International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 325 - 328, 2014, ISSN: 2319–8656

Distributed Addressing Protocol for Node Auto configuration in Ad Hoc Networks using Bloom Filters

Bini M Issac
Amal Jyothi College of Engineering
Kanjirappally, India

Deepu Benson
Amal Jyothi College of Engineering
Kanjirappally, India

Abstract: The importance of wireless ad hoc networks in community and commercial connectivity cannot be underestimated in view of the benefits associated with such networks. An ad hoc network must assemble itself from any devices that happen to be nearby, and adapt as devices move in and out of wireless range. High levels of self-organization will minimize the need for manual configuration. However, efficiently providing unique addresses in ad hoc networks is still an open research question. The goal of this paper was to develop algorithms for address auto-configuration. The paper addresses the following among other problems: Achieving high levels of address uniqueness without compromising on latency and communication overhead. The proposed protocol uses bloom filters to reduce the storage overhead and remove communication overhead.

Keywords: Ad Hoc Networks, Bloom filters, Simulation, IP address, Birthday paradox

1. INTRODUCTION

An ad hoc network is a type of peer to peer wireless network mode where wireless devices communicate with each other directly, without the aid of a wireless access point device. Wireless networks typically depend on a base station or WAP device to manage and direct the stream of data between wireless devices. In an ad hoc setup, the network is built spontaneously as and when devices communicate with each other. These devices should ideally be within close range of each other; however quality of connection and speed of the network will suffer as more devices are added to the network. The term “ad hoc” tends to imply “can take different forms” and “can be mobile, stand alone, or networked”. Ad hoc implies that the network is formed in a spontaneous manner to meet an immediate demand and specific goal. Ad hoc networks have the ability to form “on the fly” and dynamically handle the joining or leaving of nodes in the network. Mobile nodes are autonomous units that are capable of roaming independently. Typical mobile ad hoc wireless nodes are Laptops, PDAs, Pocket PCs, Cellular Phones, Internet Mobile Phones, Palmtops or any other mobile wireless devices. Mobile ad hoc wireless devices are typically lightweight and battery operated.

2. BACKGROUND

The nodes of a network need some mechanism to interchange messages with each other. The TCP/IP protocol allows the different nodes from the network to communicate by associating a distinct IP address to each node of the same network. In wired or wireless networks with an infrastructure, there is a server or node which correctly assigns these IP addresses. Mobile ad hoc networks, on the other hand, do not have such a centralized entity able to carry out this function. Therefore, some protocol that performs the network configuration in a dynamic and automatic way is necessary, which will utilize all the nodes of the network (or only part of them) as if they were servers which manage IP addresses.

2.1 Related Work

Address auto configuration proposals that do not store the list of allocated addresses are typically based on a distributed protocol called Duplicate Address Detection (DAD) [4]. In this protocol, every joining node randomly chooses an address and floods the network with an Address Request message (AREQ) for a number of times to guarantee that all nodes receive the new allocated address. If the randomly chosen address is already allocated to another node, this node advertises the duplication to the joining node sending an Address Reply message (AREP). When the joining node receives an AREP, it randomly chooses another address and repeats the flooding process. Otherwise, it allocates the chosen address. This proposal does not take into account network partitions and is not suitable for ad hoc networks [1].

Other proposals use routing information to solve the addressing problem. Weak DAD [3], for instance, routes packets correctly even if there is an address collision. In this protocol, every node is identified by its address and a key. Collisions with the other nodes are identified by information from the routing protocol. Weak DAD can continuously detect duplicate addresses with information added to routing protocol packets. The main idea is to add a key to each address that is distributed by the routing protocol. Thus, the routing protocol packet format has to be modified. Other more complex protocols were proposed to improve the performance of network merging detection and address reallocation [6]. In these protocols, nodes store additional data structures to run the addressing protocol.

MANETconf [4] is a stateful protocol based on the concepts of mutual exclusion of the Ricart Agrawala algorithm. Using MANETconf, each configured node is able to assign addresses to new nodes and, therefore, maintains an allocation table of already assigned addresses in the network. In this protocol, nodes store two address lists: the Allocated list and the Allocated Pending list. A joining node asks for an address to a neighbour, which becomes a leader in the address allocation procedure. The leader chooses an available address, stores it on the Allocated Pending list, and floods the network. If all MANETconf nodes accept the allocation request and positively answer to the leader, then the leader informs the allocated address to the joining node, moves the allocated address to the Allocated list, and floods the network again to confirm the address allocation. After receiving this message, each node moves the address from the Allocated Pending list to Allocated list. MANETconf handles address reallocation, but partition detection depends on periodic flooding. Therefore, this protocol incurs in a high control overhead.

3. PROPOSED PROTOCOL

The proposed protocol uses IP addresses for communication. Every new node in the ad hoc network randomly selects an IP address. But due to birth day paradox problem, there is a chance for address collision. So the protocol performs duplicate address detection. The protocol uses a distributed bloom filter to represent the current set of allocated addresses. This filter is present at every node to reduce the control overhead required to solve address collisions inherent in random assignments [1]. If more than one node selects the same IP address then address collision will occur and it will detected with less overhead.

In probability theory, the birthday problem or birthday paradox[5] concerns the probability that, in a set of n randomly chosen people, some pair of them will have the same birthday. By the pigeonhole principle, the probability reaches 100% when the number of people reaches 367 (since there are 366 possible birthdays, including February 29). However, 99.9% probability is reached with just 70 people and 50% probability with 23 people.

3.1 Distributed Approach

The choice of a distributed approach [1] alleviates the need for instituting a process for the election of a central node that performs the address allocation process. The responsibility for address configuration has to be borne by all nodes that are already part of the network. There must not be a single Dynamic Host Configuration Protocol (DHCP) server since it is impossible to guarantee that the server will always be available. All nodes should collectively perform the functionality of a DHCP server.

3.2 Bloom Filter

The Bloom filter [6] is a compact data structure used on distributed applications. The Bloom filter is composed of an m-bit vector that represents a set $A=a_{1,}a_{2,....}a_{n}$ composed of n elements. The elements are inserted into the filter through a set of independent hash functions, whose outputs are uniformly distributed over the bits. First, all the bits of the vector are set to zero. After that, each element is hashed by each of the hash functions, whose output represents a position to be set as 1 on the m-bit vector. To verify if an element belongs to A, we check whether the bits of the vector corresponding to the positions are all set to 1. If at least one bit is set to 0, then A is not on the filter. Otherwise, it is assumed that the element belongs to A. There is, however, a false-positive probability that an element be recognized as being in A. This may happen when the bits at the positions are all set by previously inserted elements.

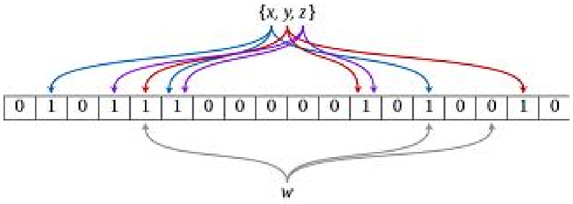


Figure 1 Bloom Filter

The steps involved in the protocol implementation are:

- Creation of traffic and topology
- Implementation of address configuration protocol and bloom filter
- Simulation using nam
- Analysis of trace file and Performance evaluation

4. SIMULATION ENVIRONMENT

We implemented the protocol in the Network Simulator- 2 (NS-2) and evaluated it considering the Two Ray Ground model for radio propagation and the NS-2 IEEE 802.11 model for the Medium Access Control. These models account for creating a scenario similar to a real community network, using parameters of commercial equipment. Simulation parameters are shown in table 1.

Table 1. Simulation Parameters

Parameters	**Environment**
Number of nodes	10
Maximum node speed	100.0
Radio propagation	Two Ray Ground
Network interface	Wireless physical
Area	1000 x 1000
MAC type	802_11
Link layer type	LL
Antenna model	Omni Antenna
Interface queue	DropTail/PriQueue
Simulation time	20 seconds
Routing protocol	AODV
Recorded parameters	Average end to end delay, total Transmission time ,Throughput

5. ANALYTICAL RESULTS

The probability of address collision is analyzed. A collision occurs when two different joining nodes generate AREQs with the same address. The joining nodes do not notice that their addresses are the same because the message from the other node seems to the first node like a retransmission of its own message. A joining node always sends an AREQ and, when any node that has already advertised the address receives the AREQ, it must check for a collision, regardless of its current state. Assuming there is no malicious behavior in the network, this situation occurs only in the initialization or when nodes join the network at approximately the same time because both nodes could choose the same available address in the filter. Therefore, if two or more nodes choose the same address, then address collision is detected.

The probability that two nodes choose the same address for an AREQ, causing a collision is given by equation 1 , can be derived by considering the birthday paradox, with being the space size of the concatenation of the address with the identifier number, and the number of nodes that are trying to access the network at approximately the same time, which means a set of initiator nodes or a set of joining nodes that search.

The protocol were run a number of times to evaluate the probability of collision and the results shows that for getting one address collision, the protocol has to be simulated at least 5 times.

5.1 Parameters Evaluated

The following metrics were chosen to evaluate the performance of the protocol.

1) Average Throughput: The throughput is directly related to address collisions. Throughput obtained will be zero, if an address collision is detected. Otherwise, a positive value will be obtained.

2) Total transmission time: Total transmission time for the packets is observed to be 20 seconds.

3) Average end to end delay: End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

Table 2. Sample Throughput and Delay Values

Simulation No	Average Throughput	Average End to end delay
1	461.059KB	159.180 ms
2	234.053 KB	243.123 ms
3	339.581KB	305.110 ms
4	402.124 KB	151.240 ms

Some of the values obtained for throughput and end to end delay are shown in table 2.

Figure 2 shows the throughput versus time graph of the proposed protocol.

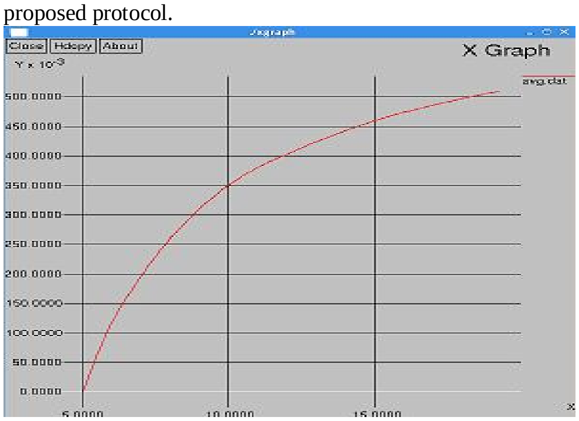


Figure 2 Throughput versus time graph

6. CONCLUSION

Lack of manual management in ad hoc networks means that automatic configuration is highly desirable. Automatic configuration of nodes in wireless ad hoc network will help in reducing administration efforts by users and network administrators. Initial investigation into this area identified the need for achieving high levels of address uniqueness without compromising on latency and communication overhead. Simulation experiments were done in NS2 to test the performance of the protocol and the various parameters were evaluated. Address filters avoids address collisions, reduces the control load, and decrease the address allocation delay.

7. REFERENCES

[1] Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte “An Efficient and Robust Addressing Protocol for Node Autoconfiguration in Ad Hoc Network” ,IEEE/ACM Transactions on Networking, VOL. 21, NO. 3, JUNE 2013

[2] C. E. Perkins, E. M. Royers, and S. R. Das, “IP address autoconfiguration for ad hoc networks,” Internet draft, 2000Tavel, P. 2007 Modeling and Simulation Design.

[3] N. H. Vaidya, “Weak duplicate address detection in mobile ad hoc networks,” in Proc. 3rd ACM MobiHoc, 2002, pp. 206216

[4] S. Nesargi and R. Prakash, “MANETconf: Configuration of hosts in a mobile ad hoc network,”in Proc. 21st Annu. IEEE INFOCOM, Jun. 2002, vol. 2, pp. 10591068.

[5] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security Privacy, May 2005, pp. 4963.

[6] Deke Guo , Jie Wu , Honghui Chen , Ye Yuan , Xueshan Luo “The Dynamic Bloom Filters” In Proc. IEEE infocom citations: 16 – 24 (2006)

[7] M. Fazio, M. Villari, and A. Puliafito, “IP address autoconfiguration in ad hoc networks: Design, implementation and measurements,” Comput Netw., vol. 50, no. 7, pp. 898920, 2006

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 329 - 332, 2014, ISSN: 2319–8656

A Recapitulation of Data Auditing Approaches for Cloud Data

Poonam Dabas
Kurukshetra University
Kurukshetra, India

Divya Wadhwa
Kurukshetra University
Kurukshetra, India

Abstract: Cloud Computing, a buzzword, a technology, has been exploring over the years since 1990s and presently, being considered as a today's s era dependency for the interconnected users. Online resources (like CPU processing power, memory space), software, hardware, capacities are being delivered to the associated users with no headache of handling the intricacies that could come while utilizing the services of this computing methodology. This dependency on server resources for all the major requirements of clients made this computing paradigm, a popular emerging trend in technical world. Now, the biggest concern that one must take into consideration while adopting the benefits of cloud computing is what we call it as 'security'. Obviously, it is the necessary attribute of any computing methodology that is considered as a priority concern. One primary aspect of cloud computing security is maintaining user data integrity which is the key point of this literature review paper. Integrity checking has been designed as a cloud security service by various protocols proposed by many researchers which are being discussed here in this paper.

Keywords: Cloud Computing; IAAS; PAAS; SAAS; Cloud Security; Integrity Checking

1. INTRODUCTION

Cloud Computing has been envisioned as the definite and concerning solution to the rising storage costs of IT Enterprises. Clouds have emerged as a computing infrastructure that enables rapid delivery of computing resources as a utility in a dynamically scalable virtualized manner. Cloud Computing is now on the way. It is a scalable and managed infrastructure and payable as per its usage [1]. The cloud computing technology has been evolved as business cloud models to provide computing infrastructure, data-storage, software applications, programming platforms and hardware as services.

Cloud computing architecture has basically three levels or layers over which it resides and operates. First level is SaaS (Software as a Service). Second layer is PaaS (Platform as a service). The third layer is IaaS (Infrastructure as a service).These levels or layers can also be regarded as cloud service models [2]. A brief idea about these levels is presented below:

- SaaS (Software as a service): At this level, occurrences of a software application can be shared among various users through internet browser. One does not have a need to install and manage particular application, it can be utilized online. Thus, software application is being provided a s a service. Google Docs is a cloud provided SaaS based service.
- PaaS (Platform as a service): In this Layer, customers can develop new applications using APIs which are deployed and configured remotely. There is no need to manage software and corresponding hardware for implementation and placement of application. Google App Engine is one of the PaaS examples.
- IaaS (Infrastructure as a service): In this service model, virtual machines and other abstract hardware and operating system are being made available for cloud users. More clearly, virtualization of computing power, storage and network connectivity is done by this service. The computing resources can be scaled up and down by users dynamically, that is, are hosted by the customer. Example includes Amazon's Elastic Compute Cloud (EC2).
Thus, the provision of dynamically scalable and often virtualized resources can be made as a service by this evolving cloud computing technology over the internet.

This paper is structured as follows: An introduction to cloud computing and different service models are described in this section. Further, a look is made to cloud security pertaining to data integrity issue through section 2. Next, a review of the related work concerning data integrity checking protocols developed so far is presented in the section 3. Analysis based challenges and future scope is being lightened upon in section 4. Finally, a report of the conclusion of the study of cloud data integrity maintenance is outlined in section 5.

2. A LOOK AT CLOUD SECURITY: CONCERNING DATA INTEGRITY

Security! It is the key for the eminence of a cloud. It is a primary matter of concern for many cloud consumers. Actually, security and privacy interests are a compelling hurdle that is hindering the considerable acceptance of the public cloud across IT entities. As in today's era, computing continuity continues, more devices are adopting more applications, and all these advancements leads to storage of data on external resources which ultimately relates to various privacy issues. These issues comprise the intentional alteration of data without the knowledge of actual data owner, unauthorized access to customer data, not being able to access stored data, unpredicted deletion of crucial information, etc. One of the solution, one might think is to store the data in such a manner that it is of no use to anyone except real owner. Sometimes, the very much strong concern for cloud security make implementation too complex and bulky, while on the other hand, if more attention is paid over reducing all that complexity, security is compromised as a consequence. Whatever approach is realized, all it needs that all the data protection schemes comprises a compromise between security and the comfort of implementation, no doubt, it should include more secured results [3]. An economic solution is looked upon so that the companies and organizations can focus on their businesses rather than on infrastructure. Well! The very concern of the presented literature review is regarding one aspect of cloud security that is named as Data Integrity Maintenance especially in dynamic cloud environment. Dynamic keyword elaborates in the sense that cloud data does not remain static, it keeps on changing from time to time. Protecting such dynamic data and related alteration comes under this aspect of cloud security. Data integrity is defined as the accuracy and consistency of gathered data, in absence of any modification to the data, while having two continued updates of a file or record. Cloud services should confirm data integrity and provide trust to the user privacy. We had a look over the various methods that have been developed for auditing cloud data and thereby, presenting here in this paper.

3. LITERATURE REVIEW

Various researchers have made major contributions to data integrity maintenance in reference to cloud security access issue. The protocols they developed, utilizes various cryptographic algorithms for implementing and imposing a desired level of security for cloud users so that their data can reside in a secured way, that is, the data could not be seen or altered by some untrusted party on cloud. Zhang Jianhang et al. [4] proposed a new data integrity check scheme based on the well known RSA security assumption. The very obvious advantage of their scheme was that the client did not need to store the copy data in their client side so this indeed freed the client from storage burden. A secure and efficient scheme/ terminology came into play, in which not only data owner but also a third party verifier can check data integrity. Qian Wang et al. [5] proposed an integrated approach of public audibility and dynamic data operations as two salient features of the designed protocol. They concentrated on this very fact because earlier works on ensuring data integrity often lacks the support of either public audibility or dynamic data operations. They designed a protocol that achieved both. A block less approach was adopted and the block tags were authenticated instead of original data blocks in the verification process. This made them noticed. Sravan Kumar R et al. [6] developed an integrity checking scheme which gives a proof of data integrity in the cloud which could be utilized by the customer to check the correctness of data in the cloud. The most important thing that came out of this addressed issue was that storage at the client was kept at minimal that would be beneficial for thin clients. This proposed scheme included an encrypting process that was limited to only fraction of whole data thereby saving on the computational time of the client. But it could not handle the case in which the data changed dynamically. Zhuo Hao, et al. [7] developed a remote data integrity checking mechanism that did not include any third party auditor. Data insertion, modification, and deletion at the block level, and also public verifiability were also promoted by this protocol. The difficulty found was that there was no clear mapping relationship between the data and the tags. Straightaway, data level dynamics could be supported by utilizing block level dynamics. At any time, a piece of data was altered; corresponding blocks and tags were also renewed. Ricardo Neisse et al. [8] presented a system that facilitated periodical and necessity-driven integrity measurements of cloud computing infrastructures. The emphasis was on verifying the integrity of the hardware and software at runtime whenever alterations in the cloud infrastructure were performed. The system developed could remotely keep a check and prove the integrity of necessary system files.

Wenjun Luo et al. [9] addressed a remote data integrity checking protocol based on HLAs and RSA signature with the support public verifiability. Also, this very mechanism was very satisfactory of cloud storage systems because it cloud preserve the file privacy against the third part auditor. This was made possible as the file was encrypted before it was sent to the server and the encryption was kept by the client as a secret. Thereby, the TPA could not be able to get any idea regarding the original file. M. Venkatesh et al. [10**]** proposed an RSA based storage security (RSASS) method which adopted public auditing of the remote data by upgrading existing RSA based signature generation. High level security could be achieved by this public key cryptography technique. The purpose behind using this RSASS method was that, firstly, data storage correctness could be satisfied, secondly, misbehaving server could be determined with a high probability. The preliminary results realized through RSASS, suggested scheme outperforms with upgraded security in data storage when correlated with the existing methods. Henry C. H. et al. [11] studied the problem of remotely checking the integrity of regenerating-coded data against corruptions under a real time operating cloud environment. They enforced the implementation of the functional minimum storage regenerating (FMSR) code and formulated FMSR, which was a code that made the clients to remotely check the integrity of random subsets of long term archival data under a multi-server setting. T.J.SALMA [12**]** explored the problem of data security in a cloud storage, which was actually taken as a distributed storage system. She proposed an effective and competent distributed scheme with a precise dynamic data support, counting block update, delete, and append. This scheme achieved the integration of storage correctness insurance and data error localization, that is, whenever data corruption had been detected during the storage correctness verification across the distributed server(s), mischievous server could be identified simultaneously.

Xiangtao Yan et al. [13] devised a new remote integrity checking scheme for cloud storage that merged correct checking, dynamic update and privacy preserving. In the presented integrity checking scheme, verifier stored only a single cryptographic key and a pre-computed value, irrespective of the size of the file it explores to verify, as well as a small amount of some dynamic state. Yun Yang et al. [14] proposed a fine grained data integrity check scheme. The method compressed effectively the check value for data integrity to reduce storage, and improved the check efficiency of multi-data objects. The focus was made on studying the data integrity of massive storage system in the power cloud computing. Dr. S. Sakthivel et al. [15] enabled a privacy preserving data integrity protection by facilitating public audibility for cloud storage at the hand of third party auditor. The framework used here was based on an associated PDP protocol that utilizes the challenge – response algorithms and a verification protocol. As third party auditor was included, thus, TPA works on behalf of the data owner who has a huge amount of data to be placed in the cloud. Boyang Wang et al. [16] introduced a novel privacy-preserving public auditing mechanism for shared cloud data, in which, a public verifier could be able to audit the integrity of shared data without having any idea about the private identity information of the group members. The concern was made over the group dynamics. Group dynamics relates to user join and user revocation. Bo Chen Reza Curtmola [17] proposed RDC (Remote Data Checking) scheme that provided robustness and, also, supported dynamic updates, while requiring small, constant, client storage. Remote data checking allowed clients to smoothly test the integrity of data placed at servers that are not trusted. Thus the main challenge that had to overcome was to reduce the client-server communication overhead during updates under an adversarial setting. Yan Zhu et al. [18] introduced a dynamic audit service for verifying the integrity of an un-trusted and outsourced storage. This audit service provided public audibility without downloading raw data and thereby, privacy of the data could be preserved. He Kai et al. [19] proposed a public batch data integrity auditing protocol for multi-cloud storage. Also, fast identification of corrupted data could also be made possible. This could be achieved by making use of homomorphic ciphertext verification and recoverable coding methodology. With this batch auditing methodology adopted in this protocol, the total auditing time could be reduced and the communication cost was also made low.

4. CHALLENGES AND FUTURE SCOPE

As cloud computing is becoming very popular now days. Being a continuing technology in the present era, security aspects of cloud computing is worth concerning. As due to this concern, we have gone through this survey for studying and observing various security challenges. It is a very much fact that the cloud users are often interested in having the integrity of their data stored on the cloud server not get altered in any of the way. The data have to remain intact and not get modified by an unauthorized user. Remote data checking allows for data auditing so that clients could check the integrity of the data at untrusted server. As the task of checking the dynamic data integrity is done by TPA, that is, third party auditor, on behalf of cloud client, the involvement of the client can be eliminated. Moreover, there are a number of challenges in implementing data dynamics. Generating data integrity proofs while considering dynamic nature of the cloud is also contemplated as a challenge for integrity maintenance. Furthermore, block level checking schemes are a bit complex and implementing those in an efficient way can be also regarded as a challenging task. Security and complexity of algorithm are two contradictory terms. A level of balance has to be established between them. Thus, the algorithms being developed for remote data integrity checking should be time and storage efficient and well suited. Thus, Future work aims at implementing these algorithms at minimal costs.

5. CONCLUSION

Cloud computing can be termed as an online service enabling sharing of resources. Proper utilization of the cloud services being offered makes performance of an enterprise well managed in terms of increased efficiency and less overhead incurred. This review paper presented gives us an idea regarding the protocols developed so far, for cloud data integrity maintenance. Many researchers presented their contributions towards this security aspect of cloud computing. They made various successful implementations considering many environmental computing conditions. Thus, very remarkable work has been performed in this area and has made further work more accessible and smoother. We intend to explore this idea of conducting research on this integrity issue.

6. REFERENCES

[1] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya “Service-Oriented Cloud Computing Architecture”, 2010

[2] Sikder Sunbeam Islam, Muhammad Baqer Mollah, Md. Imanul Huq, Md. Aman Ullah “Cloud Computing for Future Generation of Computing Technology”, 2012

[3] Intel IT “Enhancing Cloud Security Using Data Anonymization”, 2012

[4] Zhang Jianhang, chen Hua, “Security Storage in the Cloud Computing: A RSA-based Assumption Data Integrity Check without Original Data”, 143-147 (2010)

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, “Enabling Public Audibility and Data Dynamics for Storage Security in Cloud Computing”,847-859 (May 2011)

[6] Sravan Kumar R and Ashutosh Saxena, “Data Integrity Proofs in Cloud Storage”, 2011

[7] Zhuo Hao, Sheng Zhong, Member, IEEE, and Nenghai Yu, Member, IEEE**, “**A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability”, September 2011

[8] Ricardo Neisse, Dominik Holling, Alexander Pretschner, “Implementing Trust in Cloud Infrastructures”, 524-533 (2011)

[9] Wenjun Luo, Guojing Bai, “ENSURING THE DATA INTEGRITY IN CLOUD DATA STORAGE”, 240-243 (2011)

[10] M. Venkatesh, M.R. Sumalatha, Mr. C. SelvaKumar, **“**Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing”, 463-467 (2012)

[11] Henry C. H. Chen and Patrick P. C. Lee**, “**Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage”, 51-60 (2012)

[12] Ms. T.J.SALMA, “A Flexible Distributed Storage Integrity Auditing Mechanism in Cloud Computing”

[13] Xiangtao Yan, Yifa Li, **“**A Wew Remote Data Integrity Checking Scheme for Cloud storage With Privacy Preserving”, 704-708 (2012)

[14] Yun Yang, Lie Wu, Yulin Yan, Cong Xu, “Fine-Grained Data Integrity Check for Power Cloud Computing”, 1346-1350 (2012)

[15] Dr. S. Sakthivel, B. Dhiyanesh, “A PRIVACY-PRESERVING STORAGE SECURITY FOR SPATIAL DATA IN DYNAMICS CLOUD ENVIRONMENT”, 2013

[16] Boyang Wang, Hui Li, Ming Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, 295-302 (2012)

[17] Bo Chen, Reza Curtmola, **“**Robust Dynamic Provable Data Possession”, 2012

[18] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu, “Dynamic Audit Services for Outsourced Storages in Clouds”, April-June 2013

[19] He Kai, Huang Chuanhe, Wang Jinhai, Zhou Hao, Chen Xi, Lu Yilong, Zhang Lianzhen, Wang Bin, “An Efficient Public Batch Auditing Protocol for Data Security in Multi-Cloud Storage”, 51-56 (2013)

.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 333 - 338, 2014, ISSN: 2319–8656

Modeling and Performance Evaluation TAODV Routing Protocol Using Stochastic Petri Nets

Sanaz Talebi
Department of computer science,
Shabestar Branch, Islamic Azad
University,
Shabestar, Iran

Mohammad Ali Jabraeil Jamali
Department of computer science,
Shabestar Branch, Islamic Azad
University,
Shabestar, Iran

Mehdi Ayar
Department of computer science,
Shabestar Branch, Islamic Azad
University,
Shabestar, Iran

Abstract: For a successful route request in Mobile Ad-hoc Networks (MANETs), it is important to know that routing protocols work correctly. On the other hand, this phenomenon acts randomly and it is not often possible to predict their act from one moment to the next. One way for ensuring correct operation of the protocol is to develop a formal model and analyze it. Stochastic Petri Net (SPN) is a formal modeling language which causes the analytical model to be a formal model. Also, prediction of future system's behavior is done in a shorter time than simulation. In this paper, an analytical model based on SPN was presented for TAODV routing protocol. The results showed that the analytical model acted like simulation model in terms of reliability, availability, and mean time to security failure parameters.

Keywords: Mobile Ad-hoc Networks; TAODV routing protocol; Stochastic Petri net; Modeling; Trust

1. INTODUCTION

MANETs are a set of mobile wireless nodes that form a dynamic local network. These networks do not have any central control infrastructure. MANTEs can be formed, integrated together, or divided into separate networks without depending on any fixed infrastructure management. In such networks, each mobile node does not act just as a host but also as a router which sends and transits packets to other mobile nodes if they have overlap in their transition zone [9]. These inherent properties cause MANETs to be more prone to security threats and causes security problems. Because the probability of eavesdropping, spoofing denial of service and impersonation attacks increases, MANETs need to be a trust model. So, trust management in MANETs has made variety applications such as security routing [7]. In development of trust management system in MANETs, the highest focus is on developing secure routing protocols based on trust. One of the proposed routing protocols in this topic is TAODV (Trust AODV).

Considering that simulation is only used to show details of a system, in order to analyze performance of MANET, it cannot do theoretical analysis and predict further behavior of such networks in a large scale and short time. To solve this problem, an analytical model using PNs (Petri Nets) was presented for analyzing performance of a routing protocol. To represent network features using PNs, there are two pre-requisites. 1- A model should be detailed enough to describe some important network characteristics that have significant impact on performance. 2- It should be simple enough to be scalable and analyzable [12]. To show asymptotic behavior of TAODV routing protocol, SPN (Stochastic Petri net) is used. SPN is a way for making an analytical model. It is a directed graph consisting of two parts and is made of two elements of place and transition. It provides time information of a model as exponential distribution and describes dynamic characteristics of the system (concurrency, synchronization, and inconsistency) [6]. PIPE tool [11] is an SPN-based tool. Also, MATLAB software was used to validate and determine accuracy of the proposed analytical model. The rest of this paper is organized as follows. Section 2 is a brief review of the related works. In Section 3, structure of analytical model is presented. Analytical and simulation results are given in Section 4 and conclusions are made in Section 5.

