computer Science,Free University of Bozen-Bolzano, 39100 Bolzano, Italy, 2011

[8] Jadidi O., Firouzi F. andBagliery E., “TOPSIS Method for Supplier Selection Problem”, World Academy of Science, Engineering and Technology 71, 2010

[9] Asanov D., “Algorithms and Methods in Recommender Systems”, Berlin Institute of Technology, Berlin, Germany, 2011

[10] Berkovsky S., Kuflik T. and Ricci F., “Mediation of User Models for Enhanced Personalization in Recommender Systems”, University of Haifa, Haifa, Israel, Free University of Bozen-Bolzano, Italy, 2008

[11] Azak M., “Crossing: A Framework To Develop Knowledge-based Recommenders In Cross Domains”, MSc thesis, Middle East Technical University, 2010

[12] González G., López B. and Lluís de la Rosa J., “A Multi-agent Smart User Model for Cross-domain Recommender Systems,”, Poc. Of IUI 2005 Beyond Personalization Workshop, pp.93-94, 2005

[13] Abel F. , Herder E., Houben G., Henze N. and Krause D., “Cross-system User Modeling and Personalization on the Social Web”, Web Information Systems, TU Delft, The Netherlands and IVS Semantic Web Group & L3S Research Center, Leibniz University Hannover, Germany, 2011

[14] Berkovsky S., Kuflik T. and Ricci F., “Mediation of User Models for Enhanced Personalization in Recommender Systems”, University of Haifa, Haifa, Israel and Free University of Bozen-Bolzano, Italy, 2008

[15] Tang J., Wu S., Sun J., and Su H., “Cross-domain Collaboration Recommendation”, Department of Computer Science and Technology, Tsinghua University, IBM TJ Watson Research Center, USA, August, 2012

[16] Vatter V., “Graphs, Flows and the Ford-Fulkerson Algorithm”, August 12, 2004

[17] Kaminskas M. and Ricci F., “Location Adapted Music Recommendation Using Tags”, Free University of Bolzano, Piazza Domenicani 3, 39100 Bolzano, Italy, 2009

[18] http://en.wikipedia.org/wiki/Ford-Fulkerson_algorithm

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 77-80, 2013

Semantic Information Retrieval based on Wikipedia Taxonomy

May Sabai Han
University of Technology
Yatanarpon Cyber City
Myanmar

Abstract: Information retrieval is used to find a subset of relevant documents against a set of documents. Determining semantic similarity between two terms is a crucial problem in Web Mining for such applications as information retrieval systems and recommender systems. Semantic similarity refers to the sameness of two terms based on sameness of their meaning or their semantic contents. Recently many techniques have introduced measuring semantic similarity using Wikipedia, a free online encyclopedia. In this paper, a new technique of measuring semantic similarity is proposed. The proposed method uses Wikipedia as an ontology and spreading activation strategy to compute semantic similarity. The utility of the proposed system is evaluated by using the taxonomy of Wikipedia categories.

Keywords: information retrieval; semantic similarity; spreading activation strategy; wikipedia taxonomy; wikipedia categories

1. INTRODUCTION

Information in WWW are scattered and diverse in nature. So, users frequently fail to describe the information desired. Traditional search techniques are constrained by keyword based matching techniques. Hence low precision and recall is obtained [2]. Many natural language processing applications must estimate the semantic similarity of pairs of text fragments provided as input, e.g. information retrieval, summarization, or textual entailment. A simple lexical overlap measure cannot be successful when text similarity is not based on identical words and in general when words are not independent [3].

It has long been recognized that in order to process natural language, computers require access to vast amount of common-sense and domain-specific world knowledge. However, prior work on semantic relatedness was based on purely statistical techniques that did not make use of background knowledge or on lexical resources that incorporate very limited knowledge about the world [1].

Many natural language processing tasks require external sources of lexical semantic knowledge such as Wordnet. Traditionally, these resources have been built manually by experts in a time consuming and expensive manner [4].

An advantage of using the “ontology” approach, whether based on a designed or emergent ontology, is that the terms can be explicitly linked or mapped to semantic concepts in other ontologies, and are thus available for reasoning in more sophisticated language understanding systems. Using the traditional approach of a controlled, designed ontology has many disadvantages beginning with the often difficult task of designing and implementing the ontology. Once that it done, it must be maintained and modified, an important process in domains where the underlying concepts are evolving rapidly [5].

Wikipedia has recently provided a wide range of knowledge including some special proper nouns in different areas of expertise (e.g., Obama) which is not described in WordNet. It also includes a large volume of articles about almost every entity in the world. Wikipedia provides a semantic network for computing semantic relatedness in a more structured fashion than a search engine and with more coverage than WordNet. And Wikipedia articles have been categorized by providing a taxonomy, categories. This feature provides the hierarchical structure or network. Wikipedia also provides articles link graph. So many researches has recently used Wikipedia as an ontology to measure semantic similarity.

We propose a method to use structured knowledge extracted from the English version of Wikipedia to compute semantic similarity. This model takes the system of categories in Wikipedia as a semantic network by considering that every article in Wikipedia as a concept. Our system uses spreading activation strategy on the network of Wikipedia categories to evaluate semantic similarity.