2. RELATED WORKS

According to the numerical analysis and structure of PNs, many works have been done to investigate characteristics such as reliability, availability and so on of wireless network. In [8], an analytical model was presented for AODV and DSR routing protocols using colored Petri Net. In this paper, a topology approximation method was used to solve problem of topology changes. In [4], a key management protocol for GCSs was analyzed to deal with internal and external attacks in MANETs using SPN. In this protocol, a trust chain was introduced. During the analysis, optimal length of a trust chain was calculated. In [3], a mathematical model for quantitatively analyzing a scalable region-based hierarchical group key management protocol was integrated for GCSs in MANETs. In [12], an analytical model was presented for MANETs which made the same results as analytical model. This work is similar to our model.

3. SYSTEM MODEL

In this section, a way is presented for modeling the TAODV routing protocol.

3.1. Analytical Model for Manets Using SPN

According to Table 1, operational area was assumed M * M square meters. Nodes had a radio range equal to R meters and N showed the number of nodes in network. For all the nodes, equal radio range was assumed. The allocated buffer was equal for each node. If the maximum number of received packets of a node was reduced to thresh, the node was converted into node congestion. Max parameter indicated the maximum number received packets of a node. The number of nodes in MANET was assumed constant.

In the presented model using SPN, the store place is created to save all the packets sent by nodes to each other. Figure 1 shows store place and first level of connecting nodes to store place.

Table 1. Assumed values for main parameters

Parameters	Values
M	670m
R	150m
N	4
Packet	512MB
Buffer	2GB
Thresh	1 Packet
Max	4 Packets
Source Node	1
Destination Node	4

In Figure 1, the NODE places show pattern of each node for doing routing protocol. When each of the nodes sends a packet, the OUT transition is fired. Then, the packets are located in the store place. In order to add a new node to the network, a pattern of the node is created and connected to the store place. In SPN, token is used to represent sending and receiving packets. In each node, after packet creation, a copy equal to the number of neighboring nodes is taken and sent to store place, which is shown by weights of the output arc from the OUT transitions. When weight of arc is 3, it means that 3 copies of the packet are sent to the store place. Then, packets are sent to the neighboring nodes.

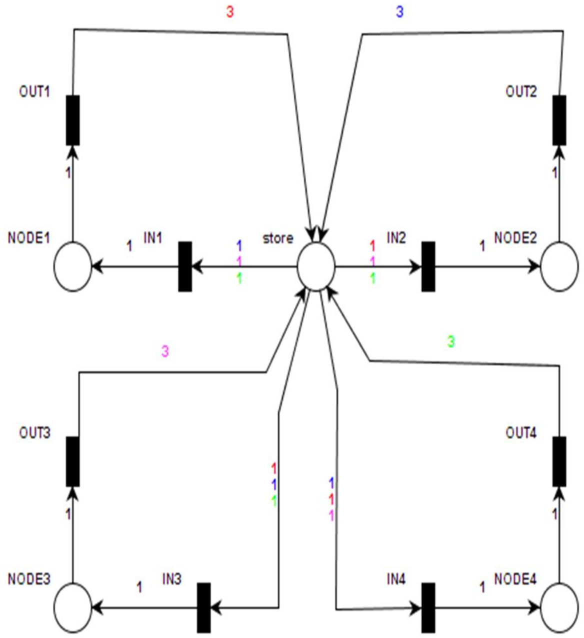


Figure1. Connection nodes to the store place

Figure 2 shows receiving route request packet by a node. For each neighbor node, an arc of the store place is received with 1 weight and the same color with packets of neighbor node.

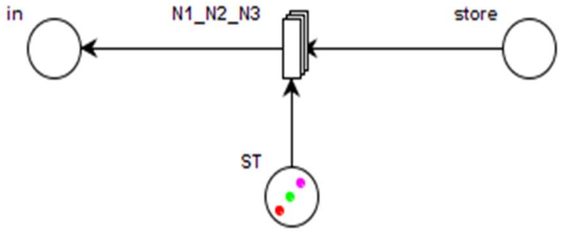


Figure 2. Receiving route request packet by a neighbor node

Because all nodes use the store place, it is possible for a node to receive a packet more than once from a specific node. To avoid this problem, in Figure 2, a place is assumed to be called ST. Initial tokens in the ST place indicate the current node neighbors.

3.2. Analytical Model for TAODV Protocol Using Stochastic Petri Nets

In this analytical model, there are two patterns of nodes in the network: pattern of intermediate nodes and pattern of source and destination nodes. The rest of the paper discusses patterns of nodes.

3.2.1. Intermediate Node's Pattern

There are three types of patterns for receiving packets in intermediate nodes. Intermediate nodes receive the route request packet in order to discover route, the chock packet due to congestion of neighbor nodes and the RREP packet in order to make path. Figure 2 shows receiving the route request packet's pattern and Figure 3 demonstrates receiving the chock packet's pattern by a node. When the RREP packet is generated, if the node is congested, it makes the choke packet and sends to one hop neighbor nodes. Thus, neighbor nodes are notified of the node congestion's condition.

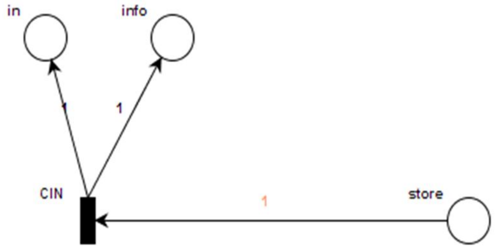


Figure 3. Receiving the chock packet's pattern

In the chock packet's pattern, separate colors are intended for each node. When a node receives the choke packet from the store place, the CIN transition is fired and one token is put in place for processing and allocating a buffer. Also, one token is put in the info place, which shows that a node received the choke packet.

Figure 4 shows the RREP packet's pattern in the intermediate node. In this pattern, when a node received the RREP packet, by firing the REP transition, a token is put in the inc-pen place and one of the inc (the MT1 or the MT2 transition) is fired for calculating penalties or incentives node. The inc transition is for calculating incentive and the MT1 and MT2 transitions are used for calculating penalties. If r> thresh and the sed transition is fired, the RREP packet was sent to the next node. In the route place, the node receiving the RREP packet is specified. The uni place guaranteed that the node will receive the RREP packet just once. When

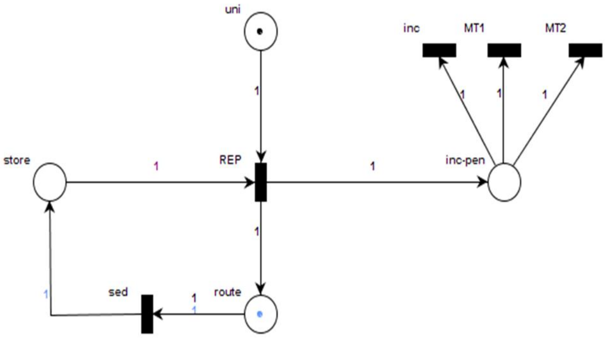


Figure 4. Receiving the RREP packet's pattern

the source node receives the RREP packet, the route discovers the ends.

In Figure 5, when the Ai transition is fired, the packet receives memory from the buffer place. Then, the packet in the WBi place waits for receiving the buffer. An inhibitor arc is necessary from the WBi place to the Ai transition to control the number of input packets. The number of initial tokens in the buffer place indicates the total number of buffer space. If there is a token in the buffer place, the GBi transition is fired, a token is put in the IBi place to process the node, and a token is put in the PM1 place to calculate incentives or penalties. If the input packet is a route request packet, the Te transition is fired. Otherwise, the rec-ch transition is fired to process the choke packet. If the Te transition is fired, it means that the packet is the output packet for the current node. The packet generated by the Ai transition could be deleted in the network. Thus, the received packet from the Te transition was sent to the RBo place for making decisions about sending or deleting the packet. If the rec-ch transition is fired, a token is put in the CH place for receiving the choke packet.

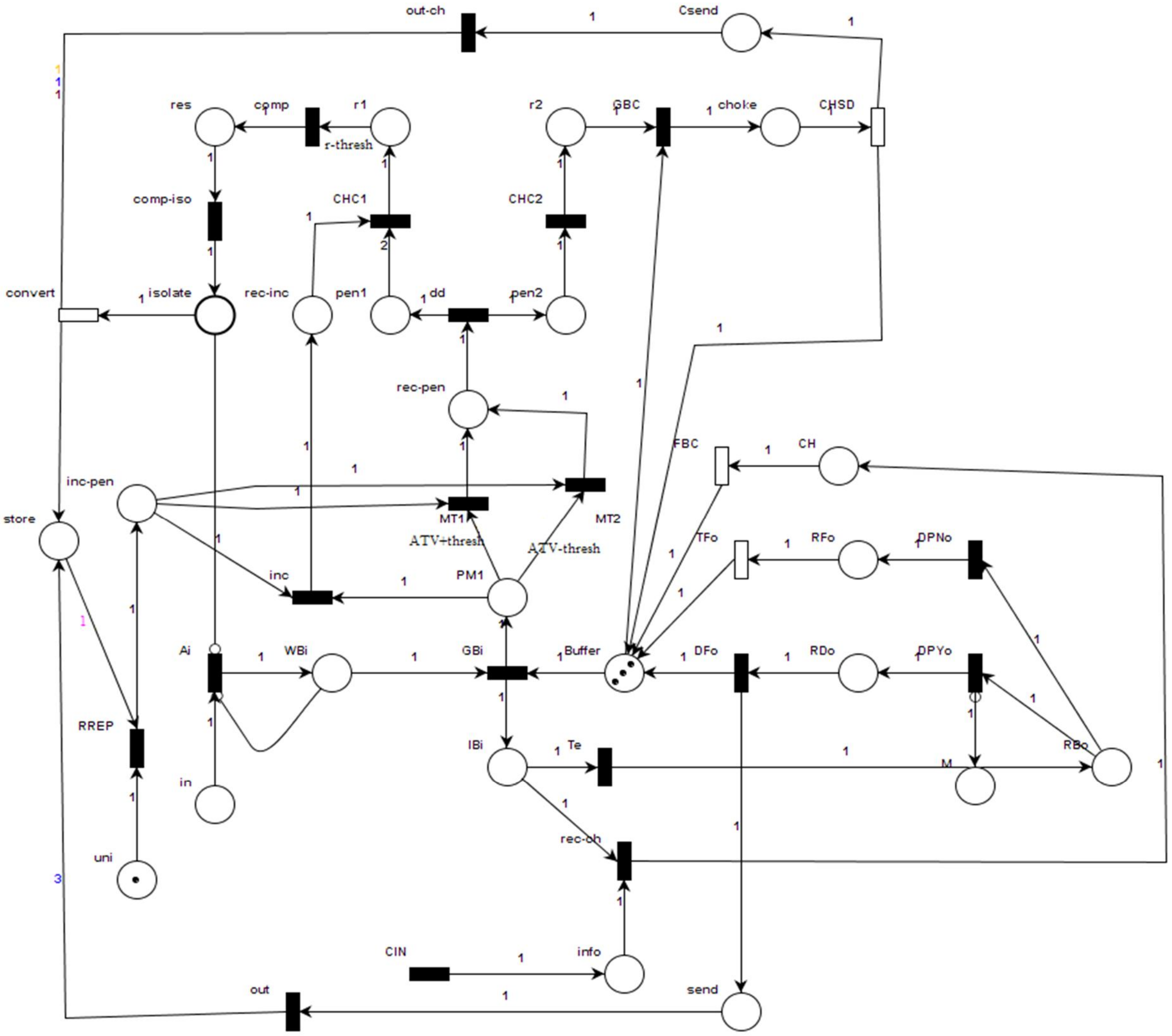


Figure 5. Intermediate node

After ending the choke packet life, the FBC transition is fired and the allocated buffer space is released. The node is congested when the number of receive the RREP packets is outside the node tolerance limit. Otherwise, it will receive incentive. If the node is congested, one of the MT1 and MT2 transitions will happen. Otherwise, one token is placed in the rec-pen place as a penalty and the node is penalized for selfish behavior (no packet is sent to the neighbor node). If none of the MT1 and MT2 transitions are fired, the node will receive incentive.

When a token is placed in the pen2 place as penalty, the CHC2 transition is fired. The presence of a token in the r2 place causes the choke packet to receive the buffer and the choke packet is generated. The CHC1 transition is used to calculate the reduction amount of r parameter (r parameter is the number of packets that a node can receive). For this reason, if the node is not congested, the inc transition is fired and receives incentive. Reduction and multiplicative factors of r parameter are respectively penalties and incentives. For two penalties and one incentive, one token is placed in the r1 place. The comp transition is fired when the number of tokens in the r1 place is equal or more than (r- thresh). In this case, r parameter falls below the thresh parameter. When a token is placed in the isolate place, it does not allow the fire to the Ai transition and the node cannot receive packet until the convert transition is fired.

If there is one token in the RBo place, in the first packet, M place is empty. When the DPYo transition is fired, it puts a token in the RDo place and gets ready to send packet. If the DFo transition is fired, the allocated buffer space is released and a token is placed in the send place. Then, the out transition is fired and the same number of the neighbor nodes makes copy and sends to the store place. If the M place is not empty, the packet is a duplicate packet; so, to delete the packet, the DPNo transition is fired. When a token is placed in the RFo place, the packet gets ready to delete. Firing the TFo transition causes the allocated buffer to get free and the packet to be deleted. When the CHSD transition is fired, one token is put in the Csend place and the choke packet gets ready to send. Then, the out-ch transition is fired and the same number of the neighbor nodes makes copy and sends to the store place.

3.2.2. Source and Destination Node's Pattern

In the source and destination nodes according to Figure 6, the Ao transition is fired as a producer packet and a token is put in the WBo place as a packet. Inhibitor arc is necessary for controlling the number of input packets to the node. With fire the GBo transition, the produced packet receives a buffer and a token is put in the IBo place. Token waits in the IBo place until being put to the RBo place by firing the WTo transition. In this place, there are two cases: first, to send a packet to the neighbor nodes by firing the DPYo transition, the packet gets ready to transfer. In the first

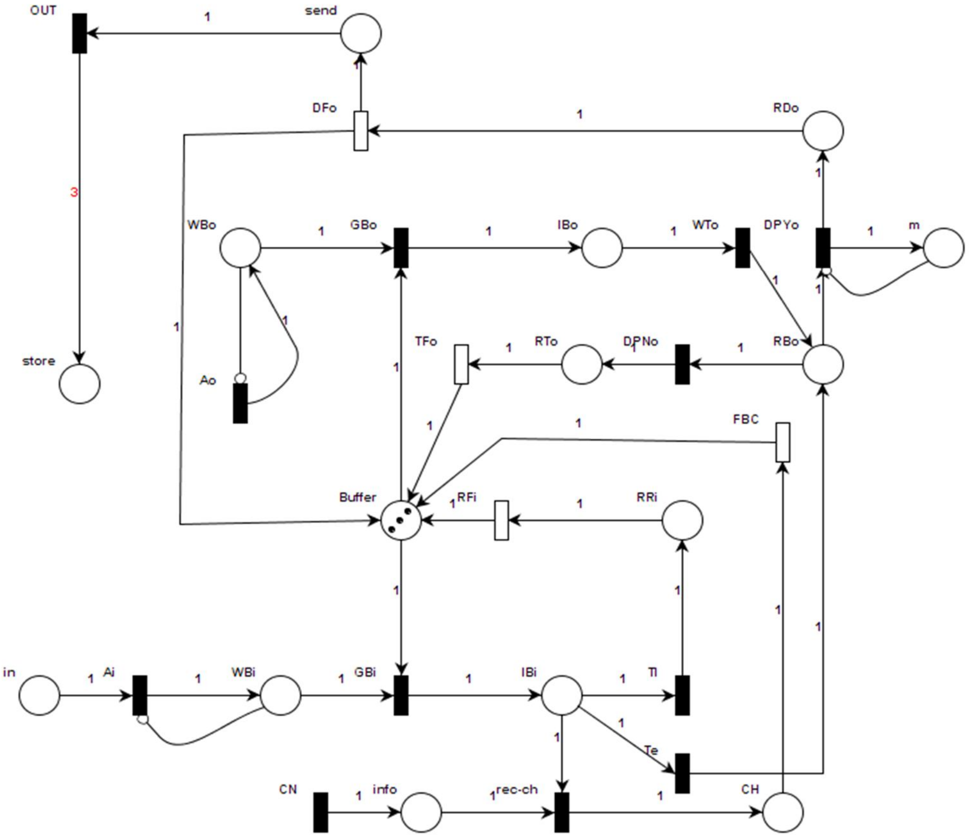


Figure 6. Source and destination node's pattern

time, the packet sends these transition fires. The DFo transition shows start of sending the packet and releasing the buffer. When the OUT transition is fired, the same number of neighbor nodes is put token in the store place. Second, when the DPNo transition is fired, the node gets ready to delete the input packet. The TFo transition shows completion of deleting the packet and releasing the buffer space.

The input packet is entered to current node, when the Ai transition is fired and with inhibitor arc is controlled the number of the input packets. After receiving the buffer and firing the GBi transition, the node will have three cases: first: if the packet should be transmitted to the neighbor node, the Te transition is fired immediately. Second: if the node is the destination node, the Tl transition is fired and a token is put in the RRi place as a received packet. The RFi transition shows completion of the receive packet and releases the allocated buffer space. Third: the input packet is the choke packet; so, the rec-ch transition is fired and a token is put in the CH place. After ending life of the choke packet, the FBC transition is fired and specified space buffer is released to the choke packet. Priority of the transitions is shown in Table 2.

Table 2: Firing priority in intermediate, source and destination nodes

Transitions	Probabilities
rec-ch	3
Te	2
Tl	1
DPNo	1
DPYo	2
MT1	2
MT2	2
MT2	2

4. EVALUATION OF RESULTS

In this section, the designed model is evaluated and compared with the simulation model.

4.1 Evaluation Methods

PIPE tool was used for evaluating the presented model. For validation and comparing the result with the analytical model, MATLAB software was used for simulation.

4.2. Evaluation Criteria

In the following part, the criteria of reliability, availability, and mean time for security failure are introduced.

- Reliability: Reliability in terms of packet delivery rate is a critical factor in the MANETs that evaluates performance of a routing protocol. Packet delivery rate is ratio of number of packets arrived in the destination node to total sent packets from the source node to the destination node [1], [10].
- Availability: To calculate availability, the number of available routes is divided by total number of possible routes [2], [5].
- Security failure: During the following conditions, security failure occurs in the MANETs: 1- if the nodes pretend to congest, 2- more than 1/3 nodes are compromised. In this paper, among the security failure parameters, mean time to security failure (MTTSF) was calculated which showed life time of the network before its arriving at condition of security failure. The high the MTTSF, the later the network's losing integrity or availability.

To calculate the MTTSF in the SPN model, reward allocation method was used so that the reward of 1 was given to all states, except states which will lead to security failure (condition 1 or 2). In each time of receiving reward, a time unit was added to the total time of the network's life time [3].

4.3. The Results of Evaluated

The result of 20 times of simulation by MATLAB software with different topologies was also presented. The nodes were dynamic during the routing. Also, the result of analytical model was presented by PIPE tool with the same topology of simulation environment.

Figure 7 shows rate of packet delivery at the TAODV protocol. On average, packet delivery rate in the simulation was 57% and, based on the proposed analytical model, it was 55%. Usually the simulation result is considered a result; closeness of the result of analytical model to that of simulation model shows that the presented model is accurate.

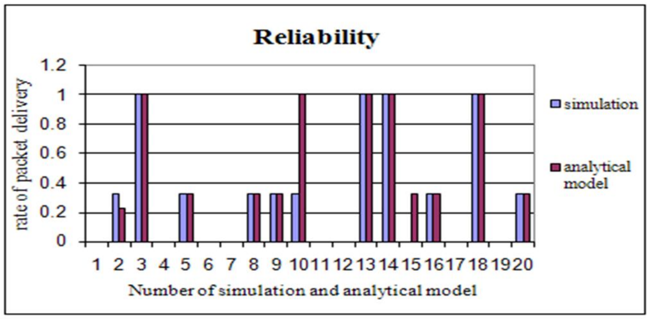


Figure 7. Rate of packet delivery at the TAODV protocol

Availability of simulation and analytical model is shown in Figure 8. The average availability of simulation was 62% and the result of analytical model was 64%.

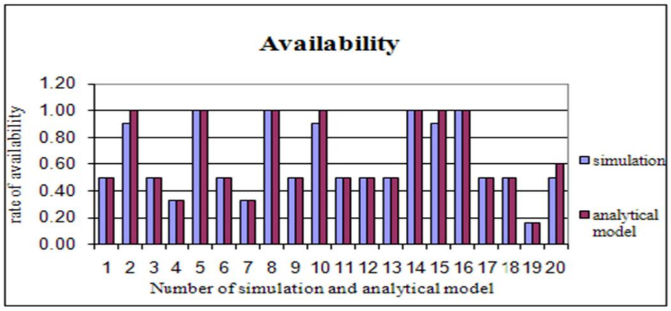


Figure 8. Rate of availability at the TAODV protocol

Figure 9 shows MTTSF in TAODV protocol. In parts that the value was zero, there was not any security failure. Topology of dynamic node showed that analytical model and simulation had different values. In general, in topologies in which there was security failure, the average MTTSF of simulation was 11.6 sec and the average of analytical model was 18.62 sec.

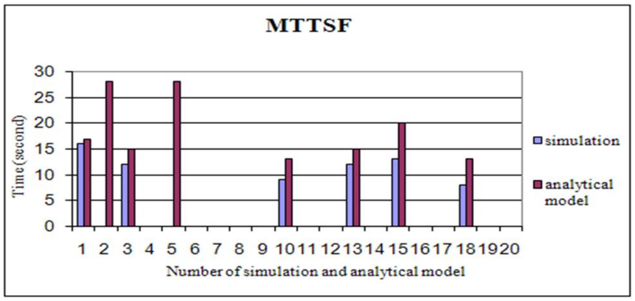


Figure 9. MTTSF in TAODV protocol

5. CONCLUSIONS

In this paper, an analytical model was presented using SPN for TAODV routing protocol. This paper provided a method for analyzing the system properties. This model also presented a theatrical solution while the simulation model presented only details of the system. The obtained results showed that the results of analytical model were close to simulation; so, the proposed analytical model could be a useful alternative for the simulation.

Some properties can be achieved by changing or slightly modifying the model. In this model, all of the time delays were approximated by exponential distributions, which is not always true in a real system. For instance, delays are sometimes constant. As future work, Erlang distributions with a given mean will be applied in the SPN model to approximate the constant distribution, which will increase computational complexity but can improve the presented model with better practicability.

6. REFERENCES

[1] Amandeep, K. G. (2012). Performance Analysis of AODV Routing Protocol in MANETs. *International Journal of Engineering Science and Technology (IJEST).*

[2] Chander K, S. G., Bharat B. (2011). Impact Of Various Factors On Probability Of Reachability In MANETs: A Survey. International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC), 3, 12.

[3] Cho J, C. I. (2010). Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks. Performance Evaluation 68, doi:10.1016/j.peva.2010 .09.005, Published by Elsevier B.V, Journal Homepage: www.elsevier.com/locate/peva

[4] Cho J, S. A., Chen I. (2011). Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. Journal of Network and Computer Applications, doi:10.1016/j.jnca.2011.03 .016, Published by Elsevier Ltd, Journal Homepage: www.elsevier.com/locate/jnca

[5] Gupta S, K. C., Nagpal C.K, Bhushan B (2012). Performance Evaluation of MANET in Realistic Environment I.J.Modern Education and Computer Science, 2012, 7, 57-64, Published Online July 2012 in MECS Avalable: (http://www.mecs-press.org/) , DOI: 10.5815/ijmecs. .

[6] Haas, P. J. (2002). Stochastic Petri Nets: Modelling, Stability, Simulation: Springer-Verlag New York Berlin Heidelberg.

[7] Omar M, C. Y., Bouabdallah A. (2011). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. Journal of Network and Computer Applications, *doi:10.1016/j.jnca.2011 .08.008, Available:* *www.elsevier.com/locate/jnca*.

[8] Prasad P, S. B., and Sahoo A. (2009). *Validation of Routing Protocol for Mobile Ad Hoc Networks using Colored Petri Nets* Department of Computer Science and Engineering National Institute of Technology Rourkela

[9] Sarkar S.K, B. T. G., Puttamadappa C. (2007). *Ad Hoc Mobile Wireless Networks, Principles, Protocols, and Applications*: Taylor & Francis Group, New York & London

[10] Sethi S, U. S. K. (2010). Optimized and Reliable AODV for MANET *International Journal of Computer Applications (0975 – 8887) 3.*

[11] tools, P. from http://pipe2.sourcefroge.net/

[12] Zhang CO, Z. M. (2003). A Stochastic Petri Net Approach to Modeling and Analysis of Ad Hoc Network *NJ, 07102*

BRAIN MACHINE INTERFACE SYSTEM FOR PERSON WITH QUADRIPLEGIA DISEASE

Sameer Taksande
Department of Computer Science
G.H. Raisoni College of Engineering
Nagpur University, Nagpur, Maharashtra
India

D.V. Padole
Department of Electronics
G.H. Raisoni College of Engineering
Nagpur University, Nagpur, Maharashtra
India

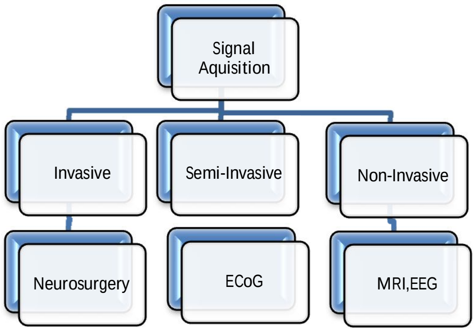
Abstract-- Brain Machine Interface (BMI) system is very helpful technique for the disabled and handicapped person to express their emotion and feeling to someone else with the help of EEG Signals coming out of our brain. As we know that, the human brain is made up of billions of interconnected neurons about the size of a pinhead. As neurons interact with each other, patterns manifest as singular thoughts such as a math calculation. As a by-product, every interaction between neurons creates a miniscule electrical discharge, measurable by EEG (electroencephalogram) machines. This system enables people with severe motor disabilities to send command to electronic devices by help of their brain waves. These signals can be used to control any electronic devices like mouse cursor of the computer, a wheel chair, a robotic arm etc. The research in this area of BCI system (or BMI) uses the sequence of 256 channel EEG data for the analysis of the EEG signals coming out of our brain by using tradition gel based multi sensor system, which is very bulky and not convenient to use in real time application. So this particular work proposes a convenient system to analyze the EEG signals, which uses few dry sensors as compared to the tradition gel based multi sensor system with wireless transmission technique for capturing the brain wave patterns and utilizing them for their application. The goal of this research is to improve quality of life for those with severe disabilities.

Keywords- Brain machine interface, BMI, machine –human interaction, EEG signals, BMI techniques, signal and brain wave simulation process.

I. INTRODUCTION

Brain-Machine Interface (BMI) asks user for brain signals instead of any muscular activities. This system enables people with severe motor disabilities to send command to electronic devices by help of their brain waves [1]. Signals should be identified, processed, and classified to specific command. Feature extraction and classification methods are playing the main role in any BMI systems; since any misclassification and error may cause a wrong command. In the past few years, many research groups focused their work on classifying EEG records to desired mental task classes [3]. Several algorithms have been investigated by purpose of increasing the classification rate and accuracy of evoked potential- based BCIs. Despite the improvements that have been achieved in this area, on-line BCI still poses some challenges. In this paper, we review the performances of different models for classification of BCI-based electroencephalogram signals regarding their real-time applications [4].

SIGNAL ACQUISITION METHOD



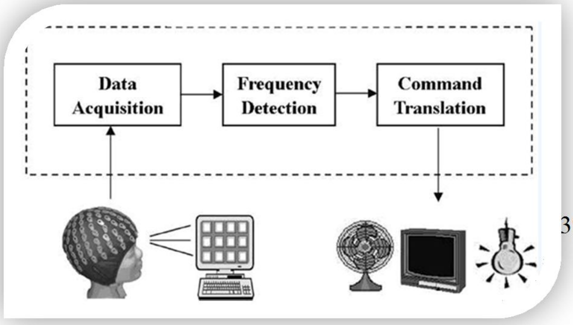
Classification of Brain Waves

Brain waves are recordings of fluctuating electrical changes in the brain. To obtain such a recording, electrodes are positioned on the surface of a surgically exposed brain (an electrocardiogram, ECoG) or on the outer surface of the head (an electroencephalogram, EEG). These electrodes detect electrical changes in the extracellular fluid of the brain in response to changes in potential among large groups of neurons. The resulting signals from the electrodes are amplified and recorded. Brain waves originate from the cerebral cortex, but also reflect activities in other parts of the brain that influence the cortex, such as the reticular formation. Because the intensity of electrical charges is directly related to the degree of neuronal activity, brain waves vary markedly in amplitude and frequency between sleep and wakefulness.

2. SYSTEM OVERVIEW

A. ARCHITECTURE

Brain-Machine interface (BMI) is a fast-growing emergent



technology, in which researchers aim to build a direct channel between the human brain and the computer. This system enables people with severe motor disabilities to send command to electronic devices by help of their brain waves. The first question arises in our mind is that what are brain waves?