The rest of the paper is organized as follows. Section 2 expresses about information retrieval based on semantic similarity. Section 3 describes motivation for the proposed system. Section 4 discusses related semantic similarity computing techniques based on Wikipedia. Section 5 provides framework of our proposed system. Section 6 mentions about semantic similarity computing using spreading activation strategy, and section 7 concludes.

1.1 Spreading Activation Strategy

Spreading Activation Strategy is a technique that has been widely adopted for associative retrieval. In associative retrieval, the idea is that it is possible to retrieve relevant documents if they are associated with other documents that have been considered relevant by the user. Also it has proved a significant result in word sense disambiguation. In Wikipedia the links between categories show association between concepts of articles and hence can be used as such for finding related concepts to a given concept. The algorithm starts with a set of activated nodes and, in each iteration, the activation of nodes is spread to associated nodes. The spread of activation may be directed by addition of different constraints like distance constraints, fan out constraints, path constraint, threshold. These parameters are mostly domain specific [5].

2. INFORMATION RETRIEVAL BASED ON SEMANTIC SIMILARITY

Information retrieval (IR) is the task of representing, storing, organizing, and offering access to information items. IR is different from data retrieval, which is about finding precise data in databases with a given structure. In IR systems, the information is not structured; it is contained in free form in text (webpages or other documents) or in multimedia content. The first IR systems implemented in 1970's were designed to work with small collections of text (for example legal documents). Some of these techniques are now used in search engines. The aim is to retrieve all the relevant information according to the given query.

There is a huge quantity of text, audio, video, and other documents relating to the various subjects available on the Internet. With the explosive growth of information, it is becoming increasingly difficult to retrieve the relevant documents. This begins challenges to IR community and motivate researcher to look for information retrieval system which can retrieve information based on some higher level of understanding of query. This higher level of understanding can only be achieved through processing of text based on semantics, which is not possible by considering a document as a "bag of words". So, nowadays, several semantic similarity techniques have been used in information retrieval systems.

The semantic similarity computing techniques define how to compare query requests to the collection of documents to obtain the semantically related documents based on the concept of using ontology. Semantic similarity computing methods have to calculate the relatedness of two concepts though they don't have the exact match. Therefore, the percentage of relevant information we get mainly depends on the semantic similarity matching function we used. For the above fact, more and more semantic similarity methods are discovered to produce the most semantically related results.

3. MOTIVATION

Vector space model represents a document or a query as a vector. Although the term vector similarity computing is applied in a number of such applications for its simplicity and reasonable accuracy, it has a problem of lack of semantic. This is due to the representation of document in a linear form (i.e., a vector of features) in which semantic relations among features are ignored. An example for such problem is found in recommender systems which find people with similar preference according to their old transactions. Therefore several approaches have developed to enhance semantic similarity distance. Some approaches use the ontology to construct the taxonomy of concepts and relations for the fragments to be compared. Building and maintaining those knowledge bases require a lot of effort from expert. Moreover, only the domain specific terms or a small fraction of the vocabulary of a language are covered by the bases. Wikipedia provides a knowledge base for computing word relatedness in a more structured fashion than a search engine and with more coverage than WordNet. So, the idea of using Wikipedia is intended for computing semantic similarity in the proposed system.

4. RELATED WORK

The depth and coverage of Wikipedia has received a lot of attention from researchers who have used it as a knowledge source for computing semantic relatedness.

Explicit Semantic Analysis (ESA) [1] represents the meaning of texts in a high-dimensional space of concepts derived from Wikipedia. ESA uses machine learning techniques to explicitly represent the meaning of any text as a weighted vector of Wikipedia-based concepts. Assessing the relatedness of texts in this space amounts to comparing the corresponding vectors using conventional metrics (e.g., cosine). However, ESA does not use link structure and other structures knowledge from Wikipedia, although these contain valuable information about relatedness between articles.

Milne and Witten [9] measure semantic relatedness by using hyperlink structure of Wikipedia. Each article is represented by a list of its incoming and outgoing links. To compute relatedness, they use tf-idf using link counts weighted by the probability of each link occurring.

In WikiRelate [11], the two articles corresponding to two terms are retrieved firstly. Then the categories related to these articles are extracted and map onto the category network. Given the set of paths found between the category pairs, Strube and Ponzetto compute the relatedness by selecting the shortest path and the path which maximizes information content for information content based measures.

WikiWalk[10] evaluates methods for building the graph, including link selection strategies and performing random walks based on Personalized PageRank to obtain stationary distributions that characterize each text. Senamtic relatedness is computed by comparing the distributions.

Majid Yazdani et al. [3] build a network of concepts from Wikipedia documents using a random walk approach to compute distances between documents. Three algorithms for distance computation such as hitting/commute time, personalized page rank, and truncated visiting probability are proposed. Four types of weighted links in the document network such as actual hyperlinks, lexical similarity, common category membership and common template use are considered. The resulting network is used to solve three benchmark semantic tasks- word similarity, paraphrase detection between sentences, and document similarity by mapping pairs of data to the network, and then computing a distance between these representations.