Figure 2.1: **Block diagram of Proposed Architecture**

So, the brain waves are nothing but the electrical discharge generated by the interaction of neurons. As we know that the human head is made up of billions of interconnected neurons. As neurons interact, patterns manifest as singular thoughts such as watching movie. Every interaction between neurons creates a miniscule electrical discharge, measurable by EEG. These charges are impossible to measure from outside the skull. But in a dominant mental state, driven by hundreds of thousands concurrent discharges, can be measured.

B. INTRODUCTION TO EEG SIGNAL CLASSIFICATION

These brain waves are classified into four different categories according to the different mental states and frequency range.

Alpha Wave	7-13Hz
Beta Wave	13-40Hz
Theta Wave	4-7Hz
Delta Wave	0-4Hz

1. Alpha Wave

The alpha state is where meditation and relaxation begins. This is where we start to encounter the wealth of effortless creativity flowing just beneath our conscious state. In this state we are awake but deeply relaxed. Studies have shown the alpha state has been associated with "peak performance." It has been found that Elite athletes produce alpha brainwaves prior to concentrated performance (shooting a free throw, hitting an important golf shot), whereas the amateur athletes produce more of the anxious beta brainwaves. In the alpha state we learn, process, memorize and recollect large sums of information fast and with peak effectiveness. Highly creative people have been shown to have "bursts" of alpha brainwaves when they have good ideas. Alpha brainwaves are thought to make the brain "act young" again. In the alpha state fears, habits and phobias begin to melt away. Alpha brainwaves bring an effortless sense of comfort, peace and harmony. Thus Alpha brain waves can be claimed as best for "super learning". The alpha state is thus the first layer of our subconscious mind which can also be called as a gateway to deeper states of awareness.

2.Beta Wave

The beta brainwave is the predominant frequency when we are fully awake and alert. Beta brainwaves make up much of our conscious mind. The Active awareness is thus directed to the outer world. Beta brainwaves are present during stress, paranoia, worry, fear and anxiety. They are also present during hunger, depression, irritability and moodiness. Also, Insomnia is the result of producing excessive beta brainwaves. It can also be associated with excessive mental chatter and self-destructive impulses. But one has to take into account the fact that too much time in the beta state weakens the immune system. Beta Brain wave frequencies lie in the range of 13 to 40 Hz.

3.Theta Wave

Theta brainwaves become prominent when we go deeper into meditation and relaxation which can also be called as a state of trance. Here, brain activity decelerates to the threshold of the sleep stage. It can be described as a state where the indescribable and wonderful realms we can explore. The theta state produces flashes of creative visualization through vivid imagery. In this state we feel much more open and connected to other people. People often report a feeling of floating while producing theta brainwaves. Theta brainwaves are thought to bring out a person's dormant extrasensory perception (ESP) skills. The theta state amplifies the problem-solving skills. A person equipped with dominant theta brainwaves are correlated with insight and intuition. Theta brainwaves bring forth the inspired thought and increased motivation. Sometimes long-forgotten memories come to the surface, which can be credited to theta waves. Children have strong theta brainwaves, which helps to explain their superior ability to learn. Theta is briefly experienced as we climb out of the depths of delta upon waking, or when falling asleep. The theta state can be said to lie in the deeper sub-conscious to super-conscious part of the mind.

4.Delta Wave

Delta brainwave is the deepest level of meditation. The delta state is associated with "no thinking" during deep, dreamless sleep. Delta brainwaves are very rewarding. Delta is said to be the entrance to non-physical states of reality. This is considered as a crucial state which is necessary for renewal, healing and rejuvenation.

The immune system is believed to strengthen in the delta state. The delta state is the unconscious/super-conscious part of our mind. Many scientists believe this state to be the most beneficial.

C. EEG SIGNAL CLASSIFICATION AND ARTIFACTS

Recorded brain electrical waveforms are associated with electrical potentials which are not originated in brain. The sources of these electrical potentials are eye blinking, eye movement, activity of heart and muscles in general. They also can be from EEG equipment's or recording systems. These interference waveforms known as artifacts can often cause serious misclassifications. Hence, developing a practical real-time system to recognize and eliminate artifacts is essential.

3. CLASSIFICATION AND FEATURE EXTRACTION METHODS

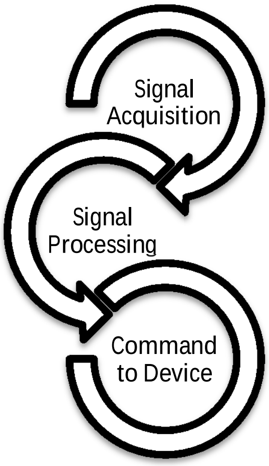


Fig3.1**: Process in the signal processing**

Classification algorithm can directly affect the BMI behavior. Therefore, any improvements have a significant impact on the real-time brain computer interface systems. In order to obtain excellent classification result, effective methods of feature extraction is necessary. To make decision about the classification method, it is essential to know what the features are, what is their application and in which way they may help classification. Feature extraction can be burden for BCI systems and make the classification process complicated and computationally costly. There are cases that some features are redundant or not enough discriminate to available data. Therefore, feature reduction helps for better result as classifier learn a robust solution and achieve a better performance. They have been introduced some classification models for EEG signals with capability of robust and accurate classification of raw EEG signal without feature extraction in prior step.

A. Underlying Neural Processes

All BCIs have to operate on observable effects of brain activity. EEG, MEG and ECoG can only detect large-scale neural dynamics. For example, 50.000 neurons firing in near-synchrony.

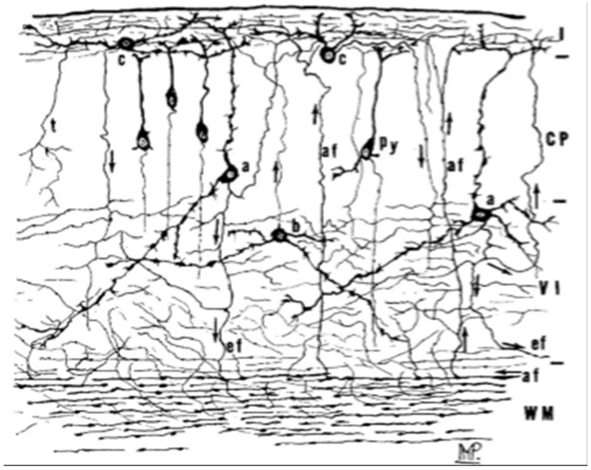


Figure 3.2: **Neuron Firing Process**

B. Signal Detectability

Root cause might not be directly observable (e.g., dopaminergic system, deep brain structures, and few neurons). Widely scattered neural populations are unlikely to exhibit synchrony (unless connected by fiber tracts). Spatially compact populations are more likely to have coordinated timing. Electromagnetic fields can cancel each other out (e.g., in the Amygdala).

i. Invasive Method

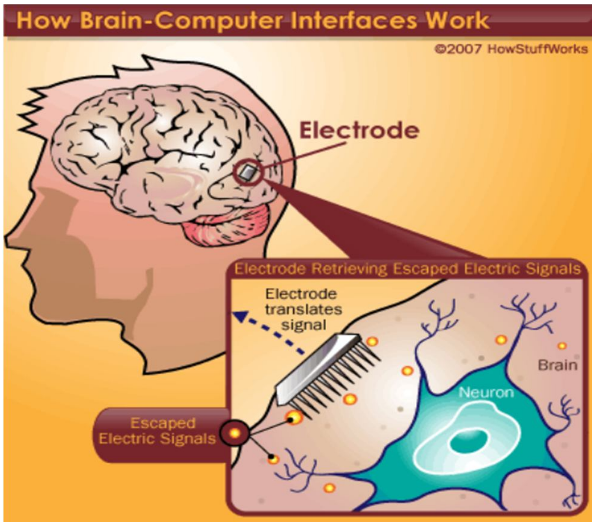

How Brain-Computer Interfaces Work
©2007 HowStuffWorks
Electrode
Electrode Retrieving Escaped Electric Signals
Electrode translates signal
Brain
Neuron
Escaped Electric Signals

Figure 3.3: **Invasive method**

Invasive BCIs are implanted directly into the grey matter of the brain during neurosurgery. In invasive method obtained highest quality of signals.

ii. Semi-Invasive Method

Figure 3.4: **Semi-Invasive method**

SEMI-INVASIVE BCI devices are implanted inside the skull but rest outside the brain rather than amidst the grey matter. They produce better resolution signals than non-invasive BCIs where the bone tissue of the cranium deflects and deforms signals and have a lower risk of forming scar-tissue in the brain than fully-invasive BCIs.

iii. Non-Invasive Method

Figure 3.5: **Non-Invasive method**

Non-invasive implants produce poor signal resolution because the skull dampens signals, dispersing and blurring the electromagnetic waves created by the neurons.

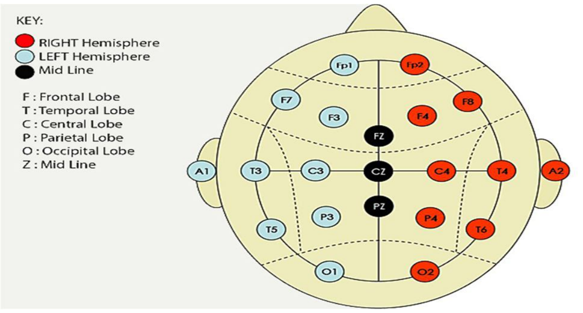


Figure 3.6: **Position of sensor on the basis of international standard 10-20 based system**

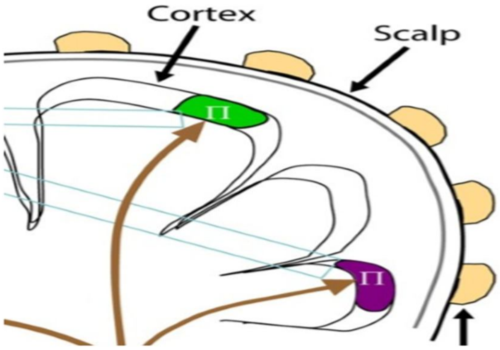
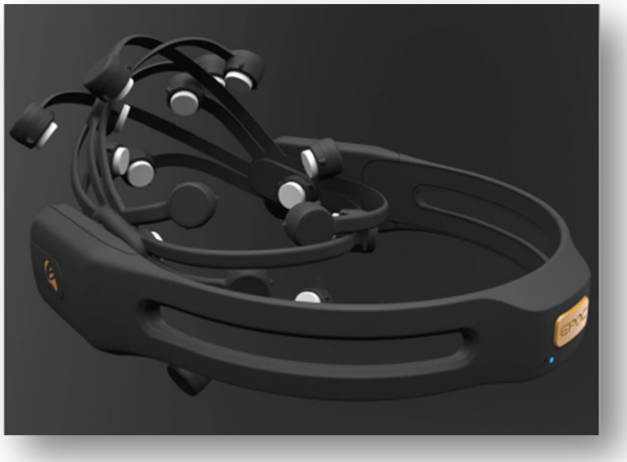


Figure 3.7: **Signal Detectability on Scalp**

We are working with Wireless Non Invasive technique of the data acquisition. For this purpose we are using EMOTIV EEG NEURO HEADSET which shown below in picture.

Figure 3.8: **Emotiv EEG Neuro Headset**



The Emotiv EEG Neuroheadset a 14 channel (plus CMS/DRL references, P3/P4 locations) high resolution, neuro-signal acquisition and processing wireless neuroheadset. Channel names based on the International 10-20 locations are: AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4.

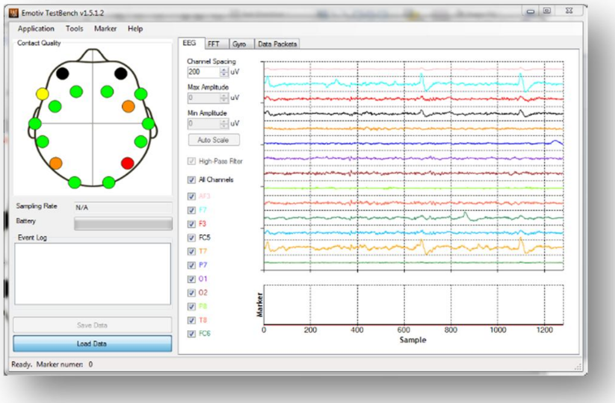
Fig3.9**: Practicing With Machinery**

4. WORKING PROCEDURE SYSTEM

The first step of my project is to capture the different EEG signals by the use of EMOTIV EEG NEUROHEADSET, and transmit these signals wirelessly to the system or laptop. A dongle is attached to the system which receives digital signal from headset and display these signals into the EMOTIV TestBench Software. After this we will have to analyze the raw EEG signals captured by the headset into the Test Bench software with respect to the different facial activity like eye blink, lip moment, teeth clench, smile, left/right wink etc. After detecting these activity on the waveform I'll have to use these signals to send different commands to the system.

The system looks like the picture shown below.
The snapshot of Test Bench software is shown below.

Fig 4.1: **Use of Test Bench Software**



Channel Spacing 200 uV
Max Amplitude 0 uV
Min Amplitude 0 uV
Sampling Rate N/A
Battery
Ready. Marker numer: 0

II. APPLICATION DEVELOPED

Brain Machine Interface (BMI) system is very helpful technique for the disabled and handicapped person to express their emotion and feeling to someone else. This particular system can allow the person with motor disability to control any particular hardware, or mouse pointer on the computer screen.

1. Acolyte (A Friendly Interface for PwD)

This application is design for the entertainment of paralyzed or handicapped person which cannot operate computer with their hands. So, with the help of this application the person can control the mouse pointer by his head movement and can click with the help of blinking of eyes.

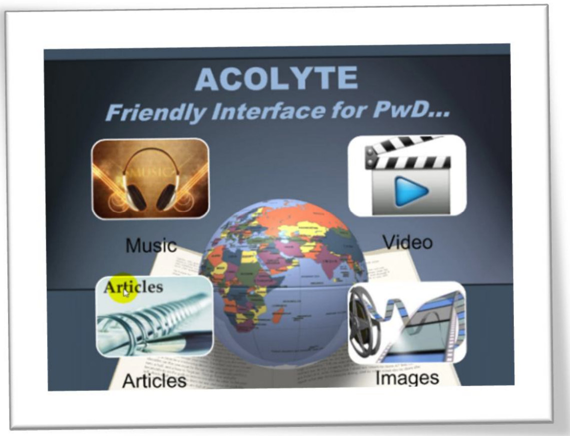


Fig 5.1:**Interface for Physically Handicapped**

2.Brain Controlled Wheel Chair

This chair is designed for to help the person who is crippled or Quadriplegic (i.e.; who is not able to move hands & legs). Who cannot control the electronic wheel chair by their hands, so by using this application he can control the motion of wheel chair by his facial expression only.

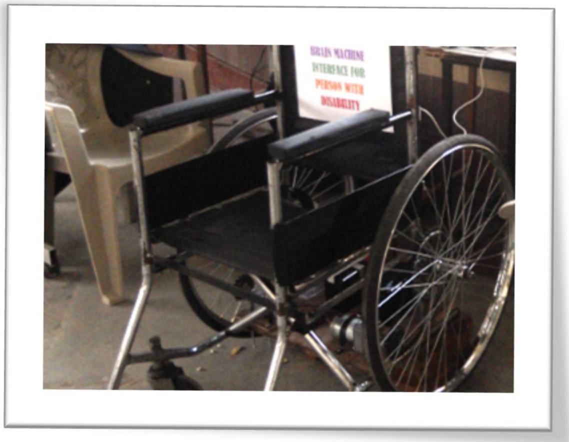


Fig 5.2: **Brain Wave Controlled Wheel Chair**

5. CONCLUSION

This project aims at developing BMI System using EEG based on same specific sensor which is controlled by uniform way, and it does depend on and analog signal. The study and implement EEG on NeuroSky Method based on non-invasive method has been done. The study and implement how to Detect Brain Wave signal on the CRO/DSO/Logic Analyzer is done. And also development of BMI on the above system based on EEG

Signal will get done in future. This helps in efficient use of Emotiv EEG Neuroheadset Module for developing any application based on real time system.

6. REFERENCES

[1] Ebrahimi, T., Vesin, J.M., Garcia, G. "Brain-Computer Interfaces in Multimedia Communication," IEEE Signal Processing Magazine, Vol. 20 14-24, 2003.

[2] J. J. Vidal, "Toward Direct Brain–Computer Communication," Annual Review of Biophysics and Bioengineering, vol. 2, pp. 157–180, June 1973.

[3] "EEG Signal Classification for Real-Time Brain-Computer Interface Applications: A Review" A. Khorshidtalab, M.J.E. Salami, 2011 4th International Conference on Mechatronics (ICOM), 17-19 May 2011, Kuala Lumpur, Malaysia.

[4] Brain Wave Signal (EEG) of NeuroSky, Inc. December 15, 2009.

[5] "A user-friendly SSVEP-based brain–computer interface using a time-domain classifier" An Luo and Thomas J Sullivan, JOURNAL OF NEURAL ENGINEERING, J. Neural Eng. 7 (2010) 026010 (10pp)

[6] "Real-Time EEG Analysis with Subject-Specific Spatial Patterns for a Brain–Computer Interface (BCI)" C. Guger, H. Ramoser, and G. Pfurtscheller, IEEE TRANSACTIONS ON REHABILITATION ENGINEERING, VOL. 8, NO. 4, DECEMBER 2000

[7] "Study on EEG-Based Mouse System by Using Brain- Computer Interface" Dong Ming, Yuhuan Zhu, Hongzhi Qi, Baikun Wan Department of Biomedical Engineering, VECIMS 2009 - International Conference on Virtual Environments, Human-Computer Interfaces and Measurements Systems Hong Kong, China May 11-13, 2009

[8] http://www.neurosky.com/aboutus/brainwavetechnology.aspx

[9]http://eocinstitute.org/meditation/brainwave_charts_brainwave_patterns/

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 345 - 348, 2014, ISSN: 2319–8656

Data Retrieval from the Discrete Media Available on Web and its Diversified Employment Perspectives

Kulvinder Singh
Department of Computer Science and Engineering,
University Institute of Engineering and Technology,
Kurukshetra University,
Kurukshetra, India

Sanjeev Dhawan
Department of Computer Science and Engineering,
University Institute of Engineering and Technology,
Kurukshetra University,
Kurukshetra, India

Pratibha
Department of Computer Science and Engineering,
University Institute of Engineering and Technology,
Kurukshetra University,
Kurukshetra, India

Abstract: Internet has provided its users with an efficient enough and quality-driven source of information in form of the interconnected web of documents. Apart from that it also facilitates its users with some of its really interesting and interactive features served in the package of all these prevailing commercial and social networking websites like facebook, Twitter, flipcart, amazon.com etc. In that particular concern of availability of information and processing it to derive some more interesting results this paper has been written to present the review of some already performed and worth mentioning contributions made by the experts in the field of information on web.

Keywords: Information Retrieval; Query Processing System; Corpora; Focused Crawling; Precision; Recall; PageRank

1. INTRODUCTION

Information we retrieve comes from a huge source of it that we call the World Wide Web. To make this retrieval to acquire its most accurate and relevant version becomes the responsibility of the programs performing it known as Web Crawlers. Their designs equip them to do all the required tasks related to information retrieval, whether it is the link crawling strategy (Breadth First or Depth First approach) or their inside algorithm which teaches them to schedule the resultant links or pages as per their prioritized and calculated ranks. This retrieved information could be mined further and utilized in any possible ways. The way we get that information can possibly suggest how proficient the crawler was while it got the required information through the links. Such information can help to improve the crawling strategies over time. It can also be implemented for creating the relationship graphs on the web. We can also get to know about the interests of people and can help them direct to their desired products and services which would enhance the interface quality as per the user's perspective. The paper is organized in 3 sections, a general introduction of the concerned topic has been given in the current section, the next section provides the brief review of the previously done related work in the respective field, third section presents the analysis and derived conclusions and the future research perspectives are provided in the last section of this paper.

2. RELATED WORK

Gupta *et al.* [1] worked upon the information retrieval system for local databases by searching the web both syntactically and semantically. They created both kinds of information retrieval systems and then compared them based upon Precision and Recall. Different databases were created for each of them, out of those comparisons it was inferred that semantic web was found to be more futuristic. Based upon the results they created an ontology-based focused Information Retrieval (IR) system for learning styles of autistic people. Such ontology can be designed for other disabilities as well. They suggested that using a larger warehouse and implementing search engine combined with properties of various Information Retrieval (IR) systems could draw some better results. As a succession to this data retrieval approach Wan *et al.* [2] worked upon-"URL Assignment Algorithm of Crawler in Distributed System Based on Hash". They described the function of every module and established some rules which parallel crawlers must follow to maintain the equilibrium of load and robustness of system when they perform the simultaneous search on the web. They further designed and implemented a new URL assignment algorithm based on hash for partitioning the domain to crawl and discuss the complete decentralization of every task. They presented an improved Hash method used by the distributed crawler system to assign URL and decentralize the different tasks of crawlers to guarantee the load balancing of the system. As a future concern of research work they stressed upon the detailed study of the scalability of the system and the behavior of its components. A further refinement has been made by Lim *et al.* [3] in the concerned arena by designing a commercial search engine based Query Processing System (QPS) which is capable of answering 5 million user queries against over 6.5 million web pages per day. For making it really fast, they employed more than one server to work in parallel even to solve a single query. They used to implement such server clusters by connecting them via high-speed LANs. Regarding memory requirements for such fast and efficient QPS, they used hierarchical 4-level cache; in its topmost level they stored the recent search result pages and more query results in its lower levels. Such QPS with its multi-level cache could save 70% of server cost for query processing. In the allied concern of fetching a prioritized list of search results, Rafiq *et al.* [4] had designed a new URL ordering algorithm which overcame the flaws of conventional PageRank algorithm. They worked upon some of the determining factors about the performance of web crawlers and then created their algorithm.

For producing an efficient site ordering, they designed a formula for computing the site score:

Final Rank = 0.223(Public popularity score using server logs) + 0.2387(Site updating frequency) + 0.35(Content similarity).

Castillo *et al.* [5] had made a further progression to the ranking task. While working on a sample web (Chilean web) they used the breadth first search approach to traverse all the relevant links and from that information they managed to perform the ranking job. Along with this they also had a serious focus on parallelism encountered while making multiple page requests simultaneously in the same session. Major concerns of their work involved (i) The time interval (w) between successive connections to same website, initially they put w=60 seconds but then reduced it to 15, (ii) The keep-alive header in HTTP/1-1 so as to download k (no. of pages downloaded per session) ≥ 1 which indeed required w ≤ 15, and (iii) The number of simultaneous requests (r) which depends completely upon the availability of relevant website. They worked upon discovering the algorithms for long-term and short-term scheduling and found that for long-term scheduling, a strategy named "length" that focuses upon the longevity of any website was decided to be efficient enough. They also discovered a few issues: a.) Page detection based on higher page ranks creates inefficiencies with the advancement in the search because some new websites and pages might keep on getting discovered and disturb the previously accomplished rankings. b.) Waiting time for retrieving websites gets amortized if we keep k>>1 for page retrieval. The presence of duplicate and near duplicate web documents on the web creates additional overhead for the search engines that critically affects their performance. In that arena Narayana *et al.* [6] presented their work in the paper "A Novel and Efficient Approach for Near Duplicate Page Detection in Web Crawling". Their proposed method used to first extract the keywords from the crawled pages and then compute the similarity scores between the pages. Documents that had a similarity score greater than some defined threshold were considered as near duplicates and rejected. This in-turn reduced the memory requirements for repositories and improved search engine quality. In the similar concern Sharma *et al.* [7] discovered some important issues regarding the lack of topic relevancy in the information retrieved in response to the quoted keywords. They paid the major concern of their work to the information retrieval evaluation measures-Precision and Recall. They also proposed the formulae to calculate these parameters. They figured it out how to model the user's efforts using gain function and discount function of their formulation called Discount Cumulative Gain (DCG). They introduced some future research arenas like predicting the ways to determine if the retrieved pages are the result of exhaustive search from the web and how to uniformly sample web pages on a website if it does not have complete list of web pages. They also stated the need to design more effective and precised algorithms that could detect the duplicity of documents available on web. A furthermore research in the field of detecting and analyzing irrelevancy in information retrieval has been made by Moshchuk *et al.* [8] who accomplished it through large-scale, longitudinal study of the web. They worked upon both the drive-by download malicious executables and the scripted page content that is capable of disrupting the end user's system by playing with his browser settings. They conducted such a crawl in May 2005, involving 18 million URLs, and from that they discovered that spyware was embedded in 13.4% of the 21,200 executables they identified. Additionally they discovered scripted "drive-by download" attacks in some other 5.9% of the web content processed by them. They also studied the frequency pattern of this spyware detection. They conducted the same experiment later in October 2005 and detected a substantial reduction in the drive-by download attacks. They made their initial studies by actually sniffing into the Internet connection at the University of Washington. It was a three step analysis i.) determining the presence of some executable software in the content extracted from web, ii.) downloading, installing and executing that software within a virtual machine and iii.) analyzing the post installation spyware infections made by that software. The prime aspect of retrieving information from a web of documents is to retrieve the most valuable web information by utilizing the least system resources and filter the useless information to the maximum extent. To achieve that Gao *et al*. [9] designed a special crawler for Internet forums. Different from General Crawler and Focused Crawler, it could get structured information directly. This crawler adopted template based processing method which is actually made to use regular expressions to extract structured information. Their forum crawler also proved to be suitable for news and blog sites. It can be applied in the field of public-opinion monitor, news collection, and search of special information such as house rent or recruitment information. However, the configuration of template files is somehow the most complicated part; hence they suggested improving it as a future perspective. Proceeding in the identical research domain, Zhai *et al*. [10] presented their work in the paper "Structured Data Extraction from the Web Based on Partial Tree Alignment" in which they proposed about the problem of structured data extraction from arbitrary web pages. They gave a novel and effective technique called Data Extraction based on Partial Tree Alignment (DEPTA) via which they performed the automatic web data extraction. It was a two step technique: i) identifying individual records in a page and ii) aligning and extracting data items from the identified records. Experimental results proved the worth of this technique. The web source which provides the relevant and most reliable information becomes prior to be visited the most, working in that direction Forsati *et al.* [11] extended the traditional association rule problem by allowing a weight to be associated with each item in a transaction so as to reflect the interest/intensity of each item. They assigned a significant weight to each page based on the time spent and visiting frequency of user for that page, taking into account the degree of interest instead of binary weighting. They presented a new personalized recommendation method based on the proposed weighted association-mining technique. The experimental results showed that the Weight Association Rule (WAR) based model could significantly improve the recommendation effectiveness.

In continuation to the above recapitulation, information extraction and its usage in concern with Social Media is an equally significant and related domain of research. In that particular context, Nemeslaki *et al.* [12] explained the process of mapping business relationships using social media information. They made a study over the business ecosystems in Hungary by examining 5000 out of 15000 facebook users who publically displayed their employers. Then they depicted the complexity of connections graphically through a simulator. Also they transformed the overall graphical network into a relationship graph of employers. The more individuals it showed related to each other in the network between firms, the stronger the relationships became. While making advancement to the same context Neunerdt *et al.* [13] presented their work in the paper "Focused Crawling for

Building Web Comment Corpora". They proposed two algorithms for collecting and processing web comments in context of social blogging. The first approach proposed by them was a combination of a link-based and a content-based focusing algorithm. A relevance classifier was also combined with the link-based Online Page Importance Computation (OPIC) scoring algorithm. They compared OPIC combined with comment detection (OPIC + COMMD) and usual comment detection (COMMD) focused algorithm to the standard breadth-first search (BFIRST) crawling approach. These algorithms allowed for type-specific focused crawling to build web comment corpora. For future endeavors they proposed topic-specificity in the web comment corpus, topic classification in the relevance scoring of web pages, ontology-based corpus generation tool for further refinement and the need for a more improved and sophisticated web comment detection approach. Working on the similar perspective Agarwal [14] proposed his remarkable research work on "Prediction of Trends in Online Social Networks". He used the "directed links of following" in the social media of Twitter to determine the flow of information. This strategy indicates a user's influence on others that could decide if the topic is trendy or viral in the social network. His automated system takes raw tweets, processes them using NLP to filter out noise (spams or chats) and extract informative tweets and then mine them further to predict the trending topics in their early stages. An aggregate score for each tweet is calculated by that system. But since Twitter is really spontaneous and dynamic therefore extracting the complete Twitter graph and thence resolve all the relations for the users is impossible. So, as the future perspective he proposed to work on some more effective data structures and algorithms to deal with the dynamic Twitter graphs. To make it more reasonable Nooralahzadeh *et al.* [15] presented their work in the paper entitled "2012 Presidential Elections on Twitter - An Analysis of How the US and French Election were Reflected in Tweets". In their analysis they studied the sentiments that prevailed before and after the presidential elections, held in both US and France in the year 2012. To achieve it, they retrieved the content information from the social medium-Twitter and used the tweets from electoral candidates and the voters, collected by means of crawling during the course of election. In order to gain useful insights about the US elections, they scored the sentiments for each tweet using different metrics and performed a time series sentiment analysis for candidates and different topics retrieved as per the quoted keywords by the formula:

Number of Positive Tweets - Number of Negative Tweets/Total Number of Tweets

In addition to this, they compared some of their insights obtained from the US election with their observations from the French election. They made these observations to understand the inherent nature of elections and to bring out the influence of social media on elections.