Behanam et al. [8] extracted the multi-tree for each entity from Wikipedia categories network. Then combined two multi-trees and used multi-tree similarity algorithm to this combined tree to compute similarity.

Lu Zhiqiang et al. [6] used snippets from Wikipedia to calculate the semantic similarity between words by using cosine similarity and TF-IDF. That is different from other methods which used Wikipedia taxonomy. The stemmer algorithm and stop words are also applied in the preprocessing the snippets from Wikipedia.

In [5], Wikipedia articles, and the category and article link graphs are used to predict concepts common to a set of documents. Zareen Saba Syed et al. describe several algorithms to aggregate and refine results, including the use of spreading activation to select the most appropriate terms.

Stephan Gouws et al. [12] propose the Target Activation Approach(TAA) and the Agglomerative Approach (AA) for computing semantic relatedness by spreading activation energy over the hyperlink structure of Wikipedia. Relatedness between two nodes can be measured as either 1) the ratio of initial energy that reaches the target node, or 2) the amount of overlap between their individual activation vectors by spreading from both nodes individually. The second method is adaptation of the Wikipedia Link-based Measure (WLM) approach to spreading activation.

5. PROPOSED SEMANTIC INFORMAITON RETRIEVAL

The figure illustrates the overview of the system.

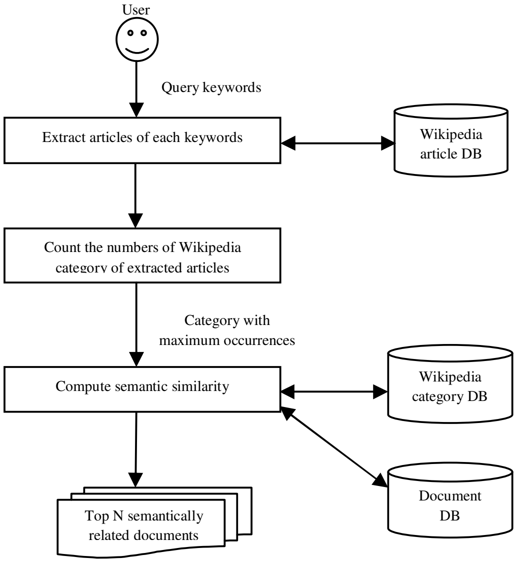

User
Query keywords
Extract articles of each keywords
Wikipedia article DB
Count the numbers of Wikipedia category of extracted articles
Category with maximum occurrences
Compute semantic similarity
Wikipedia category DB
Document DB
Top N semantically related documents

Figure. 1 Overview of proposed system

The system intends to utilize the wide range of knowledge from Wikipedia. The system uses the method of spreading activation for computing semantic similarity using category tree of Wikipedia. It can reduce the effort of building ontology for computing semantic similarity. It will produce the semantically related results.

The steps of the system are as follows. When the user enters the query as keywords he wants to search, the system will extract the corresponding Wikipedia articles of each keyword in the query. Then system will collect the lists of the categories of each article and count the categories which belong to the articles. The system will search the required information based on the category having the most occurrences. To rank the information according to their semantic similarity, the system will compute semantic similarity using spreading activation strategy based on the category tree of Wikipedia. So, the system has two main parts: one is searching for the category that has the most occurrences and another is computing the semantic similarity able to retrieve the semantically relevant information.

6. COMPUTING SEMANTIC SIMILARITY WITH SPREADING ACTIVATION STRATEGY

To compute semantic similarity for our IR system, firstly we extract the Wikipedia categories of each query key word. Then we also extract the Wikipedia categories of document title in the document database. Before we do the latter extraction, we need to search for the corresponding Wikipedia articles of the document title. Finally, we use all these categories extracted as the nodes of the category tree of Wikipedia and apply the spreading activation method to this category tree to get semantic similarity value.

The followings are the node input function, output function and semantic similarity computing function.

$$I_j = \sum_i O_i \qquad (1)$$

$$O_j = \frac{A_j}{D_j * k} \qquad (2)$$

$$\text{Similarity Value} = \frac{\sum_{\forall A_i \in Act} A_i}{|Act| * \max(A_i)} \qquad (3)$$

Where the variables are defined as:

O_i : Output of node i connected to node j

A_j : Activation value of node j

k : iteration number

D_j : Out degree of node j

I_j : input to node j from the child node i

(is also Activation value of node j)

Act : set of activation value

The activation process is iterative. All the original nodes take their occurrences as their initial activation value. And the activation values of all the other nodes are initialized to zero. Every node propagates it activation to its parents. The propagated value (O_j) is a function of its activation level. After a certain number of iterations, the highest activation value among the nodes that are associated with each of the original node is retrieved into a set Act = {A_1, A_2,…,A_{n+m}}. Then the similarity value is computed using the values from the Act set with the equation (3). The similarity value is normalized to value between 0 and 1.

7. CONCLUSION

In this system, we proposed the use of Wikipedia category tree and spreading activation strategy to compute semantic similarity. This system uses Wikipedia as an ontology. So it can reduce the effort of expert required to build ontology. Spreading activation strategy has produced excellent results for other semantic related system such as word sense disambiguation, semantic similarity computing using ontologies and describing documents. Therefore, the proposed system uses this method in the information retrieval system to produce the semantically related information along with the information required for the user.