3. CONCLUSIONS

In this paper we presented the review of the work done in the domain of information extraction, mining and processing it, in order to derive some meaningful results. It summarized the explorations made by some very proficient researchers in the respective field. The paper encloses the explorations made about the relevant arenas of information, ranging from usual information retrieval to focused crawling, derivations about information retrieval from usual commercial websites to social blogging sites, from ontology-based Information Retrieval (IR) to spyware detection embedded in scripted documents. We also presented the work done about more efficient and improved ranking algorithms, more promising Query Processing Systems (QPS), duplicity detection methods, data mining and processing from social blogging sites as well. The valuable findings, flaws and future endeavors about every referred paper are well presented in this paper.

4. SCOPE FOR FURTHER RESEARCH

For the future perspectives, we would work on the real-time data retrieval from the social networking websites like Twitter and perform the analysis of that data to derive the results regarding the trending and viral issues. We would work upon extracting and observing the social graphs of relationships on such SNSs to understand the plotting criteria and then employ those results for plotting the results obtained from the analysis of the data retrieved.

5. REFERENCES

[1] Dr. Deepak Garg and Sanchika Gupta, "A Frequent Pattern Based Approach to Information Retrieval", 2011.

[2] Yuan Wan and Hengqing Tong, "URL Assignment Algorithm of Crawler in Distributed System Based on Hash", Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference, April 2008, pp 1632-1635, 2008.

[3] Sungchae Lim and Joonsen Ahn, "A Hierarchical Cache Scheme for the Large-scale Web Search Engine", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp 1643-1647, 2011.

[4] Sandhya and M. Q. Rafiq, "Performance Evaluation of Web Crawler", International Journal of Computer Applications® (IJCA)/International Conference on Emerging Technology Trends (ICETT), pp 43-46, 2011.

[5] Carlos Castillo, Mauricio Marin, Andrea Rodriguez and Ricardo Baeza- Yates, "Scheduling Algorithms for Web Crawling", 2010.

[6] V.A. Narayana, P. Premchand and Dr. A. Govardhan, "A Novel and Efficient Approach For Near Duplicate Page Detection in Web Crawling", 2009 IEEE International Advance Computing Conference (IACC 2009), Patiala, India, pp 1492-1496, 2009.

[7] Dr. Deepak Garg and Deepika Sharma, "Information Retrieval on the Web and its Evaluation", International Journal of Computer Applications (0975-8887), pp 26-31 Issue 3/Volume 40, 2012.

[8] Alexander Moshchuk, Tanya Bragin, Steven D. Gribble and Henry M. Levy, "A Crawler-based Study of Spyware on the Web", Department of Computer Science & Engineering, University of Washington, pp 9-13, {anm, tbragin, gribble, levy}@cs.washington.edu.

[9] Qing Gao, Bo Xiao, Zhiqing Lin, Xiyao Chen and Bing Zhou, "A HIGH-PRECISION FORUM CRAWLER BASED ON VERTICAL CRAWLING", Proceedings of IC-NIDC, pp 362-367, 2009.

[10] Yanhong Zhai and Bing Liu, "Structured Data Extraction from the Web Based on Partial Tree Alignment", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, pp 1614-1628, VOLUME 18/NO. 12, 2006.

[11] R. Forsati, M. R. Meybodi and A. Ghari Neiat, "Web Page Personalization Based on Weighted Association Rules", International Conference on Electronic Computer Technology, pp 1317-1321, 2009.

[12] Nameslaki, Andràs; Pocsarovszky and Kàroly, “Web crawler research methodology”, 22nd European Regional Conference of the International Telecommunications Society (ITS2011), 2011. Available at http://hdl.handle.net/10419/52173 .

[13] Melanie Neunerdt, Markus Niermann, Rudolf Mathar and Bianka Trevisan, RWTH Aachen University, “Focused Crawling for Building Web Comment Corpora”, The 10th Annual IEEE CCNC- Work-in-Progress, pp 761-765, 2013.

[14] Pranay Agarwal, Department of Computer Science and Engineering, IIT Delhi, Thesis on “Prediction of Trends in Online Social Network”, 2013.

[15] Farhad Nooralahzadeh, Viswanathan Arunachalam and Costin Chiru, “2012 Presidential Elections on Twitter - An Analysis of How the US and French Election were Reflected in Tweets”, 2013 19th International Conference on Control Systems and Computer Science, pp 240-246, 2013.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 349 - 352, 2014, ISSN: 2319–8656

Proposing an Appropriate Pattern for Car Detection by Using Intelligent Algorithms

Amin Ashir
The member of young researchers club, Islamic Azad University of
Dezful, Iran

Sedigheh Navaezadeh
Sama Technical and Vocational Training College,
Islamic Azad University,
Mahshahr, Branch
Mahshahr, Iran

Abolfazl jafari
Sama Technical and Vocational Training College,
Islamic Azad University,
Mahshahr, Branch
Mahshahr, Iran

Abstract: Nowadays, the automotive industry has attracted the attention of consumers, and product quality is considered as an essential element in current competitive markets. Security and comfort are the main criteria and parameters of selecting a car. Therefore, standard dataset of CAR involving six features and characteristics and 1728 instances have been used. In this paper, it has been tried to select a car with the best characteristics by using intelligent algorithms (Random Forest, J48, SVM, NaiveBayse) and combining these algorithms with aggregated classifiers such as Bagging and AdaBoostMI. In this study, speed and accuracy of intelligent algorithms in identifying the best car have been taken into account.

Keywords: intelligent algorithms, pattern recognition, Random Forest, J48, SVM, Naïve Bayse, AdaBoostMI

1. INTRODUCTION

Nowadays, the automotive industry has been considered by consumers, and the product quality has been recognized as an essential element in the current competitive markets. Nowadays, in business process, consumer has a crucial role in improving and developing the product, and is considered as a base for receiving reliable information. Security and comfort are important criteria and parameters in selecting a car. The framework of this paper is on the basis of quality management. Also, in this study, those indicators that have considered the consumer have been taken into account. Therefore, standard database of CED [1] has been used. In this database, there are various criteria such as security and comfort. In the rest of this paper, the criteria of car identification, investigation of intelligent algorithms, layout and the results of simulation have been respectively analyzed.

2. CRITERIA OF IDENTIFYING THE CAR IN TERMS OF SECURITY AND COMFORT

The criteria that have been used to identify the cars are as follows:

Car prices;

Maintenance cost;

The number of car doors;

The car capacity (the number of passengers);

The required space for furniture;

Security of the car.

3. AGGREGATED CLASSIFIERS AND METHODS

Generally, searching is carried out in the imaginary space in supervised learning algorithms so that an appropriate prediction can be considered to find a solution. An aggregated classifier is a supervised learning algorithm combining various theories so that a better theory is presented. As a result, an aggregated classifier is considered as a technique combining weak learners so that a strong learner is created. Fast algorithms such as decision trees are considered along with aggregated classifiers. Observations show that when diversity of models is great, aggregated classifiers perform efficiently. Therefore, different methods have been proposed to increase the diversity among combined models. The most well-known methods are Bagging and Boosting [2]. In Bagging method, the classifiers designed in various versions of data are combined, and majority voting is individually considered among classification decisions. Since re-sampling of Bootstrap is usually used to locate initial data due to imbalanced data, this method is called Bootstrap Aggregation or Bagging. One of the classifiers usi9ng Bagging and AdaBoostMI methods is Random Forest involving several decision trees, and its output is obtained through individual output trees. This algorithm combines the Bagging method by random selection of features so that a set of decision trees with controlled diversity are created. One of the advantages is high accuracy of the classifier. Also, it can perform well with many outputs [3]. The second wee-known method is Boosting that trains new samples and instances to reinforce learning samples and instances, and it makes some changes in aggregated classifier. This method has sometimes higher precision and accuracy in comparison to Bagging method. One of its disadvantages is maximum learning and training of these learning samples and instances. AdaBoostMI is one of the well-known Boosting methods.

4. SVM CLASSIFIER

This algorithm is a supervised learning method for classification and regression. This method is relatively a new method. In recent years, it has better efficiency that older method in terms of classification such as perceptron neural networks. The framework of SVM classifier is on the basis of linear classification of data. In learner classification of data, it has been tried to select a line that has more reliability margin. A solution can be found for optimization line of data through QP methods that are well-known methods in solving limited problems. Before dividing a line, data should be transferred to a space with higher dimensions so that machine can classify very complex data [4, 5].

This algorithm has theoretical foundations. It just requires a dozen of samples, and is not sensitive to the number of problem dimensions. In addition, efficient methods of SVM learning have been considerably developed. In learning process involving two classes, the aim of SVM is to find the best function for classification so that the members of two classes can be determined and distinguished in dataset. The criteria of the best classification are determined geometrically. This is true for data set analyzed linearly. The boundary defined as a part of space or separation of two classes can be defined by hyperplane. This geometric definition allows us to detect that how the boundaries are maximized, even if there are numerous hyperplanes, and only a few of them are considered as a solution of SVM. SVM persists on the largest boundary for hyperplane since it provides generalization of algorithm as well as possible. This issue helps to classification efficiency and accuracy in tested data. Also, it provides a space for better classification of future data. One of the problems of SVM is that it requires complex computations. However, this problem has been acceptably solved. One solution is that a large optimization problem can be divided into smaller problems. Each problem involves a pair precisely selected from variables. These variables can be used in problems. This process continues until all analyzed sections are solved.

5. CLASSIFIER OF NAIVE BAYES

Naive Bayes presents a predictive model in terms of output probability/special results. NB algorithms measure the patterns or the relation between data by counting the number of observations. Then, this algorithm provides a model demonstrating the patterns and their relations. After creating this model, it can be used as a predictive model. This algorithm helps us to present models for classification and prediction of various objectives. Notice the following example:

Which customers are interested in buying a special product.

Which consumers can purchase more than 10000 dollars.

Identifying the customers who do not buy the company products, and buy the products of competitors.

Predicting products that have failed, and predicting their probability.

Naïve Bayes algorithm predicts the above mentioned issues by Bayes theory supposing that data values are independent. This algorithm provides a model as quickly as possible, and it can be considered for classifying two or more than two classes [6].

6. J48 CLASSIFIER

Algorithm Description

J48 is not just an algorithm; rather, it is a set of algorithms. The performance of J48 has been described and demonstrated in figure 1. All methods of tree deduction begin from root node providing all data information, and recursively divides information into smaller sections. In this case, each ratio is tested in each node. Sub-trees show the classification of main information completing tests of determined ratio valuation. This process continues until all sets are purified; that is, all samples are placed in a group, and the growth of tree stops in this time.

The rules of classifiers

J48 introduces a list of rules in the frame of a form. Rules are designed for each class. A sample returns to its secure location by finding the primary rules. If a rule cannot be found for a sample, then it is located in presupposition class. In the rules of J48, time of CPU and required memory are considered.

```
Input: an attribute-valued dataset D
Tree={}
If D is "pure" OR other stopping criteria met then
Terminate
End if
For all attribute aϵ D do
Compute information-theoretic criteria if we split on a
End for
abest = Best attribute according to above computed criteria
Tree = Create a decision node that tests abest in the root
Ds = Induced sub-datasets from D based on abest
For all Dsdo
Treec = J48(Dv)
Attach Treec to the corresponding branch of tree
End for
Return Tree
```

Figure 1: the performance of J48 algorithm

7. LAYOUT

Data used in this paper are a set of data related to car entitled CED [1]. Collected data have six characteristics and 1728 instances. The method of this study is on the basis of pattern recognition, and it has been tried to detect and identify the best car by using intelligent algorithms. It should be mentioned that intelligent algorithms have been executed in Weka software [7].

The used instances are divided into 10 parts. By increasing this division, better results can be obtained, but it is time consuming. In the rest of this paper, the obtained results will be analyzed and studied.

8. SIMULATION RESULTS

After applying intelligent algorithms on the instances, the obtained results have been collected in three tables. Table 1 demonstrates the comparison of intelligent algorithms (Random Forest, J48, SVM, NaiveBayse) in terms of time and accuracy in identifying a secure and comfortable car.

In table 2, these algorithms have been compared with aggregated classifier of Bagging. Also in table 3, these algorithms have been compared with aggregated classifier of AdaBoostMI to identify the best car, and the criteria of time and accuracy have been investigated.

Table 1: comparing intelligent algorithms in terms of time and accuracy in secure and comfortable cars

Accuracy	**Time**	Criteria\ algorithms
%93.75	1.81 Sec	**SVM**
%85.5324	0.02 Sec	**Naive Bayse**
%92.3611	0.06 Sec	**J48**
%96.4606	0.13 Sec	**Random Forest**

As it is observed in table 1, the accuracy of time algorithm and speed of Naïve Bayes algorithm are better than other algorithms.

Table 2: comparing intelligent algorithms with aggregated classifier of Bagging in terms of time and accuracy in identifying cars.

Accuracy	**Time**	Criteria algorithms
%93.3449	13.16 Sec	**SVM**
%85.3009	0.09 Sec	**Naive Bayse**
%93.8079	0.02 Sec	**J48**
%45.5023	0.92 Sec	**Random Forest**

As it is observed in table 2, the accuracy of used algorithms has not been improved by using aggregated classifier of Bagging. In most of these algorithms, accuracy has been reduced after using aggregated classifier of AdaBoostMI.

Table 3: comparing intelligent algorithms with aggregated classifier of AdaBoostMI in terms of time and accuracy in identifying secure and comfortable cars.

Accuracy	**Time**	Criteria algorithms
%94.5023	21.80 Sec	**SVM**
%90.162	0.33 Sec	**Naive Bayse**
%961227	0.45 Sec	**J48**
%93.6921	0.14 Sec	**Random Forest**

As it is observed in table 3, accuracy of used algorithms has been improved by using aggregated classifier of AdaBoostMI.

Accuracy of J48 algorithm is above 96%. Comparing tables 2, 1 and 3 show that, by using aggregated classifier of AdaBoost, accuracy of J48 algorithm is above 96%, and 0.45 seconds has the best accuracy. In addition, in naïve Bayes algorithm without aggregated classifier of bagging and AdaBoostMI, 0.02 seconds is considered as the best time in identifying secure and comfortable cars. In J48 algorithm, 0.02 seconds is considered as the best time.

9. CONCLUSION

In order to identify a secure and comfortable car, considerable results can be obtained by considering standard CEO database and intelligent algorithms such as SVM, Naïve Bayes, J48, Random Forest as well as combining these algorithms with aggregated classifiers of Bagging and AdaBoostMI. In this paper, since evaluating simulation results on the basis of identification time and modeling accuracy and accuracy in identifying secure and comfortable car have great importance, it is better to use J48 algorithm with aggregated classifier of AdaBoostMI involving accuracy of 96.1227 percent and time of 0.45 seconds.

11. REFERENCES

[1] http://archive.ics.uci.edu/ml/datasets/Car+Evaluation, December 2011

[2] DietterichThomas G. "An experimental comparison of three methods for constructing ensembles of decision trees: Bagging, boosting, and randomization", Machine Learning 40(2), 139–158, 2000.

[3] KhoshgoftaarT.M., GolawalaM. Van HulseJ., "An Empirical Study of Learning from Imbalanced Data Using

Random Forest", Proceedings of the 19th.IEEE Conference on Tools with Artificial Intelligence, pp.310-317, 2007.

[4] Vapnik V., "Statistical Learning Theory", John Wiley & Sons, New York, 1998.

[5] Vapnik V., "The Nature of Statistical Learning Theory", Springer-Verlag, New York, 1995.

[6] Jam Sahar, Khashayar, 1390. An approach of smart business, data warehouse and data mining.www.hamsahar.com

[7] http://www.cs.waikato.ac.nz/~ml/weka, November 2011.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 353 - 357, 2014, ISSN: 2319–8656

Propose a Method to Improve Performance in Grid Environment, Using Multi-Criteria Decision Making Techniques

Robabeh Parvaneh
Department of Computer Science and Research Branch
Khorasan Razavi،
Islamic Azad University،
Neyshabur،Iran

Ali Harounabadi
Islamic Azad University
Izeh Branch
Izeh، Iran

Abstract: The most important purpose of grid networks is resource subscription in a dynamic and heterogeneous environment. They are accessible through using various methods. Subscription has mainly computational, scientific and other implications. In order to reach grid purposes and to use available resources in grid environment, subtasks are distributed among resources and are scheduled by considering the quality of service. It has been tried to distribute subtasks between resources in a way that maximum QOS can be obtained. In this study, a method has been presented. In this method, three parameters; namely, sent and transferred time between RMS and resource, process time of subtask by the resource, and the load of available tasks in resources row, have been taken into account. In this way, multi-criteria decision is made by using TOPSIS method and this priority of the resources are determined to assign them to subtasks. Finally, time response, as an efficient parameter, has been improved and optimized by optimal assignment of the resources to subtasks.

Keywords: Grid network, multi-criteria decision making, response time, Petri net, TOPSIS

1. Introduction

Grid networks are composed of a set of heterogeneous computers. They have been non-exclusively connected to each other through connection protocol and grid management system. The main purpose of grid is using common resources such as processor power, band width and tec. Also, its purpose is to make it accessible for central computer. Currently, computing grid networks are widely used in developed countries in order to prevent waste of resources, and to use them optimally. Computing grid has been considered and used in order to prevent heavy expenditure paid to use computing power of network. The most important purpose of grid networks is resource subscription is a dynamic and heterogeneous environment. They are accessible by using various methods. This subscription has mainly computing, scientific and other applications [9]. Computing grid environment is suitable to solve those problems requiring long and complex computations [6]. The main purpose of grid networks is to provide services having high efficiency, reliability and fewer costs for many users. Also, its purpose is to support cooperative tasks. In grid, efficiency is important. In order to increase efficiency in grid, we need an efficient and proper scheduling. Dynamic nature of grid resources and various demands of users have made grid scheduling complex. The purpose of grid scheduling is to assign tasks to resources optimally [2]. In this paper, a method has been presented to decrease response time as an efficient parameter to increase efficiency. By considering multi-criteria decision making and Topsis method, resource priority is determined for subtasks. In this way, Makespan of the system is decreased. Decision making involves stating purposes, evaluating their possibility and the outcomes of executing each solution, selecting and executing them. In multi-criteria decision making method, several criteria can be used to select the better alternative, instead of using one optimality criterion [3]. The proposed method is evaluated and simulated by using CPN TOOLS.

2. Background

2.1 Grid Environment

Grid is “a wide network having high computing power and the ability to connect to Internet”. Grid has not been just composed of special and homogeneous computers. It has been composed of a set of computers distributed in various levels of internet or intranet. They are non-exclusively connected to each other through connection protocol and grid management system. In other words, grid decreases the execution time of those tasks and works lasting for several hours to just some seconds. Grid is a set of resources connected to each other. Also, it involves some applications to do works. Grid has been used in 1990 for the first time to point to computing ultra structure distributed in engineering and advanced sciences. Grid concepts and technologies have been considered and used to provide resource subscription between scientific units, and the aim is to use the resources of grid environment to solve complex and difficult problems [5]. In grid environment, tasks are not individually executed just in one system. Rather, these tasks are divided into subtasks. Each of them are sent to resources that are the member of grid. Available resources are connected to each other in a network by using connection links. The link provides connection information exchange between two computers. Link topology determines connection structure between computers. Various types of link topologies have been considered in grid systems such as star, tree, ring and combinational topologies [4]. In this paper, star topology has been taken into account. In grid, the procedure of this topology is that RMS is placed in the center of system, and all resources are connected to it by connection links [6]. After receiving the task from the user, RMS divides it into some subtasks. Redundancy technique is used in resources allocated to subtasks. Then, RMS assigns each subtask to more than one resource. In this way, each subtask is allocated to two or more resources, but each resource processes only one subtask [4]. Petri networks are appropriate tools for graphical modeling on the basis of mathematic logic. Although Petri net is graphical, its mathematical base is strong. Petri net has been considered as a method for formal modeling to analyze and describe the systems that have distributed simultaneous synchronous, parallel or random characteristics. One of the important characteristics of Petri net is that it is executable. Unlike UML, analysis and implementation is carried out simultaneously in Petri nets. This attribute can be used to evaluate the behavior and efficiency of a system simultaneously [1].

3. Literature review

Azghomi and his colleagues [4] presented their paper entitled modeling of tasks distribution and computing reliability in grid networks having star topology. They considered time and colored Petri nets in investigations and implementation. Tasks scheduling is important in grid networks environment in order to reach to desired quality level. In this study, grid networks are based on resource management system. This system receives tasks from the users and divides them into subtasks. Then, each subtask is transferred and sent to one or more available resources (redundancy technique). After executing subtasks, each set of resources processing the same subtask sends and transfers the results to one location. Among the resources that are randomly selected, the resource that executes the related task as quickly as possible is identified and transferred to another location. Finally, the maximum degree is computed so that total time of the task is obtained. Above mentioned operations are simulated by using time and colored Petri nets, and reliability is computed.

Parsa and his colleagues [10] proposed the scheduling algorithm called RASA. This algorithm is based on two well-known algorithms, namely, Max-min and Min-min scheduling. RASA has the advantages of this algorithm, and it has removed disadvantages of them. RASA alternatively uses these two algorithms on the basis of estimating the end time of doing works. At first, algorithm presents a matrix of end time of t_i on R_j resource. If the number of accessible resources is odd, then Min-min strategy is used; otherwise, Max-min strategy is applied. Other works are alternatively transferred to resources by one of these strategies. One of the advantages of this method is to provide the better load balance compared to these two algorithms. RASA algorithm has better performance in comparison with algorithms in distributed systems.

Kokilavani and his colleagues [7] improved Min-min algorithm. When the number of small tasks and works is lesser that the number of large works and tasks in meta-task, this algorithm does not operate well, and it increases makespan of the system. Also, it does not create any loads in the system. They presented an algorithm called LBBM. This method has been presented in two phases. In the first phase, Min-min algorithm is presented, while in the second phase, works and tasks are scheduled to reuse the resources effectively. Their algorithm has decreased makespan, and has increased the efficiency of the resources.

Meibody and his colleagues [8] presented a scheme for resource scheduling in order to optimize resource scheduling in computing grid. On the basis of demands classification, three levels (home, local, logical) are considered. Each level has its own function to receive and deliver the subtasks to lower or higher layers. In scheduling scheme, three levels have been presented, and resources have been connected to each other by a hierarchical network involving three levels.

Saadi and his colleagues [13] proposed an algorithm for scheduling of independent tasks in computing grid. They presented weighted objective function for this scheduler, and they considered the importance of time and cost of the works done by the users.

Parsa and his colleagues [11] proposed a new category to estimate reliability of service and whet they expect from computing the time of providing service when there are some defects in grid system.

4. proposed Method

The purpose of scheduling in grid environment is to reach to maximum quality of service. Quality has various concepts. The most important parameter of service quality are efficiency, load balance, reliability, cost, time and etc, or a combination of them. In order to optimize and improve response time in presented model, three parameters are considered. These parameters are transferred and sent time between RMS and j resource to execute i subtask, processing time of i subtask by j resource, and available load in the row of each resource. They are placed in decision making matrix. After unscaling, weighting and making decision among them, the priority of resources are separately obtained for each subtask. Assuming that the subtask having smaller data has more priority in selecting the resource (because it has less time to execute it), we allocate the resource to subtasks. The result is that minimum response time is obtained.

4.1 Modeling and Scheduling Subtasks

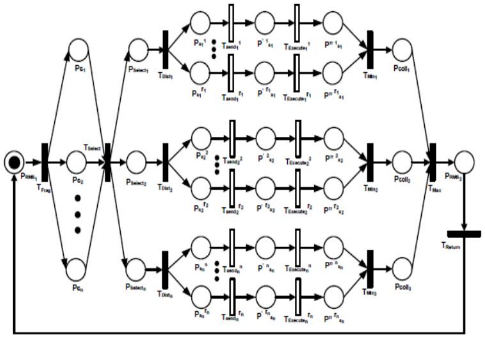


Figure1.Modeling on the basis of Petri nets

According to [4] and Fig1, at first, token is placed in P_{RMS} location. This token, that is considered as a task, is divided into subtasks after passing through frag ($T_{frag)}$ $_{route.}$ Then, tokens (subtasks) are allocated to several resources on the basis of redundancy technique. These subtasks select the optimal resource on the basis of three parameters such as transferred and sent time of data between RMS and resource, processing time of subtask by the resource and load of available works in resource row, and multi-criteria decision making. According to [4], if resources are randomly made accessible for subtasks, then after passing the selection route (T_{select}) and selecting the appropriate resources for subtasks, these resources are sent and transferred to subtasks by passing through distribution route. Then, tokens are placed in P_{si} location.

4.2 Allocating subtasks to resources by using the model of multi-criteria decision making

Decision making model is divided into two groups: multi-objectives model and multi-criteria model.

Multi-objectives models have been used for designing, while multi-criteria model are used to select the better alternative. In this method, multi-criteria models have been used to select the appropriate resource. We have taken into account Topsis method among the methods of multi-criteria models. According to [3], unscaling should be considered in order to compare different measurement scales and measures. In this way, the elements of indexes (n_{ij}) are measured without any dimension. In some cases such as MCDM, especially MADM, we should know the relation importance of available indexes (objectives). The sum of them equals one (they are normalized). The relation importance of priority of each index (objective) is measured against other for making decision. In this study, we considered entropy technique to weigh the indexes, and selected Topsis method to select the suitable resource. In this method, we considered the distance of A_i from the ideal point. Its distance from negative ideal points has been also taken into account. It means that the selected alternative should have minimum distance from the ideal solution, and it should have maximum distance from negative ideal solution. We used this method to prioritize the resources in each subtask. After converting decision making matrix to an unscaled matrix and providing an unscaled matrix, we determine ideal solution as well as negative-ideal solution.

Afterwards, we compute the distance. Distance of ith alternative from ideals can be obtained by Euclidean method.

for Ideal option (A^+) and negative ideal (A^-) defined:

Ideal Option =
$$A^+ = \{(\max V_{ij} | j \in J) \; And \; (min \; V_{ij} | j \in \acute{J} | i = 1,2, \ldots m)\} = \{V_1{}^+ \;, V_2{}^+ \;, \ldots\ldots, V_j{}^+ \;, \ldots\ldots, V_n{}^+\}$$

Negative Ideal Option =
$$A^- = \{(\min V_{ij} | j \in J) \; And \; (max \;\; V_{ij} \,|\, j \in \acute{J} \,|\, i = 1,2, \ldots m)\}$$

$$=\{V_1{}^- \;, V_2{}^- \;, \ldots\ldots, V_j{}^- \;, \ldots\ldots, V_n{}^-\}$$

Then calculate the size of separation (distance), the choice between the i-th to the ideal use of Euclidean method:

$$\text{the i} - \text{th to the ideal}, d_{i+} = \{\textstyle\sum_{j=1}^{n}(V_{ij} - V^+ j)^2\}^{0/5} \quad ; \quad i = 1,2, \ldots \ldots m$$

$$\text{the i} - \text{th to the negetive ideal}, d_{i-} =$$

$$\{\textstyle\sum_{j=1}^{n}(V_{ij} - V^-{}_j)^2\}^{0/5}; \;\; i = 1,2, \ldots \ldots m$$

Finally, we compute the closeness of A_i to an ideal solution.

$$cl_{i+} = \frac{d_{i-}}{(d_{i+} + d_{i-})} \; ; \; 0 \leq cl_{i+} \leq 1; i = 1,2, \ldots \ldots m$$

Eventually, we can rank the alternatives in the supposed problem.

5. Case Study

In this section, the results of two proposed methods are simulated and analyzed. At first, these methods are modeled by colored Petri nets; then, they are simulated ny CPN TOOLS. The results of these simulations are compared with [1] and [4]. Suppose that, in grid environment, the task entered by RMS is divided into two tasks having complex computing characteristics and required data volume. Also, suppose that although there are four resources having some characteristics such as processing speed, band width and lack of any failure in processing (P), it is possible that there is lack of failure in connection lines during transferring (q). In this method, redundancy technique is followed. This means that subtasks should be fewer than accessible resources. Therefore, after allocating the task to subtasks, each subtask is allocated to one resource, but each resource only processes one subtask. In order to improve the response time, we considered three parameters such as transferring time of data between RMS and R_j resource to execute S_i subtask (T_{ij}), processing time of S_i subtask by R_j resource (T_{ij}), and execution time in the row of each resource (q). They are computed by following equations [4].

$$\tau_{ij} = \frac{a_i}{b_{wj}}$$

$$T_{ij} = \frac{c_i}{P_{sj}}$$

A balance is provided between three parameters by using multi-criteria decision making and TOPSIS, and they are weighted. After placing them in decision making matrix, we obtain resource priority for S1 and S2. Since subtask of S2 has fewer data, selection priority is allocated to it. In this way, R2 and R3 are selected for S1 and R1, and R1 and R4 are selected for S2; hence, the selected scenario has the minimum response time (6/4). This time is the best one. As it was already mentioned, according to [4], firstly resources are randomly selected. Secondly, available load in resources is not considered. Thirdly, it does not result in a scenario with optimized response time. It has been tried by [1] to improve reliability. A method for improving response time has not been presented. It should be mentioned that, in the proposed method, reliability is high. Through using the method proposed by [4], there are different scenarios to allocate subtasks and resources. Since they are selected randomly, different modes can be observed. In this method, we analyze six scenarios.

The first scenario: in this scenario, subtask of S1 selects R_2 and R_4 resources, and subtask of S2 selects R_1 and R_3 resources.

The second scenario: subtask of S1 selects R_1 and R_4 resources, and subtask of S2 selects R_2 and R_3 resources.

The third scenario: subtask of S1 selects R_1 and R_3 resources, and subtask of S2 selects R_2 and R_4 resources.

The fourth scenario: subtask of S1 selects R_3 and R_4 resources, and subtask of S2 selects R_1 and R_2 resources.

The fifth scenario: subtask of S1 selects R_1 and R_2 resources, and subtask of S2 selects R_3 and R_4 resources.

The sixth scenario: subtask of S1 selects R_2 and R_3 resources, and subtask of S2 selects R_1 and R_4 resources.

Comparison diagram of response time in the above mentioned scenarios in the proposed and previous method has been shown in figure 2.

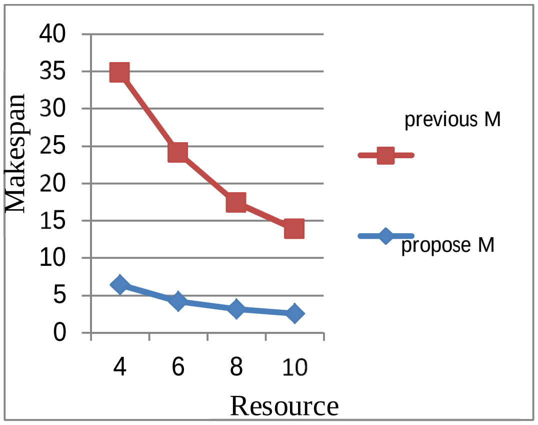


Figure 2. Comparison diagram

After determining parameters subtasks, we have simulated CPN TOOLS software. The result of this simulation has been demonstrated in figure 3,4.

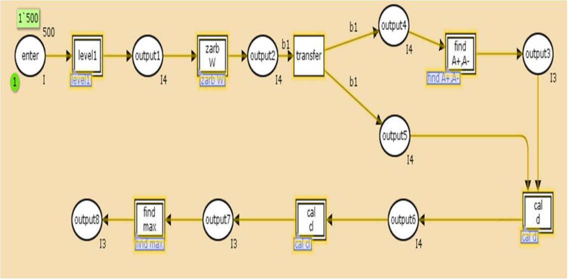
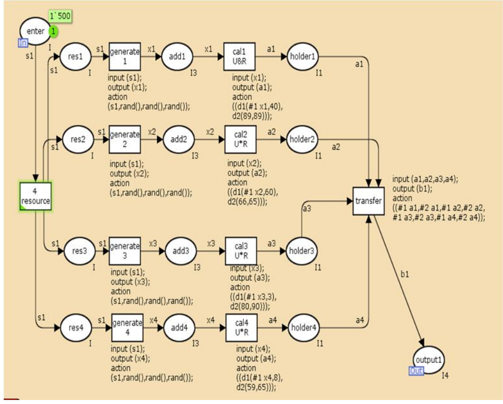


Figure 3. System simulation



```
input (s1);
output (x1);
action
(s1,rand(),rand(),rand());

input (x1);
output (a1);
action
((d1(#1 x1,40),
d2(89,89)));

input (s1);
output (x2);
action
(s1,rand(),rand(),rand());

input (x2);
output (a2);
action
((d1(#1 x2,60),
d2(66,65)));

input (a1,a2,a3,a4);
output (b1);
action
((#1 a1,#2 a1,#1 a2,#2 a2,
#1 a3,#2 a3,#1 a4,#2 a4));

input (s1);
output (x3);
action
(s1,rand(),rand(),rand());

input (x3);
output (a3);
action
((d1(#1 x3,3),
d2(80,90)));

input (s1);
output (x4);
action
(s1,rand(),rand(),rand());

input (x4);
output (a4);
action
((d1(#1 x4,8),
d2(59,65)));
```

Figure 4. Subsystem simulation of allocating resources to subtask

6. CONCLUSION

In grid, various types of computers having different abilities and operating systems can be found. Open environments such as grid have independent and heterogeneous computing nodes, and their accessibility changes over time. There are some problems due to this dynamic environment. In this study, we proposed a method by preventing the random allocation of resources, considering above mentioned parameters and using multi-criteria decision making for prioritization. In this method, we improved response time to increase the efficiency considerably. Since colored Petri nets have a strong mathematical basis to evaluate software systems, we used CPN TOOLS simulator to simulate the proposed method, and we compared our method with the method proposed by [1] and [4]. The results indicate that the priority of this method in comparison to other presented methods. The results show that this method has minimum response time compared to the methods that have been already presented.

7. SUGGESTIONS

In this Paper, the following Suggestions have been Proposed:

Considering data dependency among subtasks and expecting some sub-tasks to receive required data from sub-tasks. Also due to BandWidth and etc.

8. REFERENCES

[1] Alishahi M, Abroshan V, Harounabadi A, 1391, Modeling and optimal resource selection for the subtasks aimed at improving reliability of grid network using colored Petri Nets, The second Conference on Soft Computing and Information Technology.

[2]Arora. M, Biswas. R, Das. S, Aug .2002, “A Decentralized Scheduling and Load Balancing Algorithm for Heterogeneous Grid Environments”, Proceeding of International Conference on parallel processing workshops, pp. 499-505.

[3] Asgharpour MJ,1389, Multi Criteria Decision Making, Tehran University Press.

[4]Azghomi.M.A, Entezari-maleki. R, October 2010, ”Task scheduling modeling and reliability evalution of grid services using colored petri net ”, Future Generation Computer Systems, Vol .26, pp 1141-1150.

[5] Dastgheybifar G, Ansari S, Lotfi S, 1386, “ A new Scheduling Algorithm for Computational Grid, Thirteenth Annual Conference of Computer Society of Iran”.

[6] Fathi M, Shahriari F, 1388, Concepts of grid computing technology and its applications in various Fields.

[7] Kokilavani. T, George Amalarethinam. D.I, April 2011, “Load Balance Min-Min Algorithm for Static Meta-Task Scheduling in Grid Computing”, International Jornal of Computer Applications, Vol.20- No.2, pp.43-49.

[8] Meibodi. M, Shojafar. M, Barzegar. S, 2010, “A New Method on Recourse Scheduling in Grid Systems Based on Hierarchical Stochastic Petri Net”, 3th International Conference on Computer and Engineering,pp.175-180.

[9] Mohammad Khanli Leyli ،Etminan Far Maryam ، Ghaffari Ali. 2010 ، Reliable Job Scheduler using RFOH in Grid Computing ، Journal of Emerging Trends in Computing and Information Sciences ،©2009-2010 CIS Journal. All rights reserved. VOL. 1.

[10] Parsa. S, Entezari-maleki. R, Dec.2009,”RASA: A New Task Scheduling Algorithm in Grid Environment”, International Journal of Digital Content Technology and its Applications Vol.3,9.4,pp. 152-160.

[11] Parsa. S, Azadi Parand. F, 2012,” Estimation of service reliability and performance in grid environment”, Journal of King Saud University – Engineering Sciences 24, 151–157.

[12] Rongfei. Zeng, Yixin. Jiang, Chuang. Lin, and Xuemin (Sherman) Shen, 2012 ,”Dependability Analysis of Control Center Networks in Smart Grid using Stochastic Petri Nets” , Electrical and Computer Engineering Sept. (vol. 23 no. 9) pp. 1721-1730.

[13] Saadi H, Habibi G,Mohammadi H,1386, "design of a scheduler for grid computing using genetic algorithms", Thirteenth National Conference of Iranian Society, Kish Island, Iran.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 358 - 360, 2014, ISSN: 2319–8656

Pattern Recognition using Artificial Neural Network

Poonam Dabas
Department of Computer Science and Engineering
University Institute of Engineering and Technology
Kurukshetra University
Kurukshetra, India

Umesh Kumar
Department of Computer Science and Engineering
University Institute of Engineering and Technology
Kurukshetra University
Kurukshetra, India

Abstract: An artificial neural network (ANN) usually called neural network. It can be considered as a resemblance to a paradigm which is inspired by biological nervous system. In network the signals are transmitted by the means of connections links. The links possess an associated way which is multiplied along with the incoming signal. The output signal is obtained by applying activation to the net input NN are one of the most exciting and challenging research areas. As ANN mature into commercial systems, they are likely to be implemented in hardware. Their fault tolerance and reliability are therefore vital to the functioning of the system in which they are embedded. The pattern recognition system is implemented with Back propagation network and Hopfield network to remove the distortion from the input. The Hopfield network has high fault tolerance which supports this system to get the accurate output.

Keywords: Pattern Recognition; Hopfield network; Back Propagation Network; Training Set

1. INTRODUCTION

The Neural Network (NN) is nonlinear information processing systems that are designed from interconnected elementary processing devices known as neurons [1]. A NN could be a massively parallel distributed processor that includes a natural propensity for storing experimental data and creating it obtainable to be used. A Biological NN consists of a gaggle or teams of chemically connected or functionally associated neurons. One nerve cell may be connected to several alternative neurons and also the total range of neurons and connections during a network is also intensive. Connections known as synapses are typically fashioned from axons to dendrites. Natural nerve cells receive signals through synapses placed on the dendrites or membrane of the neuron. In most cases a NN is an adaptive system dynamical its structure throughout a learning part. NN are used for modeling advanced relationships between inputs and outputs or to seek out patterns in knowledge [2].

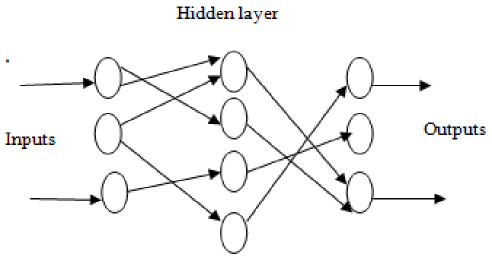


Figure 1 Basic network structure [3]

1.1 Artificial neural networks

The main characteristics of neural networks are that they need the power to find out advanced nonlinear input-output relationships, use successive coaching procedures, and adapt themselves to the information [2]. As ANN mature into industrial systems they're probably to be enforced in hardware. Their fault tolerance and reliability are so very important to the functioning of the system during which they're embedded [3]. This new approach to computing conjointly provides an additional graceful degradation throughout system overload than its additional ancient counterparts. ANN is an informatics system. During this information system the elements known as neurons process the data [1]. Artificial nerve cell is characterised by

- Architecture (connection between neurons)
- Training or learning (determining weights on the connections)
- Activation function

1.2 Pattern recognition

Machine recognition, description, classification, and grouping of patterns are necessary issues during a form of engineering and scientific disciplines like biology, psychology, medicine, marketing, pc vision, artificial intelligence, and remote sensing [2]. A pattern may be a fingerprint image, a written cursive word, a personality's face, or a speech signal. This recognition concept is straightforward and acquainted to everyone within the real world surroundings however in the world of AI, recognizing such objects is a tremendous accomplishment. The practicality of the human brain is wonderful, it's not comparable any artificial machines or software system. [4] The term pattern recognition encompasses a large vary of data process issues of nice sensible significance, from speech recognition and therefore the classification of written characters, to fault detection in machinery and diagnosis. The act of recognition will be divided into 2 broad categories: recognizing concrete things and recognizing abstract things [5]. The look of a pattern recognition system basically involves the subsequent 3 aspects: 1) knowledge acquisition and pre-processing, 2) knowledge illustration, and 3) higher cognitive process. The matter domain dictates the selection of sensor(s), pre-processing technique, illustration theme, and therefore the higher cognitive process model. It is usually in agreement that a well-defined and sufficiently unnatural recognition drawback can cause a compact pattern illustration and a straightforward higher cognitive process strategy.

2. LITERATURE REVIEW

Husam Ahmed Al Hamad [1] investigated and compared the results of 4 completely different artificial neural network models. Identical algorithmic rule was applied for all with applying 2 major techniques, 1st neural-segmentation technique; second apply a replacement fusion equation. The neural techniques calculate the arrogance values for every Prospective Segmentation Points (PSP) using the planned classifiers so as to acknowledge the higher model that increased the general recognition results of the written scripts. The fusion equation appraises every PSP by getting a fused value from 3 neural confidence values. CPU times and accuracies were conjointly reported. Jayanta Kumar Basu *et. al.,* [2] proposed that among the various traditional approaches of pattern recognition the statistical approach has been most intensively studied and used in practice. The design of a recognition system require careful attention to the following issues: definition of pattern classes, sensing environment, pattern representation, feature extraction and selection, cluster analysis, classifier design and learning, selection of training and test samples and performance evaluation. New and emerging applications, such as data mining, web searching, retrieval of multimedia data, face recognition and cursive handwriting recognition, require robust and efficient pattern recognition techniques. The objective of this review paper was to summarize and compare some of the well-known methods used in various stages of a pattern recognition system using ANN. Fajri Kurniawan *et. al.,*,[3]presented a robust algorithm to identify the letter boundaries in images of unconstrained handwritten word. The proposed algorithm was based on vertical contour analysis. The Proposed algorithm was performed to generate pre-segmentation by analysing the vertical contours from right to left. The results showed that the proposed algorithm was capable to locate the letter boundaries accurately for unconstrained handwritten. Lupus Dung *et. al.,* [4] planned that within the supervised coaching the author notice a collection of weights and biases for a pattern recognition neural network so as to classify all patterns in a very coaching knowledge set. But it might be tough if the neural network was not large enough for learning an oversized coaching knowledge set. During this paper the author planned a coaching technique and a style of pattern recognition neural network that wasn't massive however still able to classify all the coaching patterns precisely. The coaching technique facilitate the neural network to search out not only one but several sets of weights and biases for classifying all the coaching patterns, dominant the recognizing rejection and reducing the error rate. Dilruba et. *al.,*, [5] urged that NN is as an efficient tool for pattern recognition. The success rate for recognizing known and unknown pattern was comparatively terribly high with compare to alternative techniques. This paper gift a comparative study of however NN classifies the patterns from coaching knowledge and acknowledges if testing knowledge holds that patterns. For learning from the coaching knowledge many approaches were gift among that the author had selected the back-propagation technique. Back-propagation rule in a very feed-forward network was used for the feature extraction. The author have used 2 approaches and network was trained with such that knowledge. The author supposed to search out the match quantitative relation of coaching Pattern to testing Pattern and therefore the result knowledge set found from the experiment also given within the paper. Zaheer Ahmad et. *al.,* [6] planned that Urdu compound Character Recognition need sturdy techniques to develop as Urdu being a family of Arabic script was cursive right to left in nature and characters modification their shapes and sizes once they were placed at initial, middle or at the tip of a word. The developed system consists of 2 main modules segmentation and classification. Within the segmentation section pixels strength is measured to discover words in a very sentence and joints of characters in a very compound/connected word for segmentation. The most purpose of the system was to check the rule developed for segmentation of compound characters. Kauleshwar Prasad *et. al.,* [7] focused on recognition of English alphabet in an exceedingly given scanned text document with the assistance of Neural Networks. It had varied applications that embrace reading aid for blind, bank cheques and conversion of any hand papers into structural text type. The primary step was image acquisition that non inheritable scanned image followed by noise filtering, smoothing and normalisation of scanned image, rendering image appropriate for segmentation wherever image was rotten into sub pictures. The author use character extraction and edge detection algorithmic program for coaching the neural network to classify and acknowledge the written characters. Binu P. *et. al.,*[8] wear down the popularity of hand written Malayalam character using wave energy feature (WEF) and extreme learning machine. The wave energy (WE) may be a new and sturdy parameter and was derived using wave rework. It might cut back the influence totally different varieties of noise at different levels. We tend to might reflect the WE distribution of characters in many directions at completely different scales. We tend to totally differ decomposition levels that have different powers to discriminate the character pictures. These options represent patterns of written characters for classification. This algorithmic program learned abundant quicker than ancient in style learning algorithms for feed forward neural network words. Dawei Qi *et. al.,* [9] proposed that the edge detection problem in this paper was formulated as an optimization process that sought the edge points to minimize an energy function. An initial edge was first estimated by the method of traditional edge algorithm. The gray value of image pixel was described as the neuron state of Hopfield neural network. The state updated till the energy function touch the minimum value. The final states of neurons were the result image of edge detection. The novel energy function ensured that the network converged and reached a near-optimal solution. Ming-ai Li *et. al.,* [10] planned a way to beat the multiple native minimum drawback of traditional distinction Hopfield neural network. On conditions that the changed Hopfield neural network works in a very parallel mode and its interconnection weight matrix was negative, it's only 1 stable state, and therefore the stable state will build its energy perform reach to its solely minimum. On the premise of the relation between the stability of the changed distinction Hopfield network and its energy function's convergence, the changed Hopfield network was applied to resolve LQ dynamic optimization management issues for time-varying systems. It can be made by building the equivalence between the energy performs of the changed Hopfield network and therefore the performance Index of controlled system. As a result, finding LQ dynamic optimization management drawback was reminiscent of operational associated changed distinction Hopfield network from any initial state to the stable state that represents the specified best management vector. The simulation results agree well with theoretical analysis.

3. PROPOSED MODEL

In the last few years neural network is found as an effective tool for pattern recognition. The Success rate has been examined for recognition pattern as well as unknown ones. It comes out to be comparatively very high. Back-propagation algorithm in a feed-forward network is used for the feature extraction. The Hopfield model of neural network working as an associative memory is chosen for recognition purposes [6]. The back propagation network and Hopfield network are combined together to get the appropriate result as more accurate than either using back propagation network or Hopfield network. The input to this network will be numeric characters, alphabets and special characters which will be recognized using the combination of back propagation network and Hopfield network. The distorted input is fed to the new combined network to get the accurate output. The Hopfield network is present to remove the distortion from the input and to get the exact output as the fault tolerance of Hopfield network is high as compared to Back propagation network.

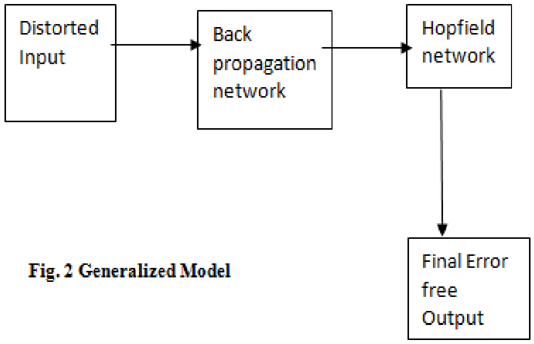


Fig. 2 Generalized Model

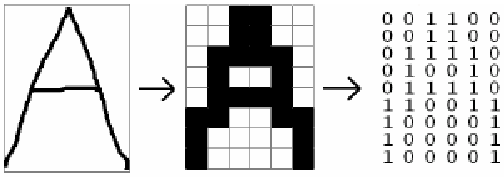

0 0 1 1 0 0
0 0 1 1 0 0
0 1 1 1 1 0
0 1 0 0 1 0
0 1 1 1 1 0
1 1 0 0 1 1
1 0 0 0 0 1
1 0 0 0 0 1
1 0 0 0 0 1

Fig 3 Input Characters

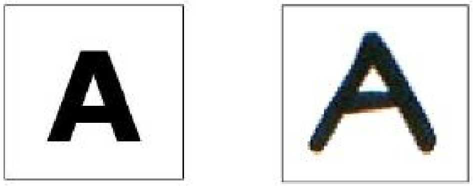


Fig 4 Output Character

4. CONCLUSION

In this present work we have implemented the Combined Network i.e. BPN and HP for pattern recognition of input patterns. In this work we have taken a sample of alphabet patterns to perform the Pattern recognition. As the initial step the image dataset is being maintained to represent different kind of character patterns. These images are trained using HP. The numbers of hidden layers are not fixed and are dependent on the complexity of the input. As fault tolerance of HP is more than BPN so the error calculating capability is more in HP. So the new defined network of HP and BPN is most suitable for recognizing the input pattern as compared to BPN. With distortion the accuracy level of output is more in new defined network as compared to only BPN. The output we get is similar to the trained dataset.

5. REFERENCES

[1] Husam Ahmed Al Hamad "Use an Efficient Neural Network to Improve the Arabic Handwriting Recognition" International Conference on Systems, Control, Signal Processing and Informatics, Page no 269-274, 2013

[2] Jayanta Kumar Basu, Debnath Bhattacharyya and Tai-hoon Kim "Use of Artificial Neural Network in Pattern Recognition" International Journal of Software Engineering and Its Applications Vol. 4, No. 2, April 2010

[3] Fajiri Kurniawan, Mohd. Shafry Mohd. Rahim, Nimatus Sholihiah, Akmal Rakhmadi and Dzulkifli Mohamad "Characters Segmentation of Cursive Handwritten Words based on Contour Analysis and Neural Network Validation" ITB J. ICT, Vol. 5, No. 1, 2011

[4] Le Dung and Mizukawa M. "A Pattern Recognition Neural Network Using Many Sets of Weights and Biases", Computational Intelligence in Robotics and Automation, Page no 285-290,2007..

[5] Dilruiba, R.A., Chowdhury, N.Liza, F.F. and Kiarmakar "Data Pattern Recognition using Neural Network with Back-Propagation Training ", Electrical and Computer Engineering, ICECE, Page no 451-455, 2006

[6] Zaheer Ahmad, Jehanzeb Khan Oraikzai and Inam Shamsher, "Urdu compound Character Recognition using feed forward neural networks,", International Conference on Computer Science and Information Technology, IEEE, pp.457-462, 2009.

[7] Kauleshwar Prasad, Devvrat C. Nigam, Ashmika Lakhotiya and Dheeren Umre "Character Recognition using Matlab's Network Toolbox" International journal service, Science and Technology Vol. 6, No. 1, page 13 February 2013

[8] Binu P, Chacko, Vimal Krishnan and G. Raju "Handwritten character recognition using wavelet energy and extreme learning machine" springer, International Journal of Machine Learning and Cybernetics, Volume 3, Issue 2, Page no. 149-161, June 2012

[9] Dawei Qi, Peng Zhang, Xuejing Jin and Xuefei Zhang "Study on Wood Image Edge Detection Based on Hopfield Neural Network", Proceedings of the International Conference on Information and Automation, IEEE, Page no 1942-1946, 2010

[10] Mingai Li, Jun-fei Qiao and Xiao-gang Ruan "A Modified Difference Hopfield Neural Network and its application" IEEE, Vol 1, Page 199-203, 2005

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 361 - 363, 2014, ISSN: 2319–8656

Effective Parameters of Image Steganography Techniques

Fariba Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University
Masjedsoleyman Branch
Masjedsoleyman, Iran

Abstract: Steganography is a branch of information hiding method to hide secret data in the media such as audio, images, videos, etc. The use of images is very common in the world of electronic communication. In this paper, the parameters that are important in steganography images, have been studied and analyzed. Steganography purposes of security, robustness and capacity of which three are located at three vertices of a triangle, each note entail ignoring others. The main parameters of the methods steganography they've Security, Capacity, Psnr, Mse, Ber, Ssim are the results of the implementation show, steganography methods that these parameters provide have mentioned goals than other methods have improved.

Keywords: Steganography;psnr;mse,ber; Capacity

1. INTRODUCTION

The term Steganography is forked from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [1]. Steganography is the art and science of secret communication, in which the secret message in a cover media such that the hidden message is not detectable [2]. Today, a large part of the communications in electronic form. As the use of digital media coverage can be a good choice to hide the secret information. The media can, text, images, audio and video, etc. (Figure 1).

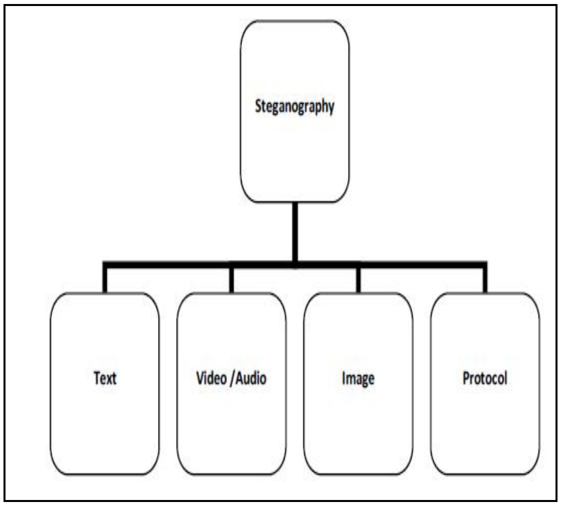


Figure 1: The media used in steganography (3)

It is very common nowadays for transferring images on the Internet. The eye is not very sensitive to the details of the pictures, so little change on steganography in an image is created, it is not tangible. Select an image masking confidential information is very important because it greatly affects the design of steganography systems. Bottom colors uniform texture images, or images are not suitable for steganography [4]. In recent years, steganography has been more noticeable secure data transfer [5]. Steganography in images is presented in many different techniques, which target all of them have access to high capacity, security, and robustness[6].

As seen in Figure 2, the three vertices of a triangle are three objectives. Should be given to the use of reconciliation established between them [7].

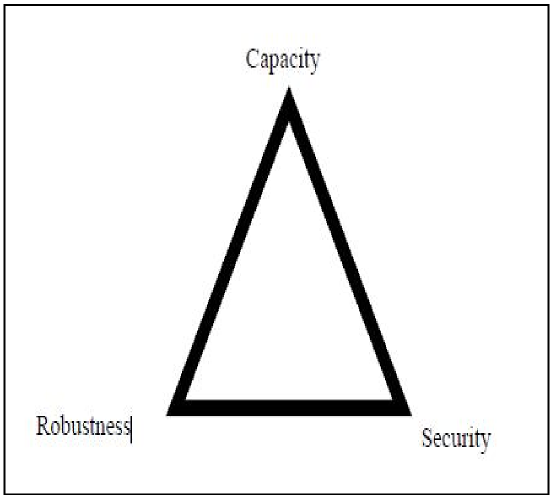


Figure 2: Characteristics of information hiding systems.

Ghasemi et al [8] have presented a method in which a combination of genetic algorithm and wavelet transform has been used. This capacity is taken into consideration. Ghorbany et al [9] have presented a method which establishes a compromise between the maximum rate and capacity are Signal to Noise.

2. Image Quality

Important factor in the field of steganography, image quality is carrying a secret message about the PSNR and MSE are considered [10]. If the original image and stego image H by H1 and HWIDTH, HLEN length and width of the image PSNR and MSE is calculated from the equation 2 is calculated from equation 1.

equation 1

$$MSE= \frac{\sum_{i=1}^{H\ LEN} \sum_{j=1}^{H\ WIDTH} [H(i,j) - H1(i,j)][H(i,j) - H1}{HLEN * HWIDTH}$$

equation 2

PSNR=10*log(255*255/mse)

The Mean squared error (MSE) is less indicative of the quality of the stego image, a low value, the maximum amount of signal to noise ratio (PSNR) indicate low quality of the image carrier [11]. The peak signal-to-noise level, noise level, which is the carrier of media placement information, the media has been created. The peak signal to noise level is measured in units of dB. If amount over thirty-dB signal-to-noise ratio, the human eye can hardly recognize the difference between the original image and data carriers [12]. Mean square error between the original image and the image shows an information carrier. As we see in Figure 3, there is an inverse relationship between PSNR and MSE. So which way is better PSNR value is high and low MSE value.

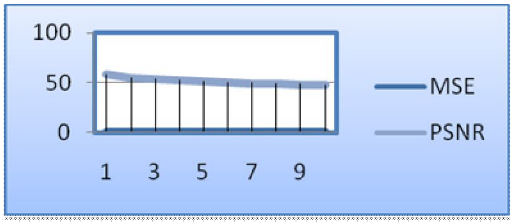


Figure 3: Relationship between PSNR and MSE

3. Similarity (SSIM)

The similarity between the original image and image information displays a carrier.

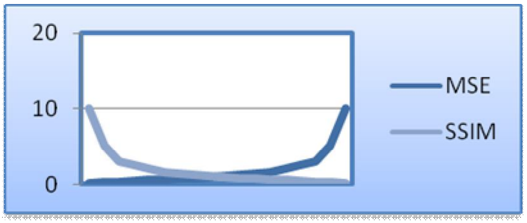


Figure 4: The relationship between MSE and SSIM

Figure 4 shows the relationship between MSE and SSIM. As you can see, there is an inverse relationship between these two cases.

4. Security Image

An attacker must be able to extract images without the secret key. Increase the security of steganography algorithms is the following:

- Use a combination of steganography and cryptography techniques.
- Use random key algorithm
- Failure to use a fixed number of bits
- Complexity of data discovery

5. Blind

At the time of extraction of secret information from the carrier object need not be the main object and the original object data can be properly extracted.

6. Bit error rate(Ber):

Information extracted from the raw data replaced the alternatives are compared, differences in the rates of high rises and shows the bit error parameter is incorrect algorithm. The bit error rate is lower, the higher the reliability of the algorithm used.

7. Capacity:

The maximum amount of information that can be carried in the media, steganography algorithm can be implanted without being carried in the media to apply tangible change. High capacity steganography algorithms is to evaluate the main parameters However, high-capacity, reduced image quality due to use of the algorithm can establish a compromise between quality and capacity of the application or the preference of one over the other.

8. conclusion

Steganography technique to hide the secret information in conventional media for safe transport through public channels such as the internet. In this study methods that are available in this area have been studied, the results show the effect of some key parameters to determine the right methods. These parameters are provided in ways that other methods than others preferences and are more reliable. Security parameters, capacity and transparency are the key parameters steganography images.

Secure random key shared between transmitter and receiver can be used or can be used to blind steganography techniques. Capacity can be used for variable bit rate. Adaptive techniques can be used for clarity images can cover up to psnr, mse, ssim be acceptable. It is suggested to have a reliable method of the key parameters must be blind steganography techniques, adaptive steganography techniques, random Key steganography techniques, variable bit rate steganography techniques used.