8. REFERENCES

[1] Gabrilovich, E. and Markovitch, S., "Computing semantic relatedness using wikipedia-based explicit semantic analysis," Proc. Of the 20th International joint Conference on Artificial Intelligence (IJCAI'07), pp. 6-12.

[2] Sapkota, K. Thapa, L. and Pandey, S., "Efficient information retrieval using measures of semantic similarity," Nepal Engineering College.

[3] Yazdani, M. and Popescu-Belis, A., “A random walk framework to compute textual semantic similarity: a unified model for three benchmark tasks”.

[4] Zesch, T. Müller, C. and Gurevych, I., “Using wiktionary for computing semantic relatedness,” Proc. Of the Twenty-Third AAAI Conference on Artificial Intelligence (2008), pp. 861-866.

[5] Syed, Z. S. Finin, T. and Joshi, A., “Wikipedia as an ontology for describing documents,” Association for the Advancement of Artificial Intelligence, 2008, pp. 136-144.

[6] Zhiqiang, L. Werimin, S. and Zhenhua, Y., “Measuring semantic similarity between words using wikipedia,” International Conference on Web Information Systems and Mining, 2009, pp. 251-254.

[7] Thiagarajan, R. Manjunath, G. and Stumptner, M., “Computing semantic similarity using ontologies,” the International Semantic Web Conference (ISWC), 2008, Karlsruhe, Germany.

[8] Hajian, B. and White, T., “ Measuring semantic smilarity using a multi-tree model,” 2011.

[9] Milne, D. and Witten, I. H., “An effective, low-cost measure of semantic relatedness obtained from wikipedia links,” Proc. Of AAAI Workshop on Wikipedia and Artificial Intelligence: an Evolving Synergy, AAAI Press, Chicago, USA, pp. 25-30.

[10] Yeh, E. Ramage, D. Manning, C. D. Agirre, E. and Soroa, A., “WikiWalk: Random walks on wikipedia for semantic relatedness,” Proc. Of the 2009 Workshop on Graph-based Methods for Natural Language Processing, ACL-IJCNLP 2009,Suntec, Singapore, Aug 7. 2009, pp. 41-49.

[11] Strube, M. and Ponzetto, S. P., “WikiRelate! Computing semantic relatedness using wikipedia,” Proc. Of the National Conference on Artificial Intellignece, 2006, volume 21.

[12] Gouws, S. Rooyen, G. and Engelbrecht, H. A., “Measuring conceptual similarity by spreading activation over wikipedia’s hyperlink structure,” Proc. Of the 2nd Workshop on “ Collaboratively Constructed Semantic Resources”, Coling 2010, Beijing, August 2010, pp. 46-54.

International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 81-85, 2013

Generating User Interesting Page (UIP) Using Supported Weight Value

Nu Yin Kyaw
University of Technology,
Myanmar

Abstract: With an increasing continuous growth of information in WWW, it is very difficult to extract useful and relevant information from the huge amount of information. So, without any help on the system, the user may spend more time to get the interested information from the website. To solve above the problem, we proposed an approach for generating user interesting page (UIP) using weight value on web log data by associating with web usage mining techniques. Web usage mining, a classification of Web mining, is the application of data mining techniques to discover usage patterns from click stream data. This information can be exploited in various ways, such as enhancing the effectiveness of websites or developing directed web marketing campaigns. The goal of our system is to analyze user behaviours by mining enriched web access log data and create a top web page for the user with common needs or interests. This paper also focuses on to provide an overview how to generate frequent access pattern for the users from a Web log database without the use of domain specific ontology.

Keywords: web usage mining, web log data, user session identification, user interesting page, click stream data

1. INTRODUCTION

With the continuous growth and abundance of information on the Internet, the World Wide Web (WWW) becomes a huge repository of information. Nowadays, the Web has become an important medium to communicate ideas, transact business and promote entertainment. The discovery and analysis of useful information from the Web documents is referred to as Web mining [1].

The Web mining [2] are the set of Data mining techniques applied to the web. Web mining can be divided into three categories: web content mining, web structure mining and web usage mining. Web content mining is the process of extracting knowledge from documents and content description.

Web structure mining is the process of obtaining knowledge from the organization of the Web and the links between Web pages. Web usage mining analyzes information about webs pages that were visited which are saved in the log files of Internet servers to discover the previously unknown and potentially interesting patterns useful in the future.

In our paper we concentrate the web usage mining topic; it is one of the intensive research areas as its potential for personalized services and adaptive web sites. Generally, Web Usage Mining consists of three processes: [3] data preprocessing, patterns discovery and patterns analysis. In the data sources of patterns discovery, the results' quality of data preprocessing influences the results of patterns discovery directly. Better data sources can not only discover high quality patterns but also improve the performance of Web Usage Mining. So, data preprocessing is particularly important for the whole Web Usage Mining processes and the key of the Web Usage Mining's quality

At present, since the web becomes the largest unstructured data source available, this condition presents a challenging task for effective design of and access to web pages and need more time to search and get interested information. To overcome the above problem, in this paper, we propose a system for improving the web site design and also for the users to collect their interested information in a better way and then generates personalized web page of their interest dynamically. Today, most web site use ontology-based model for personalization to obtain semantic information. Ontology [6] is a description of concepts and their relationships that can exist in the domain of interest. But in general, ontology does not provide the concept of personalization. So, we want to create a system that generates user interested page (UIP) without the use of the specific domain ontology.

In this paper, we give more attention for identifying clients and collecting the information from the user sessions for the analysis of HTTP requests made by clients. Usually a user session is a collection of requests made by the user within an interval of time. In the previous studies, sessions' identification was considered that a user can not be stationed on a page more than 30 minutes. [7] The current study intends to add an improvement in sessions' identification and user's identification with promising algorithms to improve the performance of generating user's interested page. Our proposed system, user interested page (UIP) , will be created by assigning weights and positioning the user interest by count the number of occurrence of each item which was collected from the web logs in a session for all users. From that it personalizes the interested pages to the web users in their next access to the system.

.

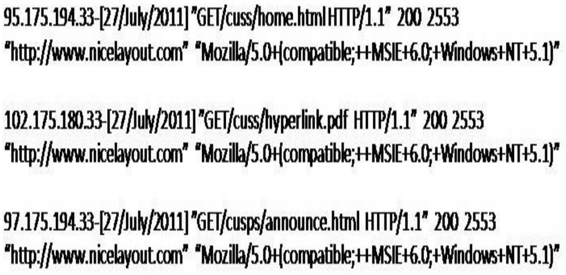
2. RELATED WORK

More and more researchers focus on Web Usage Mining recent years. There are lot of approaches dealing with web usage mining for the purpose of finding the interesting information (or) automatically discover the user pattern to improve the purpose of web site design. Pei *et al.* [12] have successfully used the log data from Web logs to discover frequent patterns, they proposed an algorithm called (WAP) Web access pattern tree for efficient mining of access patterns from pieces of logs, Murate *et al.* [13] highlights the importance of analyzing users web log data and extracting their interests of web-watching behaviors and describes a method for clarifying users interests based on the analysis of the site-keyword graph, while Borges *et al.* [14] modeled users' to capture Web navigation patterns. Dr.K.Iyakutti and P.Arun [11] also proposed a web personalized system in order to understand the behavior of the users and also to improve web site design. In this model, user identification is considered under the client IP address only. Session identification is considered using predefined time based method. In fact, time based method is not appropriate for session identification. They offered the inaccurate performance and results when giving personalized recommendation to users. However, this model has no serious drawbacks. While Spink *et al.* [15] analyzed characteristics of general Web search logs from different perspectives: terms, queries, sessions, and result pages. They showed top users short queries, a small number of search terms were used with high frequencies, few queries were modified, few result pages per query were be visited, and the popularities of query topics.

3. DATA PREPROCESSING

Log files [7] are created by web servers and filled with information about user requests on a particular Web site. These log files are stored in various formats such as Common Log Format (CLF) or Extended Log Format (ELF). Every entry in the log file stores the following fields:

- Client IP address or host name
- Access time
- HTTP request method(GET, POST)
- Path of the resource on the Web server
- Protocol used for transmission
- Status code
- Number of bytes transmitted.
- User agent(browser, operating)
- Referrer



```
95.175.194.33-[27/July/2011]"GET/cuss/home.html HTTP/1.1" 200 2553
"http://www.nicelayout.com" "Mozilla/5.0+(compatible;++MSIE+6.0;+Windows+NT+5.1)"

102.175.180.33-[27/July/2011]"GET/cuss/hyperlink.pdf HTTP/1.1" 200 2553
"http://www.nicelayout.com" "Mozilla/5.0+(compatible;++MSIE+6.0;+Windows+NT+5.1)"

97.175.194.33-[27/July/2011]"GET/cusps/announce.html HTTP/1.1" 200 2553
"http://www.nicelayout.com" "Mozilla/5.0+(compatible;++MSIE+6.0;+Windows+NT+5.1)"
```

Figure. 1 A portion of server web log

A portion of the raw web access log files on the server before data cleaning is shown in Figure.1. a successful analysis is based on accurate information and quality of web log data, preprocessing plays an important role.

Data Collecting: we collect the web logs from the commercial website, it has many items. But the web log file we compute contains the following entries:

- Date and Time Stamp
- IP Address (Internet Protocol Address)
- URL address of the access item
- User Agent
- Referrer, etc.

Data Cleaning: The purpose of data cleaning is to remove irrelevant items stored in the log files that may not be useful for analysis purposes. [8],[9]When a user accesses a HTML document, the embedded images and multi-media files are also automatically downloaded and stored in the server log. For example, log entries with file name suffixes such as gif, jpeg, GIF, JPEG, jpg, avi and flv can be removed. This can be done by checking the suffix of the URL name. In addition to this, erroneous files can be removed by checking the status of the request (such as a status of 404 indicates that the requested file was not found at the expected location). A status with value of 200 represents a succeeded request. A status with value different from 200 represents a failed request.