9. REFERENCES

[1]Blossom K, Amandeep K, Jasdeep S.2011. STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN. International Journal of Advances in Engineering & Technology,1:72-78

[2] Geetha C, Giriprakash H.2012. image steganography by variable embedding and multiple edge detection using canny operator . International Journal of Computer Applications (0975 – 888) 48:15-19

[3]Sivaiah S, Venkataiah C. 2011. An efficient lifting based 3-d discrete wavelet transform. IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network"CCSN, 2011:25-29

[4] Priya S, Amsaveni.2012. Edge Adaptive Image Steganography in DWT Domain. International Journal of Advances in Image Processing,2:91-94

[5] Hashemi Pour A, Payandeh A. 2012. A New steganography method based on the complex pixels. Journal of Information Security, 3: 202-208

[6] Pradhan A, Sharma D, Swain G. 2012. Variable rate steganography in digital images using two,three and four neighbor pixels. Indian Journal of Computer Science and Engineering (IJCSE),3:457-463

[7] Khare A, Saxena M, Jain H.2011. AMBTC-compressed image using genetic algorithm. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-2:68-71

[8] Ghasemi E, Shanbehzadeh J, Fassihi N. 2011. High capacity image steganography using wavelet transform and genetic algorithm . Proceeding of the International Multiconference of Engineers and Computer Scientists 2011 vol I,IMECS 2011. March 16-18,2011.Ho

[9] fariba ghorbany beram,Mashallah Abbasi Dezfouli,Mohammad Hossein Yektaie,"A New Steganography Method based on Optimal Coefficients Adjustment Process (OCAP)",International Journal of Computer Applications (0975 – 8887),Volume 87 – No.2, February 2014

[10] Kaushik P, Sharma Y.2012. Comparison Of Different Image Enhancement Techniques Based Upon Psnr & Mse.International Journal of Applied Engineering

[11] Verma A, Nolkha R, Singh A , Jaiswal G.2013. Implementation of Image Steganography Using 2-Level DWT Technique. International Journal of Computer Science and Business Informatics,1:1-14

[12] Maan V, Dhaliwal H.2013. Vector Quantization In Image Steganography. International Journal of Engineering Research & Technology (IJERT).2:10-15

Layered Approach for Preprocessing of Data in Intrusion Prevention Systems

Kamini Nalavade
Department of Computer Engineering,
VJTI, Matunga, Mumbai,
India

Dr. B. B. Meshram
Department ofComputer Engineering
VJTI, Matunga, Mumbai,
India

Abstract: Due to extensive growth of the Internet and increasing availability of tools and methods for intruding and attacking networks, intrusion detection has become a critical component of network security parameters. TCP/IP protocol suite is the defacto standard for communication on the Internet. The underlying vulnerabilities in the protocols is the root cause of intrusions. Therefor Intrusion detection system becomes an important element in network security that controls real time data and leads to huge dimensional problem. Processing large number of packets and data in real time is very difficult and costly. Therefor data pre-processing is necessary to remove redundant and unwanted information from packets and clean network data. Here, we are focusing on two important aspects of intrusion detection; one is accuracy and other is performance. The layered approach of TCP/IP model can be applied to packet pre-processing to achieve early and faster intrusion detection. Motivation for the paper comes from the large impact data preprocessing has on the accuracy and capability of anomaly-based NIPS. In this paper it is demonstrated that high attack detection accuracy can be achieved by using layered approach for data preprocessing in Internet. To reduce false positive rate and to increase efficiency of detection, the paper proposed framework for preprocessing in intrusion prevention system. We experimented with real time network traffic as well as he KDDcup99 dataset for our research.

Keywords: Intrusion, Security, Network, Layered approach

1. INTRODUCTION

The continuous improvements in technology have made the use of computers easy for gathering and sharing information using the Internet. The Transmission Control Protocol and Internet protocol suite (TCP/IP) is the de-facto standard for using the internet. Due to a number of reported attacks on networks originating from the Internet, security has become a primary concern for organizations connecting to the Internet. The Information flow on Internet is constantly under various attacks because of vulnerabilities lying in the structure of networks. Therefore it is essential to provide security to the information in transit. The secure connection itself must be established and maintained securely. The Transmission Control Protocol and Internet protocol (TCP/IP), which is the protocol suite that Internet was first developed in 1979. The primary focus was to ensure reliable communications between groups of networks connected by computers. At that time, security was not a primary concern as the users of the Internet were less. The information flow on Internet is constantly under various attacks. The root cause of these exploits is weaknesses in the protocols of underlying TCP/IP protocol suite.

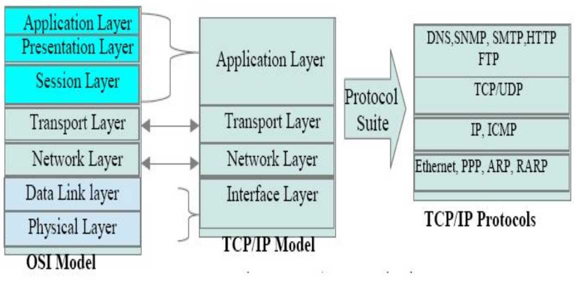


Figure 1 TCP/IP model

The TCP/IP protocol suite suffers from a number of vulnerabilities and security flaws inherent in the protocols. Those vulnerabilities are often exploited by attackers for session hijacking, sniffing, spoofing, Denial of Service (DOS) attacks and other attacks. The key vulnerability in most of the protocols of TCP/IP is lack of authentication mechanisms. This is the severe flaw which enables attacker to access the confidential information. The IP layer believes that the source address on any IP packet it receives is the same IP address as the system that actually sent the packet. The other vulnerability is connectionless communication between peers. IP layer does not ensure that a packet will reach its final destination. Also it does not guarantee that packets forwarded on network will arrive in the order. The following are the major TCP security problems. A malicious host can exhaust the server’s buffer by sending several SYN requests to a host, but never replying to the SYN & ACK the other host sends back. By doing so server will stop accepting new connections, until a partially opened connection in its queue is completed or times out. This ability to effectively remove a server from the network can be used as a denial-of-service attack. It can be used to implement other attacks, like IP Spoofing, reconnaissance.

RIP, OSPF and BGP are the widely used de facto standard of routing protocols on the Internet. These protocols suffer from major vulnerabilities which causes attacks on network such as denial of service, invalid route information. Routing attacks takes advantage of Routing Information Protocol (RIP), which is an essential component in a TCP/IP network. RIP is used to distribute routing information within networks and advertising routes out from the local network. RIP has no inbuilt authentication, and the information provided in a RIP packet is often used without verifying it. RIP's update messages are sent over UDP and can be modified by attackers. Attacks on RIP change the destination where data goes to, not where it came from. For example, an invader could forge a RIP packet, claiming his host "B" has the fastest path out of the network. All packets sent out from that network would then be routed through B, where they could be modified or scanned. An invader could also use RIP to effectively impersonate any host, by causing all traffic sent to that host to be sent to the attacker's machine instead. RIP, OSPF and BGP were studied with respect to their architecture, functionality and message types. OSPF suffers from implementation and configuration problems. BGP have vulnerabilities related confidentiality, integrity and authentication. This study provides immense help in describing security architecture for routing protocols.

Security protocols are the addition to the basic protocol set of TCP/IP suite to overcome the vulnerabilities lying in the design of these protocols. Security Protocols such IPSec, DNSSec, SSL, SSH, TLS are also prone to attacks such as DOS, spoofing, flooding etc. Attack detection in security protocols is crucial task. DNSSEC does not guard against poor configuration or bad information in the authoritative name server, and does not protect against buffer overruns or DDoS attacks. Small queries can generate larger UDP packets in response. DNSSEC has a hierarchical trust model. To securely resolve a name in DNSSEC, a root public key must be available at the resolver. The IPSEC protocols rely on a number of underlying technologies to achieve encryption and authentication. Specific SSH versions and implementations have been vulnerable to brute force attack.

In our research work we aim to develop an Intrusion Protection Systems which detects broad range of attacks along with reducing false alarms and increasing attack detection accuracy. During our research work we explored many of the vulnerabilities of these protocols and defense mechanisms for this. Although many defense techniques are the configuration based. The paper is organized as below. In section II we provide a brief overview of Intrusion Prevention Sytems. In section III Layered approach for intrusion detection is discussed. In Section IV Experimentation and results generated for our system is discussed followed by conclusion.

2. INTRUSION PREVENTION SYSTEM

Intrusion detection as defined by the Sysadmin, Audit, Networking, and Security (SANS) institute is the act of detecting activities that attempt to negotiate the confidentiality, integrity or availability of a resource [2]. Current network systems provide critical services for businesses to perform optimally and are target of attacks which aim to bring down the services provided by the network.

An Intrusion detection system (IDS) is software designed to detect unwanted attempts at accessing, manipulating, or disabling of computer systems, especially through a network. It is a specialized tool that knows how to parse and interpret network traffic and host activities. IDS technologies are not really effective against prediction a new attacks. There are several limitations, such as performance, flexibility, and scalability. The inadequacies inherent in current defenses have driven the development of a new breed of security products known as Intrusion Prevention Systems (IPS). Intrusion Prevention System (IPS) is a new approach system to defense networking systems, which combine the technique firewall with that of the Intrusion Detection properly, which is proactive technique, prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when an attack is identified, intrusion prevention block and log the offending data IPS make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. These systems are proactive defenses mechanisms designed to detect malicious packets within normal network traffic and stop intrusions dead, blocking the offending traffic automatically before it does any damage rather than simply raising an alert as, or after, the malicious payload has been delivered IPS use several response techniques. The comparison of IDS and IPS is shown in figure 2.[16]

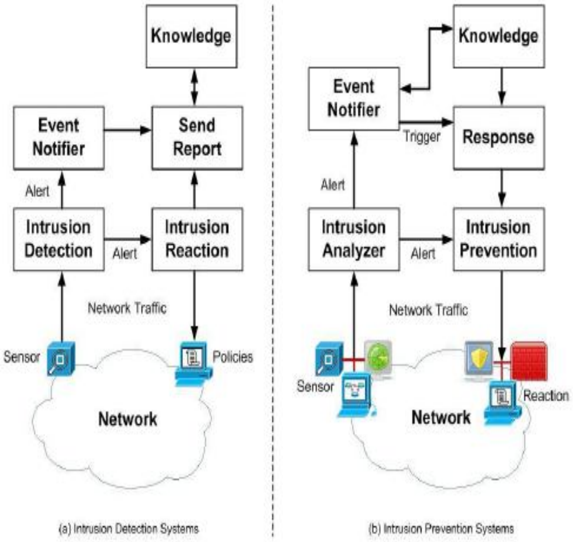


Figure 2 Comparison of IDS and IPS

Approaches to Intrusion Prevention Systems: There are different types of approaches is used in the IPS to secure the network.[14]

1. Signature-Based IPS: - It is commonly used by many IPS solutions. Signatures are added to the devices that identify a pattern that the most common attacks present. That's why it is also known as pattern matching. These signatures can be added, tuned, and updated to deal with the new attacks.

2. Anomaly-Based IPS: - It is also called as profile-based. It attempts to discover activity that deviates from what an engineer defines as normal activity. Anomaly-based approach can be statistical anomaly detection and non-statistical anomaly detection.

3. Policy-Based IPS: - It is more concerned with enforcing the security policy of the organization. Alarms are triggered if activities are detected that violate the security policy coded by the organization. With this type approaches security policy is written into the IPS device.

4. Protocol-Analysis-Based IPS - It is similar to signature based approach. Most signatures examine common settings, but the protocol-analysis-based approach can do much deeper packet inspection and is more flexible in finding some types of attacks.

IPS technologies: Basically IPS Host based and network-based.

1) Host-based IPS: Host-based IPSs [13] monitors the characteristics of a single host and the events occurring within

that host for suspicious activity. Examples of the types of characteristics a host-based IPS might monitor are wired and wireless network traffic, system logs, running processes, file access and modification, and system and application configuration changes. Most host-based IPSs have detection software known as agents installed on the hosts of interest. Each agent monitors activity on a single host and also performs prevention actions. The agents transmit data to management servers. Each agent is typically designed to protect a server, a desktop or laptop, or an application service. The agents are deployed to existing hosts on the networks, the components usually communicate over those networks instead of using a management network. Host-based IPSs run sensors on the hosts being monitored, they can impact host performance because of the resources the sensors consume.

2) Network-based IPS: A network-based IPS [13] monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity. Network-based IPS components are similar to HIPS technologies, except for the sensors. A network-based IPS sensor monitors and analyzes network activity on one or more network segments. Sensors are available in two formats: appliance-based sensors, which are comprised of specialized hardware and software optimized for IPS sensor use, and software-only sensors, which can be installed onto hosts that meet certain specifications.

3. LAYERED APPROACH FOR INTRUSION DETECTION AND PREVENTION

Preprocessing is the organization of collected data from sensors in a particular pattern. This data is then placed in a structured database format by means of parsing and reconstructing. The cleansing process is protocol specific as we need different attributes of packets for intrusion analysis. If packet is from blacklisted source then system should discard packet without verifying it. When the packets are transformed and stored in the respective data stores it triggers intrusion detection.

Layered-based intrusion detection system gets its motivation from TCP/IP model, where a number of protocols are assigned different task at different level. Similar to this model, the layered intrusion detection system represents a sequential layered approach. The goal of using a layered model is to reduce computation and the overall time required to detect anomalous events. The time required to detect an intrusive event is significant and can be reduced by eliminating the communication overhead among different layers. This can be achieved by making the layers autonomous and self-sufficient to block an attack without the need of a central decision maker. Every layer in layered intrusion detection system framework is trained separately and then deployed sequentially. We define four layers that correspond to the four attack groups mentioned in the dataset. They are interface layer, network layer, transport layer and application layer. Each layer is then separately trained with a small set of relevant features. Feature selection or reduction is important for layered approach and discussed in next section. In order to make the layers independent, some features may be present in more than one layer. The layers essentially act as filters that block any anomalous connection, thereby eliminating the need of further processing at subsequent layers enabling quick response to intrusion. The effect of such a sequence of layers is that the anomalous events are identified and blocked as soon as they are detected [2].

Data preprocessor is responsible for collecting and providing the audit data (in a specified form) that will be used by the next module to make a decision. Data preprocessor is, thus, concerned with collecting the data from the desired source and converting it into a format that is understandable by the intrusion detector. Data used for detecting intrusions range from user access patterns to network packet level features such as the source and destination IP addresses, type of packets . We refer to this data as the audit patterns.

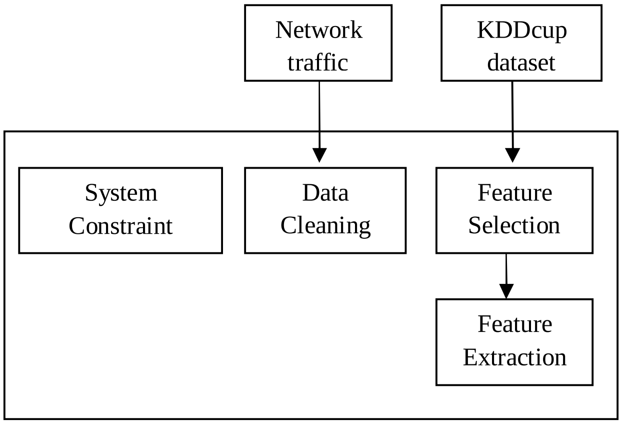


Figure 3 Preprocessing of Data

In the proposed model we have used four major functionalities in preprocessing module as shown in figure 2. Two different datasets are used for our experiments. Some experiments are carried out on real time network audit trails collected over high speed network. Often Intrusion Detection Systems are loaded with huge amount of data to be processed. Processing this enormous amount of data in real-time is major challenge faced in this area. Reduction in input data rate will provide additional time to detection engine for thoroughly process data and give more detection accuracy with less false positive. In the first round, input data cleaning by removing unwanted parameters is performed. Removal of noise and incomplete data makes the task of intrusion detection faster. But it also increases overlapping behavior of normal and intrusion data. Most modern data mining and soft computing based Intrusion Detection Systems uses data cleaning techniques to provide quality data to detection engine and in turn results in improved intrusion detection rate.

Our proposed system uses feature selection and extraction on KDD cup dataset which is freely available intrusion dataset. This dataset contains 41 features for intrusion specification. Not all the features available in raw input dataset are useful for intrusion detection. For detecting particular category of intrusion, we require only subset of these features. Removal of forged and duplicate data will help in reducing false positive rate.

Another reason for false positive is lack of knowledge about network topology, hosts and services running on the hosts. In proposed model third functionality is system constraint check or configuration based processing. Configuration data about existing network, hosts, and services are stored in a file. Configuration parameters help in differentiating normal and intrusion data by providing additional information. Some portion of overlapping behavior is the challenge for Intrusion Detection Systems. The data for which Intrusion Detection System is not sure results in false detection, either false negative or false positive. Such ambiguity can be reduced by collecting information from various sources. This again helps in reducing false positive rate in proposed system. In our approach, we perform preprocessing based on type of packet. For proliferation of performance and reducing time factor in detection, we separate the packets into TCP/IP protocols, routing protocols and security protocols. Algorithm for preprocessing is given below

```
Algorithm: PreprocessPacket(p)
Input: Packet p, System Configuration Constraints List L
Begin
2.  Read packet header $\psi$.
3. Detect Type of Protocol   $\Delta = \psi$ ->T
4.  If ($\psi$ ->T=TCP/UDP/IP/ICMP/ARP/RARP)   $\Delta = 1$.      // To separate the TCP/IP , routing and security protocols.
        else if ($\psi$ ->T = RIP/ BGP/EGP)  $\Delta=2$.
        else  $\Delta = 3$.
5. CleanPacket(Packet, Type)  //This method will remove unnecessary header fields
6. If incomplete/duplicate Packet then discard packet;
7.  End
```

We successful created data records for TCP/IP Packets and separate log files for the routing and security protocols for our experimentation. To collect the attack data, both, the web requests and the data accesses were logged. For the first data set, we generate 45 different attack sessions with 275 web requests resulting in 54,390 data requests. Combining the two together, the unified log has 45 unique attack sessions with 275 event vectors.

For the second dataset we used KDD dataset. Every record in the KDD 1999 data set symbolizes 41 features representing a variety of attacks such as the Probe, DoS, R2L and U2R. However, using all the 41 features for detecting attacks belonging to all these classes severely affects the performance of the system and also generates superfluous rules, resulting in fitting irregularities in the data which can misguide classification. Hence, we performed feature selection to effectively detect different classes of attacks. We now describe our approach for selecting features for every attack and why some features were chosen over others.

```
Algorithm: FeatureSelection
Input: Set of 41 features from KDD cup Data Set
Output: Reduced set of features R.

Step 1.  Calculate the information gain for each attribute $Ai \varepsilon D$  using (3).
Step 2.  Choose an attribute Ai from D with the maximum information gain value.
Step 3.  Split the data set D into subdatasets {D1,D2, . . . Dn} depending on the attribute values of Ai   where Cj stands for jth attribute of class C.
Step 4.  Find all the attributes whose information gain ratio > threshold.
Step 5.  Store the selected attributes in the set R and output it.
Step6:  End
```

We tested our algorithm for each category of attack. For every category, we applied all relevant attributes for that category, calculated gain for them and generated small subset which contains most relevant attributes for that category.

4. EXPERIMENTATION & RESULTS

Data preprocessing is major component of our proposed architecture. We have considered two datasets for our experimentation as mentioned in previous sections. The first data is collected over real time network using packet generators. We have developed a Java program for data formatting and implementing a layered approach. The program works as given in algorithm 1. The results achieved are logged and stored in the database. Three separate tables for TCP/IP protocols, routing protocols and security protocols are created. This helps in further analysis of packets. Before storing the packet info in the database, signatures for the attack on a specific protocol are searched. This reduces the time complexity rapidly as there is no need to check with signatures which are for other protocols.

The other dataset used is KDDcup1999 intrusion dataset which contains wide variety of intrusions simulated in network environment to acquire nine weeks of raw TCP dump data for a local-area network. A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address. Each connection is labelled as either normal, or as an attack, with exactly one specific attack type. It is important to note that the testing data is not from the same probability distribution as the training data. This makes the task more realistic. The datasets contains a total of 22 training attack types. There are 41 features for each connection record that are divided into discrete sets and continuous sets according to the feature values. It consists of number of total records 494021. The 22 different types of network attacks in the KDD99 dataset fall into four main categories: DOS (Denial of Service), Probe, R2L(Remote to

Local), U2R(user to remote). The attacks in each class are as shown below:

Table 1: Classes of Attacks

S.N	**Class**	**Attack Types**
1	DOS	Back, Land, Neptune,pod, smurf, Teardrop,
2	U2R	Buffer_overflow, loadmodule, perl, rootkit
3	R2L	ftp_write, guess_passwd, imap, multihop, phf, spy,warezlient, warezmaster
4	Probe	IPsweep,nmap, satan,portsweep

For intrusion analysis all the 41 features are not required. Some specific features are only contributing for a specific attack. This reduces the amount of work for intrusion detection and increases accuracy. The feature selecion algorithm is given above in section III. The results we achieved after applying the algorithm is given below.

Feature Selection from KDD dataset

1. Feature Selection for Probe Layer

Probe attacks are aimed at acquiring information about the target network from a source that is often external to the network. For detecting Probe attacks, basic connection level features such as the ‘duration of connection’ and ‘source bytes’ are significant. We selected only four features for Probe layer. The features selected for detecting Probe attacks are presented in Table B.1.

Table B.1: Features for Probe Detection

S.N.	Name of Feature	Feature_No
1	src_bytes	5
2	duration	1
3	protocol_type	2
4	flag	4

2. Feature Selection for DoS Attacks

DoS attacks are meant to prevent the target from providing service(s) to its users by flooding the network with illegitimate requests. Hence, to detect attacks at the DoS layer, network traffic features such as the ‘percentage of connections having same destination host and same service’and packet level features such as the ‘duration’ of a connection, ‘protocol type’, ‘source bytes’, ‘percentage of packets with errors’ and others are significant. To detect DoS attacks, it may not be important to know whether a user is ‘logged in or not’, or whether or not the shell’ is invoked or ‘number of files accessed’ and, hence, such features are not considered in the DoS layer. From all the 41 features, we selected only nine features for the DoS layer.

Table B.2: DoS Layer Features

S.N.	Name of Feature	Feature_No
1	src_bytes	5
2	duration	1
3	protocol_type	2
4	flag	4
5	count	23
6	dst host same srv rate	34
7	dst host serror rate	38
8	dst host srv serror rate	39
9	dst host rerror rate	40

The features selected for detecting DoS attacks are presented in Table B.2.

3. Feature Selection for U2R attacks

U2R attacks involve the semantic details which are very difficult to capture at an early stage at the network level. Such attacks are often content based and target an application. Hence, for detecting U2R attacks, we selected features such as ‘number of file creations’, ‘number of shell prompts invoked’, while we ignored features such as ‘protocol’ and ‘source bytes’. From all the 41 features, we selected only eight features for the U2R layer. Features selected for detecting U2R attacks are presented in Table B.3.

Table B.3: U2R Layer Features

S.N.	Name of Feature	Feature_No
1	num_compromised	13
2.	root_shell	14
3	num_root	16
4.	num_file_creations	17
5	num_shells	18
6	num_access_files	19
7	is_host_logins	21

4. Feature Selection for R2L Attacks

R2L attacks are one of the most difficult attacks to detect and most of the present systems cannot detect them reliably. However, our experimental results presented earlier show that careful feature selection can significantly improve their detection. We observed that effective detection of the R2L attacks involve both, the network level and the host level features. Hence, to detect R2L attacks, we selected both, the network level features such as the ‘duration of connection’, ‘service requested’ and the host level features such as the ‘number of failed login attempts’ among others. Detecting R2L attacks, require a large number of features and we selected 14 features. The features selected for detecting R2L attacks are presented in Table B.4

Table B.4: R2L Layer Features

S.N.	Name of Feature	Feature_No
1	src_bytes	5
2	duration	1
3	protocol_type	2
4	flag	4
5	num_failed_logins	11
6	num_file_creations	17
7	num_shells	18
8	num_access_files	19
9	is_host_login	21
10	is_guest_login	22

Feature selection is an important task of Network Intrusion application. Large amount of attacks are threats to network and information security. Using Feature selection approach kdd attacks are detected with less error rate and high accuracy.

5. CONCLUSION

Data preprocessing is widely recognized as an important stage in anomaly detection. Data preprocessing is found to predominantly rely on expert domain knowledge for identifying the most relevant parts of network traffic and for constructing the initial candidate set of traffic features. Motivation for the paper comes from the large impact data preprocessing has on the accuracy and capability of anomaly-based NIPS. The review finds that many NIPS limit their view of network traffic to the TCP/IP packet headers. Time-based statistics can be derived from these headers to detect network behavior, and denial of service attacks. A number of other NIPS perform deeper inspection of request packets to detect attacks against network services and network applications. On the other hand, automated methods have been widely used for feature extraction to reduce data dimensionality, and feature selection to find the most relevant subset of features from this candidate set. These context sensitive features are required to detect current attacks. In our proposed system, we try to evaluate attack at every level of TCP/IP Model by combining network Intrusion detection and layered approach. Our preprocessing module has packet capture, feature selection and storing it in databases. But along with these basic features it also evaluates known network attacks by protocol layer wise inbuilt detection algorithm.

6. REFERENCES

[1] Shun-ichi Amari and Si Wu, “Improving support vector machine classifiers by modifying kernel function”, RIKEN Brain Science Institute Japan.

[2] Kapil Kumar Gupta, Baikunth Nath and Ramamohanarookotagiri, “A layered approach using conditional random fields for intrusion detection”, IEEE Tranc. on Dependence and secure computing, Vol.7, 2010

[3] G.MeeraGandhi, Kumaravel Appavoo and S.K Srivasta, “Effective network intrusion detection using classifiers decision trees and decision rules”,Int. J. Advanced network and application, Vol2, 2010

[4] Bernhard scholkopf, Kah kay Sung, Chris Burges, Federico and other, IEEE Transactions on signal processing, Vol. 45 , 1997

[5] Richard Machlin and David Opitz, “An empirical Evaluation of bagging and boosting”, National conference on A.I, providence Rhode Island 1997.

[6] Sandy Peddabachigari, Ajit Abraham and Johmson Thomas, “Intrusion detection system using decision trees and SVM”, Oklahoma state university USA.

[7] Huy Anh Nguye and Deokjai choi, “Application of data mining to network intrusion detection”, Korea.

[8] Weiming Hu, Wei Hu and Steve Maybank, “Adaboost based algorithm for network intrusion detection”, Tranc. On system man and cybernetics, 2008.

[9] Shilpa Lakhina, Sini Joseph and Bhupendra Verma, “Feature reduction using PCA for effective Anomaly- based intrusion detection on NSL-KDD”, Int. J. of engineering science and technology, 2010

[10] Snehal A.Mulay, P.R Devale and G.V Garje, “Intrusion detection using SVM and decision tree”, Int. J. of computer application, 2010

[11] J.Vishumathi and K.L Shunmuganathan, “A computational intelligence for evaluation of intrusion detection system ”, Indian J. of science and technology, Jan 2011

[12] Ritu Ranjani Singh, Neetesh Gupta and Shiv Kumar, “To reduce the false alarm in intrusion detection system”, Int. J. of soft computing and engineering, May 2011

[13] Defending yourself: IEEE software September/October 2000 tutorial

[14] Xunyi Ren, Ruchuan Wang and Hejunzhou, “intrusion detection system method using protocol classification and Rough set based SVM”, www.ccsenet.org/journal.html,2009

[15] Peyman Kabiri and Ali A. Ghorbani, “Research on ID and Response:A survey ”, Int. J. of network security, 2005 M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[16] Deris Stiawan, Abdul Hanan Abdull ,”Characterizing Network Intrusion Prevention System ”*International Journal of Computer Applications (0975 – 8887) Volume 14– No.1, January 2011*

[17] Davis, Jonathan Jeremy & Clark, Andrew J. (2011) Data preprocessing for anomaly based network intrusion detection : a review. *Computers & Security*, *30*(6-7), pp. 353-375.

Different RDB to RDF mapping languages

Priyanka Shukla
Department of Computer Science and Engineering
RITM
Lucknow, India

Vaibhav Singh
Department of Computer Science and Engineering
RITM
Lucknow, India

Akanksha Shukla
Department of Computer Science and Engineering
RITM
Lucknow, India

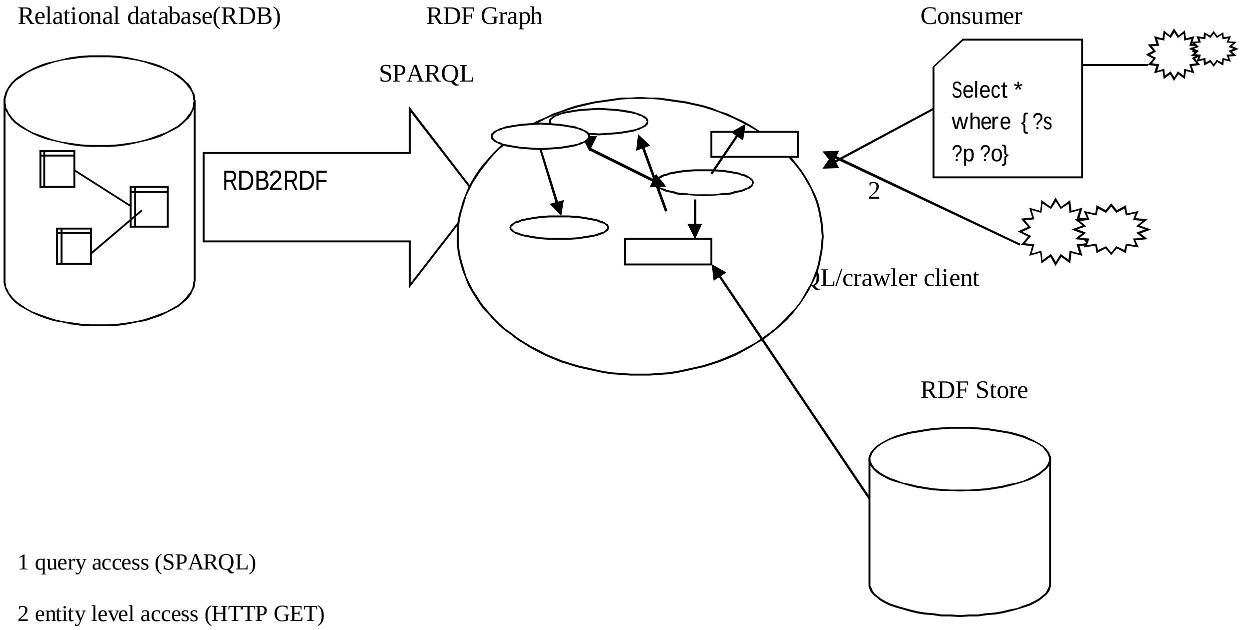
Abstract: This document deals with the different techniques, mapping languages ,tools ,applications used for mapping Relational Databastes and Resource Description Framework.This document will serve as a guide for selecting a particular language for mapping .For the development of semantic web we need to map Relational Database to Resource Description Framework.Since most of the data on web is stored on RelationalDatabase and a conceptual gap is to be bridged between the Relational Database model and RDF to make this data available on web semantic.Many mapping languages and approaches have been found leading to the ongoing standardization of the World WideWeb Consortium(W3C) carried out in the RDB2RDF Working Group(WG).This paper would provide help and recommendations for selecting a mapping language.