User Identification: A user is defined as the principal using a client to interactively retrieve and render resources or resource manifestations. [11] The Web Usage Mining methods that rely on user cooperation are the easiest ways to deal with this problem. However, it's difficult because of security and privacy. In previous case, user identification is done under IP address heuristic only. IP addresses, alone, are generally not sufficient for user identification. In our paper, we use the subsequent heuristics to identify the user. The following is the algorithm we use to identify individual user in our system. We think that our proposed algorithm will improve the efficiency and the accuracy of user identification.

Proposed Algorithm for User Identification

Input: N entries of web log file

Output: identified User Sets

***Algorithm*:**

```
 While (! last entry of log file)

{

Compare IP address of first log entry with IP address of second log entry.

      If (both are same)

         Compare the user agent of both entries

          If (both agents are same)

             Check requested page is linked with the previous access pages.

              If (they are linked)

             Identify request entries are from the same user.

               Else

               Assume that they are different users.

            Else        /* both agents are different */

              If (user path traversal is similar as previous one)

             Identify request entries are from the same user.

              Else

                Identify request entries are from the different user.

     Else   Assume that they are different users.  /* IP are different */

}  // while loop
```

Session Identification: A user session can be defined as a set of pages visited by the same user within the duration of one particular visit to a website. Users may have visited the pages for long periods of time. It is necessary to divide the log entries of a user into multiple sessions through a prescribed timeout. The method of portioning into sessions is called as Sessionization or Session Reconstruction. At present, the methods to identify user session include timeout mechanism and maximal forward reference mainly. Time-based session identification can't give accurate user's interesting page.The following is the proposed algorithm that we will use to identify user's session in our system:

Proposed Algorithm for Session Identification

Input: N requests of user set, Traversing Maximum Time, Traversing Minimum Time, 2D array.
Output: Identified Session Sets
Algorithm:

```
While (! Last entry row of 2D array)
{
    Step 1: Calculate the visiting time of a web page of a user.
    Step 2: Compare the visiting time with Traversing Maximum Time and Traversing Minimum Time of each web page.
            If the visiting time is less than Traversing Maximum Time then assign the weight as 0.

            Else if visiting time is between Traversing Maximum Time and Traversing Minimum Time then assign the weight as 1 to 10.

            Else if browsing time is greater than Traversing Maximum Time then assign the weight as 100. And if referrer URL is null then weight is assigned as 000.

            If the same page is visited by the user again in each user's set then increment the corresponding entry object.
}
```

To identify user sessions, 2D array is constructed form the user's traversal. Columns are the web pages and rows are users. Visiting time for a particular page is determined by finding the differences between the time fields of two consecutive entries of a same user. Website designers must fix traversing minimum time and traversing maximum time for all web pages as per the contents and loading times. We will compare the visiting time of a user with traversing minimum time and traversing minimum time.

If the value stored is 000 the next entry will be stored as next session in next row. The advantage of assigning weights is that we can observe behaviour of users such as navigation pages, interested pages, and longer duration pages. This information is used to discover interesting patterns of each user for the system.

Data Filtering: It is the process of leaving out less requested resources in the session and retains only the most requested ones. By removing the least requested resources, we can raise performance and accuracy of the system.

4. STAGES FOR GENERATING USER INTERESTING PAGE

Web Log categorizing: It is categorizing of the web logs. For that, it first categories every item of the website and coded as numeric based sequence.

Code	HTML Page Links
1	Shirt
2	Trouser
3	Handbag
4	Cosmetic

Gathering Click Stream Data: It is collecting of the click stream data for each user from each user session.

TABLE I: WEB LOG DATA FOR THE TWO USERS

User	Request Access items
192.168.1.2	123413231342344341
95.102.3.4	1242431234123

Counting Occurrence / Assigning weight & Ranking order: Count the number of occurrence of each item. Based upon the count, the activities that the user makes, it assigns weight and ranking the weblog data in the order of weights**.**

Generating most user interesting page: Find the interesting pages for every user. It generates most_user interesting page for personalization based upon their previous access information (web logs).

Ontology serves as Meta data schemas, providing a controlled vocabulary of concepts, each with explicitly defined meaning. It is a description of concepts and their relationships that can exist in the domain of interest. It is the easiest way to structure the information through the use of ontology, a link will be created to all the items and it is like a graph of concepts. There are lot of tools are available to create ontology's like onto edit, onto seek, onto maker etc. But in general, ontology does not provide the concept of personalization, but in our system, based upon the previous access user information, it positions the user pages based upon their weights and create interested web page to the users in their future access. So in our system, it creates user interested page (UIP) for personalization to the users based upon their previous access information (web logs).

5. PROPOSED USER INTERESTING PAGE SYSTEM

Our system intends to find out the Interesting Web Pages for each and every user by analyzing use's click stream data on the web log files. We discover that web page from the identified user's session. From each session, we find top web pages according to the following criteria.

- How many times the user will access the page (count)
- How the user will access that page either directly or through any other page
- How much time the user will spend in that page (Access time – Leave time) and

- What are the activities are done in that page such as (just looking information in the pages, ordering items, registering in the form) etc...