Keywords: Mapping Patterns, Mapping Language, R2RML,Relational Databases, SPARQL, SQL,,OWL,Semantic Web.

1. INTRODUCTION

Mostly all the websites are backed by Relational databases.Most information is still modeled and are stored in Relational databases and hence out of reach for many web semantic applications. The success of semantic web is dependent on the translation of RDB to RDF and this is done throughdirect mapping.Direct mapping is a simple translation of RDB to RDF. As a consequence, such applications need to create a corresponding mapping between the relational and the semantic models for being able to access relational data. In this paper we study why we need these mapping languages for making data available on web.Since we study different mapping languages we have to makesome comparative study for when and why to use a particular mapping language[9].This paper would describe the problems that occur with different mapping languages .So we must have certain classifications and categories which describes when to use which language.In this paper we also study a number of reusable mappings, which we define as RDB2RDF Mapping Patterns.

Mapping RDB to RDF is an active field of research . Many approaches were explored to make relational data available to Semantic Web-enabled applications. These approaches introduced mapping languages that range from simple and pragmatic to highly specific or general-purpose.



1 query access (SPARQL)

2 entity level access (HTTP GET)

3 access via dump(HTTP GET)

2. RELATED WORKS:

Satya S. Sahoo et al. has discussed different methods to generate mappings between RDB and RDF which are basically of two categories:Automatic Mapping Generation: This discusses a set of mappings between RDB and RDF namely:*A RDB record is a RDF node.The column name of a RDB table is predicate.*RDB cell is a value.An example of this approach is Virtuoso RDF View that uses the unique identifier of a record (primary key) as the RDF object, the column of a table as RDF predicate and the column value as the RDF subject. Other examples of similar tools are D2RQ and SquirrelRDF .[1] This approach also allows Semantic Web applications to query those RDB sources where the application semantics is defined in terms of the RDB schema. This approach is also called "Local ontology mapping". Domain Semantics-driven Mapping Generation: This approach incorporates domain semantics these are not captured in RDB schema .[10] Also, a mapping generated by using domain semantics also reduces the creation of triples for redundant or irrelevant knowledge. Mapping between RDB and RDF is represented by Xpath in XSLT stylesheet in a XML based declarative language.Two types of mapping implementations are–static andStatic ETL ,dynamic –query driven. ETL uses batch process to create RDF repository. Queries in systems mapping RDB to RDF may either be in SPARQL .SPARQL may be transferred into one or more sql query that are executed against RDB

.

➢ Matthias Hert et al. has discussed a feature-based comparison of the state-of-the-art RDB-to- RDF mapping languages.This comparison framework is based on use cases and requirements for mapping RDBs to RDF.In this paper we apply this comparison framework and four main categories of mapping languages have been propsed .These are Direct mapping, Read-only general-purpose mapping, Read write general-purpose mapping, and Special-purpose mapping. In direct mapping, a direct approach for mapping RDBs to the Semantic Web is proposed[2]. It maps relational tables to classes in an RDF vocabulary and the attributes of the tables to properties in the vocabulary.The goal is to expose a RDB on the (Semantic) Web to make extra statements about it. The goal of R2RMLis to define a vendor-independent mapping language for read-only data access. R3M enables bidirectional RDF-based access to the RDB, *i.e.*, read and *write* access is supported. It employs a RDF-based syntax that contains the mappings of tables to classes and attributes to properties as well as information about integrity constraints.This paper provides guidelines for a RDB-to-RDF mapping language for a given applicationscenario and its requirements.

➢ Juan F. Sequeda et al. has discussed about the problems of directly mapping a Relational database to an RDF graph with OWL vocabulary .This paper shows that direct mapping is an automatic way of translating a relational database to RDF.This paper discusses that there are basically two fundamental properties of Direct Mapping :information preservation and query preservation. A direct mapping is information preserving if none of the information is lost about the relational instance being translated, that is,there exists the ways through which original database instances may be recovered from the RDF graph resulting from the translation process[3]. A direct mapping is query preserving if every query over a relational database can be translated into an equivalent query over the RDF graph resulting from the mapping.It assures that every relational query can be evaluated using the mapped RDF data. To formally define query preservation, we focus on relational queries that can be expressed in relational algebra and RDF queries that can be expressed in SPARQL .Additionally desirable properties are:monotonicity and semantics preservation.Monotonicity is desired to avoid recomputation of the entire mapping after updating databases .In general and practical scenario direct mapping is information preserving,monotone and query preserving only when relational databases contain null values.But unfortunately we found that no monotone direct mapping is semantic preserving if foreign keys are considered.

CristianP´erez de Laborda et al. in this paper it was discussed that main drawback of semantic web is the lack of semantically rich data,so an approach was presented to map legacy data stored in relational databases into the Semantic Web using virtually any modern RDF query language.It was suggested in this paper that web developer need not to learn and adopt a new mapping language, but he may perform the mapping task using his preferred RDF query language.In this paper a technique called Relational OWL was introduced that automatically transform relational data into representatable form. It converts the schema of a database automatically into an ontology and the data items as its instances, i.e. the data is described as it was in the database.It is a reasonable and acceptable technique because legacy data stored in relational database can be easily accessed by their built-in functionalities[4]. To perform such a mapping task, a Semantic Web developer does not need to learn and adopt a new mapping language, but he may perform the mapping task using his preferred RDF query language. For this purpose, data and schema components of the original relational database are first translated automatically into their Semantic Web representation based on Relational OWL. Then they may either be processed or mapped directly to a target ontology.Using virtual RDF query language results into RDF graphs as query results.

➢ Juan F. Sequeda et al. in this paper has discussed that as we know for semantic web applications we need to map relational database to RDF .Since the W3C RDB2RDF presented two standards to map relational database to RDF .They are : Direct Mapping and R2RML mapping language. Direct Mapping is the default way of representing a relational database as RDF based on the structure of the database schema. R2RML is a language for expressing customized mappings from relational databases to RDF.Inthis particular paper different mappings have been compiled to present a non-exhaustive list of RDB2RDF mapping patterns.These mappings were represented in R2RML[5] . We present four type of mapping patterns: Attribute Mapping Patterns, Table Mapping Patterns, Join Mapping Patterns and Value Translation Patterns[8]. Each pattern consists of a name, a question that defines the problem that is being addressed, description of the context, description of the solution in R2RML, an example R2RML mapping, a discussion and related patterns.In this paper fourteen mapping patterns have been presented .

Research paper	Technology	Language	Advantage	Disadvantage
SatyaS.Sahoo et al.	Automatic Mapping and Domain Semantics generation	SPARQL	Reduced tripples	-
Matthias Hert et al.		R2RML,R3M	Read and write access is supported	
Juan F. Sequeda et al	RDF graph with OWL vocabulary	RDF query,SPARQL	Semantic preservation and query preservation	Lacks monotone direct mapping if foreign keys considered
CristianP´erez de Laborda et al	Relational OWL	RDF query language	Legacy data stored in relational database can be easily accessed	
Juan F. Sequeda et al	Mapping Patterns	R2RML	-	Increased attributes results in increased query size

Table I: Comparison table for different approaches of RDB to RDF mapping language .

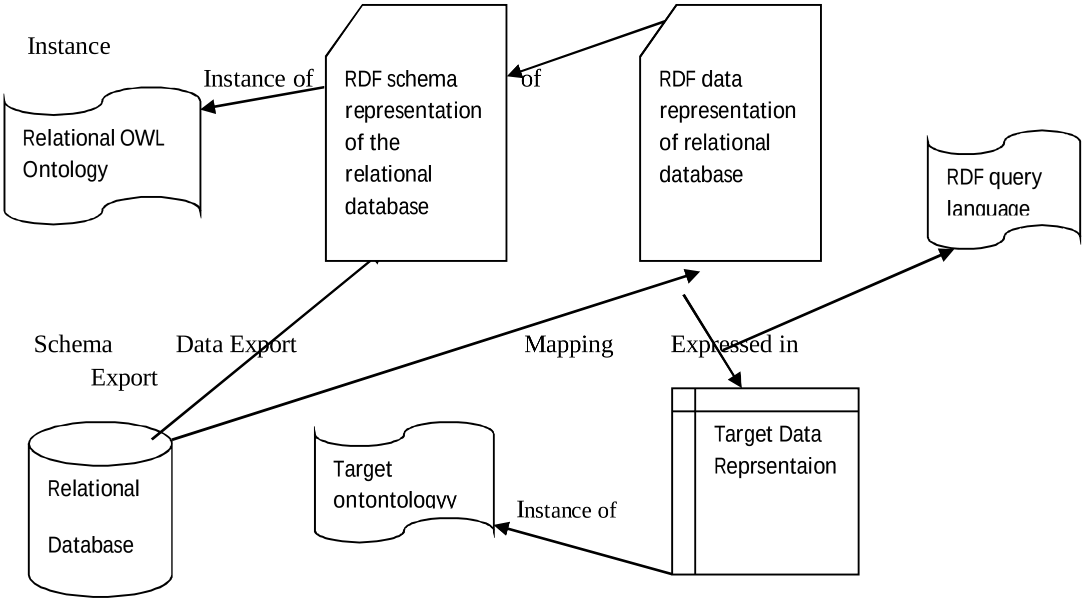


Figure 2. Mapping Process

Figure .2 shows the complete relational database to RDF mapping process. Firstly the relational OWL representation of the data and data components of the original data source are generated. The schema representation is then converted into an instance of Relational OWL ontology.AS the relational OWL representation of the relational database is done the second step of actual mapping is performed. RDF query language are used to make queries for RDF model.

3. DISCUSSION

In this paper we studied different approaches for mapping RDB to RDF.Different approaches we studied have some advantages and disadvantages like using Direct Mapping could not be semantically preserved if the foreign keys are considered[8].On the other hand mapping using domain semantics reduces the creation of triples for irrelevant knowledge.Using the concept of Triplify results in a boost of semantic web applications.Triplify mappings are implemented as PHP scripts.There exist difficulties in querying RDF graphs by using RDF query languages.All the queries must be expressed as if they are real XML documents not RDFgraphs Graphs[7].To overcome with such problems SQL syntax based languages were used in order to be easily understood and adoptable.But again such languages like RDQL have some drawbacks like the result of certain queries are not valid RDF triples.Thus to overcome with such difficulties we use different language SPARQL as representative of RDF query language .Use of different mapping patterns impacts upon the query performance.Sometimes if we increase the amount of attributes to be mapped, the size of SQL query would increase.

4. CONLCUSION

So,in this document we presented so many techniques or approaches for mapping RDB to RDF.These approaches are suggested and adopted to understand its mapping simplicity and implementing the language. These mapping languages are highly expressive.But this expressiveness sometimes results into increased complexity.So,different types of mapping languages are recommended according to the application scenarios.On the other side if we use RDF graph with OWL vocabulary for mapping RDB to RDF there exists certain problems.Combination of monotonicity with OWL vocabulary creates a problem in generating a semantically preserved direct mapping.This problem is solved by using non-monotone direct mapping.Most of the join and projection operations are not directly processed by RDQ query so they are passed to the underlying database with generated SQL query.To overcome the limitations of mapping patterns and solve performance issues we come up with new mapping patterns in areas such as Named Graphs, Blank Nodes for anonymous or sensitive data, Metadata, Languages, Data types[6].Finally we found that this is an area of research which needs to be focused and further researchers must be involved in working for the evolution of new mapping approaches to present web semantic.

5. REFERENCES

[1] BSatya S. Sahoo, Wolfgang Halb, Sebastian Hellmann, Kingsley Idehen, Ted ThibodeauJr, Sören Auer, Juan Sequeda, Ahmed Ezzat, Business Intelligence Software Division, HP”Survey of Current Approaches for Mapping of Relational Databases to RD”. In W3C RDB2RDF Incubator Group January 08 2009.

[2] ChomsHert, Matthias; Reif, Gerald; Gall, Harald (2011).A Comparison of RDB-to-RDF Mapping Languages.In:Proceedings of the 7th International Conference on Semantic Systems (I-Semantics), Graz, Austria, September 2011.

[3] Juan F. Sequeda,MarceloArenas,Daniel P. Miranker “On Directly Mapping Relational Databases To RDF And OWL” in International World Wide Web Conference Committee (IW3C2) 2012.

[4] CristianP´erez de Laborda and Stefan Conrad “Database to Semantic Web Mapping using RDF Query Languages” in 25th International Conference on Conceptual Modeling, Tucson, Arizona, November 2006, Springer Verlag

[5] Juan Sequeda1, Freddy Priyatna, and Boris Villaz_on-Terrazas ,” Relational Database to RDF Mapping Patterns” in W3C RDB2RDF Working Group(2012)

[6] RDB2RDF by “RDB2RDF Working Group” on 21-09-2012.

[7] Edgard Marx1,Percy Salas1,Karin Breitman1, José Viterbo2,andMarco Antonio Casanova1”RDB2RDF:A relational to RDF plug-in for Eclipse” in Wiley Online Library,3 july 2012.

[8] Nuno Lopes “An overview of RDB2RDF techniques and tools”in DERI conference,August 2009.

[9] Juan F. Sequeda,Daniel P. Miranker “SPARQL Execution as Fast as SQL Execution on Relational Data”,University Of Texas,Austin

[10] Kate Byrne “Relational database to RDF Translation in the Clutural Heritage Domain”in School of Informatics,University of Edinburg.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 374 - 376, 2014

Detection of Black Hole in AD- HOC Networks

Sona Malhotra
UIET
Kurukshetra, Haryana
India

Sandeep Kumar
UIET
Kurukshetra, Haryana
India

ABSTRACT: Unattended installation of sensor nodes in the environment causes many security threats in the Ad-hoc networks. The security of the DSR protocol is threaded by a particular type of attack called Black Hole attack. Black hole in Ad- hoc networks is a major problem. The proposed work includes detection and countermeasure rules to make the sensor network secure from these attacks. In our research DSR routing protocol is used to detect which node sends the reply after getting the request packet. This work will lead to minimum delay of packets in simulation results.

Keywords: Ad-hoc network, Black hole, routing protocol, DSR.

1. INTRODUCTION

Ad-hoc networks are a collection of thousands of nodes that are small in size, cheaper in price with restricted energy storage, less memory space and limited processing capability. Ad-hoc networks are mobile wireless networks that have no fixed infrastructure. There are no fixed routers instead each node acts as a router and forwards traffic from other nodes. Ad hoc networks are a new paradigm of wireless communication for mobile hosts which are also known as nodes.This network allow spontaneous formation and deformation of mobile networks. A mobile ad hoc network is a collection of mobile hosts that communicates with each other within the network. MANET has Multi-hop commutation capability. There is no defined administration or a backbone network to support it. In these types of networks each node works as an independent router. Each mobile host use wireless RF transceivers as network interface.

1.1 Security Attributes

- Availability: ensures the survivability of network services despite denial of service attacks. A denial of service attack can be launched at any layer of an ad hoc network. On the physical and media access control layers an adversary node employ jamming to interfere with communication on physical channels. On the network layer, an adversary node could destroy the routing protocol and disconnect the network. On the higher layers an adversary node could bring down high-level services.
- Authentication: enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary node could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
- Non-repudiation: ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.
- Confidentiality: Ensures that secret information or data is never disclosed to unauthorized devices. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.
- Integrity: Ensures that a message received is not corrupted. A message could be corrupted because of benign failures such as radio propagation impairment or because of malicious attacks on the network.

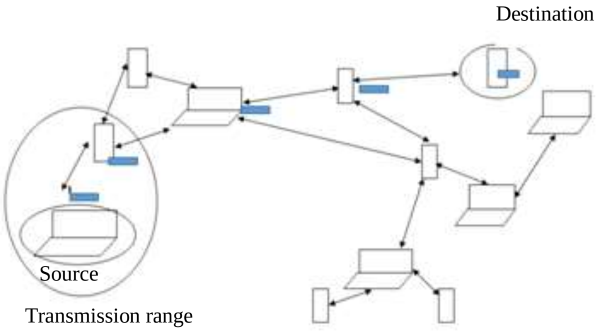


Figure 1.1 Data transmission in Ad-hoc network

1.2 Types of attacks

Black hole attack: The Black hole is a kind of denial of service where a malicious node can attract all other packets by falsely claiming a fresh route to the destination and then absorb them without forwarding. [1][2]. Cooperative Black hole means the malicious node acts in a group. A black hole attack can be easily launched by an adversary node in the sensor network. The Black hole attack is an active insider attack. Since the data packets do not reach the destination node on account of this attack data loss will occur. It has two properties: first the attacker consumes the diverted packets without any forwarding to the receiver. Second the nodes destroy the mobile ad hoc routing protocol to promote itself as it is having a valid route to a destination node. The defected node tried to advertise itself about the path of the route to the destination node.

Gray hole Attack: The attacker node initially forwards the packets and participates in routing. The Gray Hole node advertises itself as having a valid or shortest path to the destination node initially. A Gray Hole may exhibit its malicious behaviour in various techniques. It simply drops packets coming from or destined to certain specific nodes in the network while forwarding all the packets for other nodes[3].

1.2 Protocol Used

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks. DSR allows the network to be completely self-organizing and self-configuring without the need for any existing network infrastructure or administration. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well even with very high rates of mobility. This document specifies the operation of the DSR protocol for routing unicast IPv4 packets. In DSR every mobile node in the network needs to maintain a route cache where it caches source routes that it has learned. When a host wants to send a packet to some other host it first checks its route cache for a source route to the destination. In the case a route is found the sender uses this route to propagate the packet. Otherwise the source node initiates the route discovery process. Route discovery and route maintenance are the two major parts of the DSR protocol.

2. RELATED WORK

1. Leela Krishna Bysani *et al.* [4] suggested that WSN will emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks since once deployed these networks were unattended and unprotected. Some of the inherent features like limited battery and low memory makes sensor networks infeasible to use conventional security solutions which needs complex computations and high memory. There were lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the data attacks in sensor nodes are wormhole, black hole and selective forwarding attack. In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack was selective forwarding attack where compromised node drops packets selectively which may deteriorate the network efficiency. In this paper the author discussed about selective forwarding attack and some of the mitigation schemes to defend this attack.
2. Jatin D. Parmar *et al.* described that Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore interest in research of Mobile Ad-hoc Network has been growing since last few years. In this paper the author have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security was a big issue in MANETs as they were infrastructure-less and autonomous. Main objective of writing this paper was to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. This article would be a great help for the people conducting research on real world problems in MANET security.
3. Sukla Banerjee *et al.* [31] proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks in the hope that the malicious nodes can be detected & removed in between transmission. Flow of traffic was monitored by the neighbors of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving.
4. Sarvesh Tanwar *et al.* [1] suggested that with the advancement in radio technologies like Bluetooth IEEE 802.11 a new concept of networking has emerged; this was known as ad hoc networking where potential mobile users arrive within the range for communication. As network was becoming an increasingly important technology for both military and commercial distributed and group based applications, security was an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks MANETs were more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks or internal attack and external attacks the security services such as confidentiality, authenticity and data integrity were also necessary for both wired and wireless networks to protect basic applications. One main challenge in design of these networks were their vulnerability to security attacks. In this paper the author study the threats an ad hoc network faces and the security goals to be achieved.
5. Sonia *et al.* [2] proposed that due to the spontaneous nature of ad-hoc networks, they were frequently established insecure environments, which made them vulnerable to attacks. These attacks were launched by participating malicious nodes against different network services. Ad hoc On-demand Distance Vector routing (AODV) was broadly accepted network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack was one of the severe security threats in ad-hoc networks which could be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper a review on different existing techniques for detection of pooled or co-operated black hole attacks with their defects were presented.
6. Fidel Thachil *et al.* [3] presented a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. In this approach every node monitors neighbouring nodes and calculates trust value on its neighbouring nodes dynamically. If the trust value of a monitored node goes below a predefined threshold, then the monitoring node assume it as malicious and avoids that node from the route path. The experiment reveal that the proposed scheme secures the AODV routing protocol for MANET by mitigating and avoiding black hole nodes.

3. PROPOSED WORK

The proposed work will check the percentage of packets received. This will combat black hole in DSR routing protocol. In this approach any node uses number rules to inference about honesty of reply's sender. The main aim is to check out the set of malicious nodes locally at each node whenever they tries to act as a source node. The network will wait and check the replies from all neighbouring nodes to find a safe route. The performance is measured in terms of packet delivery then DSR (Dynamic source Routing Protocol) in the presence of black holes with minimum delay. The use of dynamic source routing is it allows packet routing to be loop-free. It does not require any up-to-date routing information in the intermediate nodes through which packets are forwarded. The Simulation's results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional DSR in the presence of Black holes with minimal additional delay and Overhead.

4. CONCLUSION

In this paper, we discuss the security issues in a MANET related to black hole attack. This type of attack can be easily deployed in MANET. The black hole node may be single or it may form a co-operative black hole attack. The solution provided in this paper is simulated using a simulator created in java and it demonstrated the detection of black hole attacks in MANET. Once a black hole is detected the node last sending the data packet, stores in it the information about the black hole, so that it doesn't interact with black hole again. Future works can be concentrated on ways to propagate the information about the black hole in the entire network so as to isolate the attacking node.

5. REFERENCES

1. Leela Krishna Bysani and Ashok Kumar Turuk "A Survey On Selective Forwarding Attack in Wireless Sensor Networks" International conference on devices and communications, February, 2011
2. Jatin D. Parmar, Ashish D. Patel, Rutvij H.Jhaveri and Bhavin I. Shah "MANET Routing Protocols and Wormhole Attack against AODV" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010
3. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008
4. SarveshTanwar, Prema K.V. "Threats & Security Issues in Ad hoc network: A Survey Report" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013
5. Sonia and Abhishek Aggarwal "A Review Paper on Pooled Black Hole Attack in MANET"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013
6. Fidel Thachil and K C Shet "A trust based approach for AODV protocol to mitigate black hole attack in MANET" International Conference on Computing Sciences, 2012

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 377 - 380, 2014

Parameter Estimation of Software Reliability Growth Models Using Simulated Annealing Method

Chander Diwaker
UIET
Kurukshetra, Haryana
India

Sumit Goyat
UIET
Kurukshetra, Haryana
India

Abstract: The parameter estimation of Goel's Okomotu Model is performed victimisation simulated annealing. The Goel's Okomotu Model is predicated on Exponential model and could be a easy non-homogeneous Poisson method (NHPP) model. Simulated annealing could be a heuristic optimisation technique that provides a method to flee local optima. The information set is optimized using simulated annealing technique. SA could be a random algorithmic program with higher performance than Genetic algorithmic program (GA) that depends on the specification of the neighbourhood structure of a state area and parameter settings for its cooling schedule.

Keywords: SA, NHPP, SRGM, MVF, FIF.

1. INTRODUCTION

Due to increasing dependence and demand for software system, it's necessary to develop and maintain its reliableness. The system-reliability drawback is that the series-parallel redundancy allocation drawback wherever either system dependability is maximized or total system testing cost/effort is reduced. The keen interest of users in software system reliability models has enhanced since the software system element became a very important issue in several Engineering projects [1]. Reliableness is measured over execution time so it a lot of accurately reflects system usage. Reliability isn't time dependent. Failures occur once the logic path that contains a mistake is executed. Reliableness growth is determined as errors are detected and corrected. During this paper we have a tendency to present an approach to estimate the parameters of Goel's Okomotu Model victimisation simulated annealing. The planned approach provide similar results because the ancient estimation approach victimization the most probability technique while not using info from previous projects, except that the planned approach is far easier to use and no numerical technique is needed.

2. SOFTWARE RELIABILITY GROWTH MODELS

Software reliability growth model could be an elementary technique that asses the reliableness of the software system quantitatively. The SRGM need smart performance in terms of predictability. Any software system needed to control smart reliableness should endure intensive testing and debugging. These processes might be expensive and time intense and managers still need correct info associated with however software system reliability grows. SRGMs will estimate the amount of initial faults, the software system reliability, the failure intensity, the mean time-interval between failures, etc. These models facilitate to measure &amp; track the expansion of reliability of the software system as software system is improved [7]. Within the literature survey of SRGM, solely random processes like NHPP, S-shaped, Exponential, etc., are considered that model the entire behaviour of the amount of failures as a function of time.

3. GOEL'S OKOMOTU MODEL

This Model is predicated on Exponential model and could be an easy non-homogeneous Poisson process (NHPP) model. Goel-Okumoto (G-O) model curve is incurvature. This model provides an analytical framework for describing the software system failure development throughout testing.

- It is predicated on following observations:-

-Number of failures per unit testing time decreases exponentially.

-Cumulative variety of failures versus check time follows an exponentially growing curve.

- In this model it's assumed that a softwar package is subject to failures haphazardly times caused by faults present within the system

.

$$P\{N(t)=y\} = \frac{(m(t))^y e^{-m(t)}}{y!}, \; y = 0,1,2,\ldots\ldots\ldots$$

Where

$$m(t) = a(1- e^{-bt})$$
$$\lambda(t) = m'(t) = abe^{-bt}$$

Here m(t) is that the expected variety of failures determined by time t and λ(t) is that the failure rate.

Information Requirements:-

- The failure counts in every of the testing intervals i. e. fi

- The completion time of every period that the software package is below observations i. e. ti

The mean value value (MVF)

$$\mu\ (t) = a\ (1\text{-}e^{-bt})$$

The Failure Intensity function (FIF)

$$\lambda(t) = abe^{-bt}$$

Where a is taken because the expected total variety of faults within the software system before testing and b is that the failure detection rate.

4. SIMULATED ANNEALING

Simulated annealing (SA) could be a heuristic improvement model which will been applied to resolve several tough issues within the numerous fields like programming, facility layout, and graph colouring / graph partitioning issues. SA algorithmic program is galvanized from the method of hardening in metal work. SA has its name related to the employment of temperature as a quantity which may be modified based on a cooling schedule used as a tunable algorithmic program parameter . Annealing involves heating and cooling a fabric to {change} its physical properties because of change in its internal structure. Travelling salesman problem is that the best example of this algorithmic program. SA could be a random algorithmic program with higher performance than Genetic algorithmic program (GA) that depends on the specification of the neighbourhood structure of a state area and parameter settings for its cooling schedule. The key algorithmic feature of simulated annealing is that it provides a method to flee native optima by permitting hill-climbing moves i.e. moves that worsen the target operate worth. The value function returns the output f related to a collection of variables. If the output decreases then the new variable set replaces the previous variable set. If the output will increase then the output is accepted

$$R <= e^{[f(p_{old}) - f(p_{new})]/T}$$

$$R <= e^{[f(p_{old}) - f(dp_{old})]/T}$$

Where R could be a uniform random variety and T could be a variable analogous to temperature. The new variable set is rejected. The new variable set if found by taking a random step from the previous variable set

$P_{new} = dp_{old}$

The variable d is either uniformly or unremarkably distributed regarding P previous. This management variable sets the step size so at the start of the method the algorithmic program is forced to form massive changes in variable values. At this time the values of T and d decreases by a definite percent and also the algorithmic program repeats. The algorithmic program stops once T_0. The decrease in T is thought because the cooling schedule. If initial temperature is T0 and also the ending temperature in tn then the temperature at step n is given by

$T_n = f\ (T_0, T_N, N, n)$

Where f decrease with time.