For each and every user, it counts the number of occurrence of each item which was collected from the web logs. For each item of the user, the system will find out the time difference between the entry and exit in each item, the operations which was done in that item, how many access the web pages etc.

The system stores all these information in user's corresponding record of pre-database. Based upon the count, time and activity it assigns weights for that page and store it in the weight database. It positions the weights in decreasing order and stored it in the weight database. For each and every user, their will be a separate record in pre-database and a weight database where the weight database contains the user-id, item and the corresponding weight. Based upon the position, it will measure the users' most interested web page in the web site and the same process will be used to generate the User Interested Page (UIP) for all users.

The important concept of our system is that our UIP will be updated dynamically based upon the access of the web pages by the users even when they change their desires. The final step of the proposed model is to generate personalized web pages to the user after completing the above steps. We can also find the user's interested web page for next times when the user will enter into the website. Suppose during that time if the user will access some more pages which were not accessed during his previous visit, the model will collect those information from the web logs and based upon that it updates the counts and weights in the corresponding users' corresponding record of pre-database and the weight database. From that it measures the positioning and updates that users' UIP dynamically and the updated version of that UIP will be personalized to that user during their next visit.

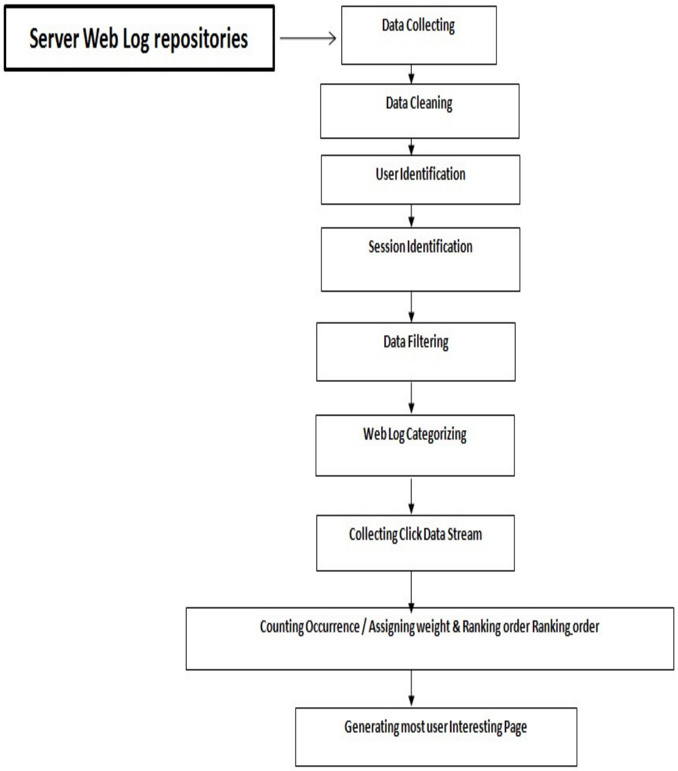

Server Web Log repositories
Data Collecting
Data Cleaning
User Identification
Session Identification
Data Filtering
Web Log Categorizing
Collecting Click Data Stream
Counting Occurrence / Assigning weight & Ranking order Ranking order
Generating most user Interesting Page

Figure. 2. A proposed system that generating UIP for web personalization

We design our system as shown above figure-2 that generates the UIP from that it find out the interesting web pages for the users and also it personalize those pages to the users during their next visit. And this system will be implemented in the Java Language.

Our system will assign some value for the supported weight on the corresponding items. If the weight of the access web page is greater than the support weight assigned by the system, the system accept that item and store it in the weight database, otherwise it just keep that object in that users' corresponding record of pre-database.

In future, if the user will access the item from the website, then the system will increment the corresponding count in the record of pre-database and if the item's count is greater than the support weight, then it updates its weight in the weight where the item's already available in the weight database itself. This dynamic updating of the user's interest was done in our system.

Ontology is the formal, explicit specification of shared conceptualizations. In general, ontology does not provide the concept of personalization, but in our system it creates User Interested Page for personalization that find out the interested web pages to the users based upon their previous access information. The User Interested Page will be generated as follows:

- It creates a link to the most interested web page which was available in weight database and that link will be accessed by that user.
- The above process (creating link) is repeated for all the remaining items available in the weighted database for that user.

From that UIP, it personalizes the most interesting web pages to the users. If we apply the above methods in a website, in future, the user will access the website, it personalizes the interesting pattern to those users without wasting their time with fine accuracy. This is the concept of analyzing browsing behavior by collecting basic browsing elements and defining the most interesting pages for each user using user interested page (UIP) generation system for web personalization.

6. PROSPECTS AND DISCUSSION OF OUR PROPOSED SYSTEM

Our system will guide the user to find their interested information they want in accurate and fast manner without browsing the whole web site. There are several approaches dealing with web usage mining for the purpose of finding the interesting information (or) automatically discover the user pattern. But in our system, the whole process will be divided into nine sub processes they are: 1.Data Collecting 2.Data Filtering 3.Data Cleaning 4.User Identification 5.Session Identification 6.Web Log Categorizing 7.Collecting Click Stream Data 8.Counting Occurrence/ Assigning weight & Ranking order 9. Generating most user interesting page. Our proposed system can be simple. This system may generate personalized user most interested web page without using privacy information of users. It also help the web designer which page category are getting top for user's interest and which one is less for users and also improve the web site design too.Once this is successfully completed then the system will provide the positive personalization or recommendation to the user. This new system will be implemented in Java Language. And we will collect log files from the commercial web server.

By implementing our UIP system with above promising algorithms for user and session identification, we believe that our system will be difference than existing cases when generating user's interested information. Our system will also perform the actions with good accuracy, performance and fast manner in accessing the desired web pages.

The main purpose of our system is to find out the interesting web pages for the users based upon the user's interest. It may also be possible to improve the website design. The main aim of our system is to improve the performance of the access method for the website, (i.e.) the personalization process will surely improve the system performance when compared to the normal access by the user.

7. CONCLUSION

At the beginning we present on data preprocessing which has been performed on the log files. Here we presented the methods that we proposed for session and user identification with algorithms. Having the data preprocessing step done, we can then go to other important steps for information mining, the one of effectively extracting useful information from the raw web log data. Mining web important information from web site pages is an important task as it helps web site designers to improve the design of the site. It gives better satisfaction for the final user. By mining most user's interested web pages from web logs; the web site designer can discover the bad web page in the web site and can change the design. Our system presents different ways of solving this problem with better performance. The novelty brought by this work will be implemented by the Java application with a friendly graphical user interface. When implementation is completed, our system can be helpful for site developer in order to arrange the pages and so bring customer satisfaction and increase sells. This also will help web site designers and developers to improve the initial design created and so attract more visitors by the user friendly interface developed. So, the web site designers can determine the web pages that are not correct located and bring them to the right position. But our proposed system will depend on professional web designer to assign weight on every web page of the web site to generate interesting web pages. When our current proposed system is finished completely, our practical experimental results will suggest the significance of the proposed approach.

8. REFERENCES

[1] C.P. SUMATHI, R. PADMAJA VALLI, T. SANTHANAM,"An overview of preprocessing of web log files for web usage mining", Journal of Theoretical and Applied Information Technology, 15th December 2011.

[2] J. Srivastava, R. Cooley, M. Deshpande and P. Tan, "Web usage mining: discovery and applications of usage patterns from web data", SIGKDD Explorations, 1(2):12–23, 2000.

[3] Jaideep Srivastava, Robert Cooley, Mukund Deshpande, Pang-Ning Tan. "Web Usage Mining: Discovery and Applications of Usage Patterns from Web Data", SIGKDD Explorations, 2000, Vol. 1(2):1-12.

[4] S.SenthilKum ar and T.V.Geetha, "Personalized Ontology for Web Search Personalization", Annual Bangalore Compute Conference**,** Proceedings of the 1st Bangalore annual Compute conference Bangalore, India, Year of Publication: 2008 ISBN: 978 -1-59593 -950-0.

[5] Alexander Maedche and Steffen Staab," Ontology Learning for the Semantic Web", Ontoprise GmbH, Haidund-Neu-Strasse 7, 76131 Karlsruhe, Germany.

[6] K.R. Reshmy and S.K.Srivatasa, "Automatic Ontology Generation for Semantic Search System Using Data Mining Techniques", Asian Journal of Information Technology 4(12) 1187-1194, 2005.

[7] D.Claudia Elena**,** "Association and Sequence Mining in Web Usage", Annals of "Dunarea de Jos" University of Galati Fascicle I. Economics and Applied Informatics,1 June 2011.

[8] R.Cooley, Bamshad Mobasherand Jaideep Srivastava, "DataPreparation for Mining World Wide Web Browsing Patterns." Knowledge and Information Systems, 1(1), 1999, 5-32.

[9] R.Cooley, B. Mobasher and J. Srivatsava, "Web mining: Information and pattern discovery on the World Wide Web." 9th IEEE Inernational Conference on Tools with Artificial Intelligence. CA, 1997, 558-567.

[10] Li Chaofeng," Research and Development of Data Preprocessing in Web Usage Mining", Journal of Wuhan 430074, P.R. China.

[11] P.Arun, K.Iyakutti," Ontology Generation from Session Data for Web Personalization", Int. J. of Advanced Networking and Application 241 Volume: 01, Issue: 04, Pages: 241-245 (2010).

[12] J. Pei, J. Han, B. Mortazavi-Asl, H. Zhu, "Mining access patterns the efficiently from web logs" in PADKK '00: Proceedings of the 4 Pacific-Asia Conference on Knowledge Discovery and Data Mining, Current Issues and New Applications. London, UK: Springer- Verlag, pp. 396-407, 2000.

[13] T. Murata and K. Saito, "Extracting Users Interests from Web Log Data", Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence, Hong Kong, China, pp.343-346, 2006.

[14] J. Borges, M. Levene, "A Fine Grained Heuristic to Capture Web Navigation Patterns," ACM SIGKDD Explorations, Vol.2, No.1, pp.40-50, 2000.

[15] A. Spink and B.J. Jansen, "Web search: Public searching on the Web", Dordrecht: Kluwer Academic, 2004.