5. LITERATURE SURVEY

.Karambir et al. [1] represented that it's harder to measure and improve the reliableness of internet applications as a result of the big system has extremely distributed nature. Hardware faults might be simply expected instead of the software system faults. During this paper the author used the Goel Okumoto SRGM to observe the amount of faults during a fixed time and estimate its reliableness in regard of internet applications. The speed of modification was calculated by executing the check cases for actual defects per day. The Goel-Okumoto model used exponential distribution to predict the amount of faults in internet applications. This work don't predict the reliability of internet applications that could be a limitation to the present proposed work. Praveen Ranjan Srivastava et al. [2] steered that software system testing could be a crucial a part of the software system Development Life Cycle. The amount of faults occurred and glued throughout the testing section might probably improve the standard of a software package by increasing the likelihood of product success within the market. The method of deciding the time of allocation for testing section is a crucial activity among quality assurance. Extending or reducing the testing time was enthusiastic about the errors uncovered within the software system parts that will deeply have an effect on the general project success. Since testing software system incurs significant project value over-testing the project that resut in higher expenditure whereas inadequate testing would go away major bugs undiscovered resulting in risking the project quality. Therefore prioritizing the parts for checking was essential to realize the optimum testing performance within the assigned test time. This paper conferred a check point Analysis primarily based Module Priority approach to work out the optimum time to prevent testing and unleash the software system. Razeef Mohd et al. [3] planned variety of analytical models throughout the past 3 decades for assessing the reliableness of the software. During this paper the author summarize some existing SRGM give a critical assessment of the underlying assumptions and assess the relevance of those models throughout the software system development cycle using an example. Latha Shanmugam et al. [4] planned that several software system reliableness growth models had been steered for estimating reliableness of software system as software system reliableness growth models. The Functions steered were non-linear in nature therefore it had been tough to estimate the correct parameters. During this paper the discussion includes an Estimation technique supported ant Colony algorithmic program during which parameters were estimated. Using existing ways information sets cannot be obtained wherever as within the planned technique at least one answer might be obtained. The accuracy of the results using planned technique in comparison with PSO algorithmic program has higher accuracy for a minimum of ten times for majority of the models. This work cannot support ways for dividing the answer area and setting the initial worth parameters. D. Haritha et al. [5] steered that the usage of software system reliableness growth model place a really vital role in observation progress accurately predicting the amount of faults within the software system throughout each development and testing method. The high complexness of software system is that the major contributory issue of software system reliableness problem. The amount of faults determined in real software system development surroundings. During this paper the author explore the utilization of particle swarm optimization algorithmic program to estimate software system reliableness growth models parameters. This work didn't develop a polynomial structure model to supply a correct result for the higher model within the computer code reliableness prediction method. Pradeep Kumar et al. [6] planned a NHPP primarily based computer code reliableness growth model for three-tier shopper server systems. The conferred model was composed of 3 layers of client-server design associated with presentation logic, business logic and information keep at backend. Presentation layer contains forms or server pages that presents the program for the applying, displays the information, collects the user inputs and sends the requests to next layer. Business layer, which offer the support services to receive the requests for information from user tier evaluates against business rules passes them to the information tier and incorporates the business rules for the applying. Information layer includes information access logic, information drivers, and query engines used for communication directly with the information store of an information. The limitation of this work is that this algorithmic program didn't have any mechanism once to prevent the testing method and unleash the products to the top user with higher quality inside budget and without any delay. Shih-Wei Lina b et al. [7] steered that Support vector machine (SVM) could be a novel pattern classification technique that's valuable in several applications. Kernel parameter setting within the SVM coaching method beside the feature choice significantly affected classification accuracy. The target of this study was to get the higher parameter values whereas additionally finding a set of options that don't degrade the SVM classification accuracy. This study developed a simulated Annealing (SA) approach for parameter determination and has choice within the SVM termed SA-SVM. To live the planned SA-SVM approach many datasets in UCI machine learning repository are adopted to calculate the classification accuracy rate. The planned approach was compared with grid search that could be a standard technique of performing arts parameter setting and numerous alternative ways. The disadvantage of this analysis is that this cannot be applied on real world issues. Chin-Yu Huang *et al.* [8] steered that Software Reliability Growth Models (SRGM) have been developed to greatly facilitate engineers and managers in tracking and measuring the growth of reliability as software is being improved. However some research work indicates that the delayed S-shaped model may not fit the software failure data well when the testing-effort spent on fault detection is not a constant. Thus in this paper the author first review the logistic testing-effort function that can be used to describe the amount of testing-effort spent on software testing. The author describes how to incorporate the logistic testing-effort function into both exponential- type and S-shaped software reliability models. Results from applying the proposed models to two real data sets are discussed and compared with other traditional SRGM to show that the proposed models can give better predictions and that the logistic testing-effort function is suitable for incorporating directly into both exponential-type and S-shaped software reliability models. Gaurav Aggarwal *et **al.*** [9] categorized Software Reliability Model into two types, one is static model and the other one is dynamic model. Dynamic models observed that the temporary behaviour of debugging process during testing phase. In Static Models, modelling and analysis of program logic was performed on the same code. This paper reviewed various existing software reliability models and there failure intensity function and the mean value function. On the basis of this review a model was proposed for the software reliability having different mean value function and failure intensity function. Lilly Florence *et al.* [10] described that the ability to predict the number of faults during development phase and a proper testing process helped in specifying timely release of software and efficient management of project resources. In the Present Study Enhancement and Comparison of Ant Colony Optimization Methods for Software Reliability Models were studied and the estimation accuracy was calculated. The Enhanced method showed significant advantages in finding the goodness of fit for software reliability model such as finite and infinite failure Poisson model and binomial models.

6. PROPOSED WORK

In Earlier Researches PSO (Particle Swarm Optimization) and ACO (Ant Colony Optimization) algorithmic program are explored to estimate SRGM parameters. These algorithms were accustomed handle the modeling issues for the facility model, the Delayed s-shaped model and also the Exponential model. The planned Model can estimate the parameters victimization Simulated annealing (SA) algorithmic program. Simulated annealing could be a common native search meta-heuristic accustomed address separate and, to a lesser extent, continuous optimization issues. The Simulated annealing algorithmic program is employed to handle these models and can show potential benefits in finding the matter. Initial answer is assumed as ω. The temperature counter is modified and t_k is meant to be the temperature cooling schedule. Assume an initial temperature T and variety of iterations are performed at every tk. choose a repetition schedule Mk that represent the repetition rate of every issue. This simulated annealing formulation leads to M0 + M1 +……….. + Mk total iterations being executed, wherever k corresponds to the value for at that the stopping criteria is met. Additionally if for all k, then the temperature changes at every iteration.

7. CONCLUSION AND FUTURE SCOPE

The optimized result of the proposed model using simulated annealing are far better than optimizing the software reliability models using other techniques such as PSO, ACO, Neural Network. Using PSO it is hard to balance development time and budget with software reliability.The PSO produce good results but the number of iteration were increased which indirectly decreases the efficiency. The SA will increase the efficiency and reliability of the software. The failure rate will be reduced. In future works this technique would be applicable to various real life domains such as biometrics, VLSI design, Data mining etc.

8. REFERENCES

1. Mr. Karambir, Jyoti Tamak “Use of Software Reliability Growth model to Estimate the Reliability of Web Applications” International Journal of Advanced Research in Computer Science and Software Engineering , ISSN : 2277-128X, June 2013, Volume 3, Issue 6, pp:- 53-59.

2. Praveen Ranjan Srivastava, SubrahmanyanSankaran, Pushkar Pandey “Optimal Software Release Policy Approach Using Test Point Analysis and Module Prioritization” MIS Review Vol. 18, No. 2, pp: 19 – 50, March 2013
3. RazeefMohd., MohsinNazir “Software Reliability Growth Models: Overview and Applications” Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 9, pp: 1309 – 1320, SEP 2012
4. LathaShanmugam and Dr. Lilly Florence “A Comparison Of Parameter Best Estimation Method For Software Reliability Models” International Journal of Software Engineering & Applications (IJSEA), Vol.3, No.5, pp:91 - 102, September 2012
5. D. Haritha, T.Vinisha, K.sachin “Detection of reliable software using particle swarm optimization” Vinisha et al, GJCAT, Volume 1 (4), pp: 489-494, 2011
6. Pradeep Kumar and Yogesh Singh “A Software Reliability Growth Model for Three-Tier Client Server System” International Journal of Computer Applications, pp: 9 – 16,2010
7. Shih-Wei Lina,b , Zne-Jung Lee b, Shih-ChiehChenc and Tsung-Yuan Tseng “Parameter determination of support

8. vector machine and feature selection using simulated annealing approach” Applied Soft Computing 8, pp: 1505–1512,2008

9. Chin-Yu Huang, Sy-Yen Kuo, “An Assessment of Testing-Effort Dependent Software Reliability Growth Models” IEEE Transactions On Reliability, ISSN :0018-9529,June 2007, Vol. 56, No. 2, pp:- 198-211

10. Gaurav Aggarwal and Dr. V.K Gupta “ Software Reliability Growth Model” International Journal of Advanced Research in Computer Science and Software Engineering, January 2014,Volume 4, Issue 1,pp :- 475-479,

11. Lilly Florence, Latha Shanmugam “Enhancement And Comparison Of Ant Colony Optimization For Software Reliability Models” Journal of Computer Science 9 (9), ISSN: 1549-3636, 2013,pp: 1232-1240.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 381 - 384, 2014, ISSN: 2319–8656

Various Clustering Techniques in Wireless Sensor Network

Mamta
Geeta Institute of Management and Technology
Kurukshetra University
Kurukshetra, Haryana
India

Abstract: This document describes the various clustering techniques used in wireless sensor networks. Wireless sensor networks are having vast applications in all fields which utilize sensor nodes. Clustering techniques are required so that sensor networks can communicate in most efficient way.

Keywords: wsn, wireless sensor networks, clustering, weight based clustering ,leach, Network.

1. INTRODUCTION

A wireless sensor network [1] can be an Unstructured or Structured network. An unstructured network does not have a fix topology. A structured network have a fix topology.WSN are unstructured network because sensors keep on changing their location continuously. WSN can efficiently create routes among the nodes of a network. A WSN can be static and dynamic depending upon nature of route created. In static network, the configuration of nodes is done manually. Network administrator makes these entries in a static table and routers uses entries from these routing table for performing their routing function well. In dynamic networks all configuration is made dynamically by a dynamic routing protocol. Node can leave and join the network dynamically at run time. As sensors in wireless sensor network changes there location constantly, so arranging a communication system for them is a typical task. To resolve this problem clustering algorithms for WSN are proposed which provides a structured way of communication for unstructured WSN. This algorithm divides WSN nodes into clusters choosing a cluster head for each node which performs data aggregation and data processing task for whole cluster thus saving energy. Cluster head thus consume more energy than other nodes.

Clustering is the activity [5] of creating sets of similar objects. Various researches are performed on clustering. Nodes in a clustered wireless sensor network can also be classified as primary nodes and secondary nodes. Primary nodes can perform data aggregation and data processing function instead secondary nodes only performs data forwarding functions.

Clustering increases the network scalability and life. It makes distribution control over the network more diverse. It saves energy by distributing load by making intelligent decision. Nodes having high energy are allocated more loads thus increasing the lifetime of the network. The clustering is done in such a way that data has to travel minimum. Only cluster heads communicates with cluster head thus reducing the data redundancy which usually happens when each node perform its own data aggregation and transmission [8] function separately. This algorithm provides very efficient way of communication in sensor networks. Such algorithm creates easy to maintain algorithms. Clustering in WSN network makes them suitable for use in uneven environments.

In this paper we will perform a survey on wireless sensor network with dynamic capability. Topic is less frequently discussed through surveys. We will see each clustering algorithm developed for wireless sensor networks with dynamic capability.

2. TYPES OF CLUSTERING ALGORITHMS

A. *Event-to-Sink Directed Clustering*

Event-to-Sink Directed Clustering is another type of protocol which provides high efficiency in terms of energy consumption. When a node discovers an event, it sends its report to sink. A sensor node sends this collected data to cluster head thus avoiding redundancy. This technique provides two new improvements:

1. Clustering is only performed when an event occurs, so no unnecessary clustering rounds need to perform.

2. There is minimum movement of data in the cluster because clusters are form in the direction from event to sink.

3. Cluster heads are selected from up-stream nodes and non-cluster nodes are selected from downstream nodes. So flow of data is almost one directional.

The author Alper Bereketli,Ozgur B. Akan [2] has evaluated the performance of Event-to-Sink Directed Clustering algorithm in his paper ”Event-to-Sink Directed Clustering in Wireless Sensor Networks” and compared it with LEACH algorithm. They kept total reporting nodes and total nodes in the ratio of one third.They analyzed that per hop delay in Event-to-Sink Directed Clustering in Wireless Sensor Networks was around 200 ms as compared to LEACH which has a 460 ms delay almost double of Event-to-Sink Directed Clustering.

B. Load balanced clustering scheme

Another algorithm called load balanced clustering scheme was proposed by Shujuan Jin, Keqiu Li [8]. Whole heavy tasks of a network are performed by cluster head. This much excessive load can kill it by consuming all of its energy. In load balanced clustering scheme an assistant node is selected to help the cluster head to perform its data aggregation and data processing task. Assistant node transmits the data to base station. Cluster head process the received data and sends it to assistant node. Assistant node sends this data to base station.Multi hop data transmission is used to avoid early death of assistant node.

Disadvantage of this scheme is that data flow among nodes is not uniform. Nodes closer to base station receives more data than nodes which are farther away. So closer nodes consumes excessive energy hence get depleted very soon.

C. K-means algorithm

K-means algorithm [5] was another Clustering algorithm which uses following two factors as its selection criteria for a cluster head:-

1. Euclidian distances

2. Residual energies of nodes.

All nodes send their data to a central node which stores this information in a list. After it has collected data from all its nodes it performs the k-mean clustering algorithm.

This technique works better when clustering is performed by distributed method instead of doing it centrally. If central node is installed at one place, whole system will break down if this node got failed. In distributed computing even if a single node fails it cannot harm other nodes.

There are more chances of packet loss in centralized system since if packet is lost; it has no other copy to reach other nodes. In distributed System, even if a packet to a node fails, node will get it through any another way since in distributed network every node in receiving range broadcasts its packets to its neighbors.

To enhance the efficiency [6] of clustering in wireless sensor networks, another technique is used is which is called capability of energy harvesting. Nodes that have the capability of energy harvesting can generate energy from various sources like sun, water and air etc.As nodes are charged again and again by using conventional sources of energy so they never go out of energy. However it is not feasible to embed capability of energy harvesting in all nodes of a wireless sensor network due to various infrastructural limitation. So nodes with energy harvesting capability are evenly distributed in wireless.

The nodes with harvesting capability cannot be elected as cluster heads since they are highly dependent on nature for their source of energy which is not a reliable source of energy. But these nodes can be made to serve as relay nodes between cluster head and base station. Pengfei Zhang, Gaoxi Xiao and Hwee-Pink Tan (2011) in their paper “A Preliminary Study on Lifetime Maximization in Clustered Wireless Sensor Networks with Energy Harvesting Nodes” has proposed an algorithm called single cluster algorithm. This algorithm selects the optimal position of cluster head. Position of cluster head is made to choose in such way that it maximizes its battery lifetime. They then observed the effect of installing the energy harvesting relay nodes between cluster heads and base station. There algorithm which has utilized the use of energy harvesting node has increased the lifetime of network by approximately 8.59%.However algorithm worked for single cluster only.

The normal notion of network lifetime [9] is time consumed until first now in the network becomes dead. However this notion does not go well with wireless sensor network’s lifetime. Since nodes in the wireless sensor are not even in terms of energy. Cluster heads consumes high energy instead of non-cluster heads which uses comparatively less energy than cluster heads. Network lifetime of a wireless sensor network can be better defined in terms of time for which a cluster has worked properly. However only network lifetime does not serve as better criteria for evaluating the performance of the network. Other factors like amount of data gathered also plays a key role. Tianqi Wang, Wendi Heinzelman, and Alireza Seyedi has proposed a new optimization technique in their paper,” Maximization of Data Gathering in Clustered Wireless Sensor Networks for maximizing the amount of data gathered during the lifetime of a network.

D. Low-Energy Adaptive Clustering

Low-Energy Adaptive Clustering [10] is one of the milestones in clustering algorithms. The aim of Low-Energy Adaptive Clustering was to select nodes as cluster heads in such a way that every node gets a chance to become cluster head. As cluster head consumes higher energy then non cluster heads, so load is evenly distributed among nodes. So a single node does not go out of energy after a short time span just because it was frequently elected as cluster head.

Low-Energy Adaptive Clustering involves two phases of operation

1. Set up phase
2. Steady state phase

In Set-up phase clusters are made and a cluster head is selected for each cluster. Cluster head is selected based upon a probabilistic factor. Probably of a node to become a cluster head is calculated on the basis of two factors which are as follows:

1. Number of times a node has been a cluster head.
2. Suggested total number of cluster heads for a network.

If the value of probabilistic factor for a node is less than threshold, then it is elected as cluster head.

In steady state phase all data collected by cluster heads is sent to base station.

Disadvantage of Low-Energy Adaptive Clustering is that it does not consider initial energy as a factor to elect cluster head. So Nodes which have become cluster heads for same number of time as others but have less initial energy than other nodes are likely to become dead sooner than nodes which have high initial energies. The algorithm does not work well with large sized sensor networks since algorithm utilizes the single-hop inter-cluster technique which is not optimal for large size networks.

E. Hybrid Energy-Efficient Distributed clustering

Hybrid Energy-Efficient Distributed clustering considers two factors to decide whether to make a node cluster head or not. These are as follows:

1. Residual Energy
2. Intra-cluster communication cost

The main goal of Hybrid Energy-Efficient Distributed clustering is that all the cluster heads in the network get uniformly distributed.

Algorithm conserves more energy and is more scalable.

The disadvantage of Hybrid Energy-Efficient Distributed clustering is that sometimes it elects extra cluster heads. As cluster heads consumes more energy so efficiency of network considerably decreases. Also it consumes large bandwidth since it takes a lot of iterations to make clusters and a lot of packets are broadcast during each iteration.

F. Energy Efficient Hierarchical Clustering

Energy Efficient Hierarchical Clustering [3] is a probabilistic clustering algorithm. Algorithm was a extended version of LEACH with multiple hope architecture.

At first each node decides whether it can become cluster head or not. If it became cluster head it advertises its presence to all its neighbor nodes. The cluster head is now called volunteer cluster head. All nodes that are not k-hop farther away from cluster head receives all messages from cluster head. Any node which is not a cluster head if receives this advertisement message becomes a member of cluster head from which it has received its advertisement.

G. Weight-Based Clustering Protocols

In weight based clustering protocols, Weight is used as criteria for election of cluster head. This weight can be measured in terms of many factors like residual energy and distance of nodes from cluster head or no of times a node has become cluster head depending upon the algorithm. Each node calculates its weight in each iteration of clustering. Clusters are formed in such a way that minimum energy consumption occurs in a wireless sensor network.

Weight Based Clustering [7] is a clustering technique for heterogeneous networks. It chooses the better cluster heads thereby increases the lifetime and throughput of WSN by its efficient clustering algorithm.

The goals of Weight Based Clustering is as follows

i. To increases the life of sensor nodes by electing sensor nodes which has high residual energy.
ii. To avoid the election of low energy sensor nodes as cluster heads.

Weight Based Clustering algorithm chooses cluster head in such a way that cluster head always has highest residual energy. Residual energy is energy left in a node after performing its processing and data transferring functions. It avoids the selection of low energy sensor nodes as cluster heads. It upgrades the life time of wireless sensor network. Other than residual energy it also considers other factors like number of live neighbors and distance from base station to elect the cluster head.

If the energy of the sensor node is greater than residual energy it is elected as a cluster node otherwise it is considered as a normal node. A sensor node is considered dead if its energy drops below a particular threshold level.

Every node broadcast an “I am alive” message after each clustering round. Thus it calculates the number of live neighbors of each node. Then it calculates the residual energy of each node using first order radio energy model. Node having highest residual energy is elected as cluster head.

But this scheme has a disadvantage that it unnecessarily elects extra cluster heads. As cluster heads consume more energy so somehow it degrades the efficiency of network.

3. CONCLUSION

In all clustering techniques, Weight based clustering technique is best. Weight based clustering technique is more efficient. There is less number of dead nodes as compared to other clustering techniques. Also first dead takes considerable delay. Technique also perform better in dynamic networks. But this technique sometimes generates unnecessarily extra cluster heads.

4. REFERENCES

1. A.K.M. Muzahidul, Jalan Semarak (2013),*"Communication Protocols on Dynamic Cluster-based Wireless Sensor Network* ",978-1-4799-0400-6/13/$31.00 ©IEEE.
2. Alper Bereketli,Ozgur B. Akan (2009),*"Event-to-Sink Directed Clustering in Wireless Sensor Networks"* ,Next generation Wireless Communications Laboratory (NWCL) Department of Electrical and Electronics Engineering Middle East Technical University, Ankara ,Turkey, 06531 978-1-4244-2948-6/09/$25.00 © IEEE.
3. Basilis Mamalis, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou," *Clustering in Wireless Sensor Networks*", Zhang/RFID and Sensor Networks AU7777_C012 Page Proof Page 324 2009-6-24.
4. G.Y. Durga Devi (2013),*"Clustering Algorithms In Wireless Sensor Networks-A Survey*, ISSN (Online): 2347-2820, Volume -1, Issue-2.
5. P. Sasikumar ,Sibaram Khara (2012)," K-Means Clustering In Wireless Sensor Networks", 978-0-7695-4850-0/12 $26.00 © 2012 IEEE DOI 10.1109/CICN.2012.136.
6. Pengfei Zhang, Gaoxi Xiao and Hwee-Pink Tan(2011) ,*"A Preliminary Study on Lifetime Maximization in Clustered Wireless Sensor Networks with Energy Harvesting Nodes"*,978-1-4577-0031-6/11/$26.00 © IEEE
7. Ravi Tandon, Biswanath Dey and Sukumar Nandi (2013)," *Weight Based Clustering In Wireless Sensor Networks"*, 978-1-4673-5952-8/13/$31.00 © IEEE.
8. Shujuan Jin, Keqiu Li (2009)," *LBCS: A Load Balanced Clustering Scheme in Wireless Sensor Networks"*, Third International Conference on Multimedia and Ubiquitous Engineering, 978-0-7695-3658-3/09 $25.00 © 2009 IEEE DOI 10.1109/MUE.2009.47.
9. Tianqi Wang, Wendi Heinzelman, and Alireza Seyedi (2010)," *Maximization of Data Gathering in Clustered Wireless Sensor Networks"*,978-1-4244-5638-3/10/$26.00 ©IEEE.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 385 - 389, 2014, ISSN: 2319–8656

Parallel Implementation of Travelling Salesman Problem using Ant Colony Optimization

Gaurav Bhardwaj
Department of Computer Science and Engineering
Maulana Azad National Institute of Technology
Bhopal, India

Manish Pandey
Department of Computer Science and Engineering
Maulana Azad National Institute of Technology
Bhopal, India

Abstract: In this paper we have proposed parallel implementation of Ant colony optimization Ant System algorithm on GPU using OpenCL. We have done comparison on different parameters of the ACO which directly or indirectly affect the result. Parallel comparison of speedup between CPU and GPU implementation is done with a speed up of 3.11x in CPU and 7.21x in GPU. The control parameters α, β, ρ is done with a result of best solution at 1, 5 and 0.5 respectively.

Keywords: Travelling Salesman Problem, Ant colony optimization, parallel, OpenCL, GPU.

1. INTRODUCTION

Travelling salesman problem [1] is an NP-hard problem in a set of combinatorial optimization problem. In travelling salesman problem we have to found a Hamiltonian circuit having minimum total edge weight. TSP has various applications such as JOB Scheduling, DNA sequencing, designing and testing VLSI circuits, graph coloring, vehicle routing etc. There are various methods to solve such type problems such as ANT colony optimization, neural network, Genetic algorithm etc.

ACO [2] is a heuristic algorithm for solving combinatorial optimization problem. ACO imitates the behavior of real ants to search food. Ants communicate indirectly to the agents of their colony with a trail of a chemical substance called pheromone. Pheromone is a chemical substance that shows the trace of an ant. Other ants follow the smell of the food and the trace of the pheromone to find out the minimum distance to the food.

Complex problem such as TSP needs huge computational power as well as time to solve. It takes lots of time for a single processor to solve such large problems single handedly.ACO can be implemented parallel with high efficiency.[4] Parallel computing is the new paradigm to solve such type of problems using General Purpose Graphical Processing Unit. GPUs are meant to do graphical processing such as simple arithmetic operations also on graphics in the form of matrices. So we can utilize GPUs processor to solve our problem to speed up the computational time.

GPU [9] consist of large no. of processors embedded together in a chip to perform a specific type of operations. Open CL [10] (OPEN Computing Language) is the framework used to write programs that can be executed on heterogeneous platforms.

This paper applies ACO to the Travelling Salesman Problem in heterogeneous platform using OpenCL framework to achieve parallelism in ACO. We have compared the time taken in sequential as well as the parallel program used to solve this problem with some standard graphs. [11]

In section 2 previous sequential approaches for ACO has been discussed with travelling salesman problem. In section 3 Travelling salesman problem with different approaches to solve this problem is discussed. Section 4 gives the briefing of the Ant Colony Optimization algorithm. Section 5 gives the parallel approach to solve TSP using ACO on GPU. Section 6 gives the experimental comparison with different parameters.

2. RELATED WORK

Travelling salesman problem is one of the oldest mathematical problems in history. Scientist had a great interest to solve such type of problem using different approaches. M.Dorigo and T.stizzle in 1992 [6] has designed an biological approach to solve such type of combinatorial optimization problem such as Travelling Salesman Problem called ACO. The first ACO algorithm was proposed by them called Ant System basic approach on ACO. Then many other algorithm were proposed based on it such Max-Min approach, Ant colony System. All these approaches are successors of Ant system. M.Dorigo has given the basic parallel approach to solve ACO parallel as he has discussed the basic parallel behavior of ants in real life. There after many parallel approaches has been delivered with the parallel strategies. This paper describes the parallel implementation of ACO on heterogeneous platform using OpenCL and comparing their parameters.

3. TRAVELLING SALESMAN PROBLEM

Travelling Salesman Problem represents a set of problem called combinatorial optimization problem. In TSP a salesman is given a map of cities and he has to visit all the cities exactly once and return back to the starting city with the minimum cost length tour of all the possible tour present in that map. Hence the total no. of possible tour in a graph with n vertices is (n-1)! .

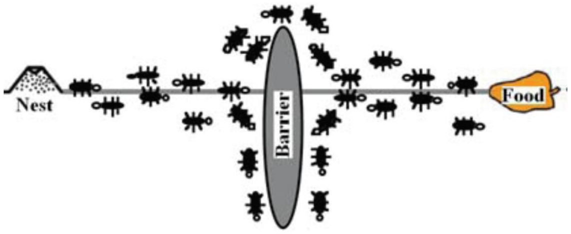
There are various approaches to solve TSP. Classical approach to solve TSP are dynamic programming, branch and bound which uses heuristic and exact method and results into exact solution. But as we know TSP is an NP-hard problem so the time complexity of these algorithms are of exponential time. So they can solve the small problem in optimal time but as compared to the large problem time taken by these algorithms are quite high. So no classical approach can solve this type of problem in reasonable time as the size of the problem increases complexity increases exponentially.

So many alternate approaches are used to solve TSP which may not give you the exact solution but an optimal solution in reasonable time. Methods like nearest neighbor, spanning tree based on the greedy approach are efficiently used to solve such type of problems with small size. To overcome this different other approaches based on natural and population techniques such as genetic algorithm, stimulated annealing, bee colony optimization, particle swarm optimization etc. are inspired from these techniques.

4. ANT COLONY OPTIMIZATION

ANT colony optimization [5][6] technique introduced by Marco Dorigo in 1991 is based upon the real ant behavior in finding the shortest path between the nest and the food. They achieved this by indirect communication by a substance called pheromone which shows the trail of the ant. Ant uses heuristic information of its own knowledge the smell of the food and the decision of the path travelled by the other ants using the pheromone content on the path. The role of the pheromone is to guide other ants towards the food.

Ant has the capability of finding the food from their nest with the shortest path without having any visual clues. At a given point where there are more than one path to reach to their food then ants distribute themselves on different paths and the path and lay pheromone trace on that path and return with same path. Thus the path with minimum distance will acquire more pheromone as compared to other paths as the ants will return faster from that path comparative to the other path. So the new ants coming in the search of food will move with probability towards the path having higher pheromone content as compared to the path having lower pheromone content and in the end all the ants will move towards the same path with the minimum shortest path to their food. Now figure 1 shows the behavior of ants going from the upward direction will return early as compared to the ants going from the downward direction so the pheromone content in the upward direction is more as compared to the downward direction due to that in the end all the ants will start moving towards the upward direction which is the shortest path to their food.



Group Fig 1: shows the behavior of real ants.

ACO uses the set of artificial ants which co-operate each other to solve the problem and find the optimal solution of the problem. ACO can be used to solve combinatorial optimization problems such as Travelling Salesman Problem, Vehicle Routing, Quadratic Assignment, Graph Coloring, Project Scheduling, Multiple Knapsack etc. maximum of the problems are NP-hard problem [3] i.e. they take exponential time complexity in their worst case.

In the travelling salesman problem we are given with a set of cities and the distance between them. We have to found a shortest tour such that each city should be visited exactly once and then return to the stating city. Formally we can say that we have to found a minimal Hamiltonian circuit in a fully connected graph.

In ACO we stimulate no. of artificial ants on a graph where each vertex represents the city and the edge represents the connection between the two cities [7]. Pheromone is associated with each edge which shows the trace of the ant can be read and modified by the ants. It is an iterative algorithm where no. of ants is used to construct a solution from vertex to vertex without visiting any vertex more than once. At every vertex ant select the next vertex to be visited stochastically that is based upon the pheromone as well as the heuristic information available to it.

```
ACO algorithm
set parameters and pheromone value
            while termination condition not met do
            construct Ant solutions
            update pheromone
endwhile
```

in the above algorithm artificial ants will construct a solution. Ants start with an empty partial solution. At each iteration partial solution is modified by adding a set of components and updating the pheromone content. Creating a solution is completely based on a probabilistic stochastic mechanism. Updating pheromone value means increasing the pheromone content on the edges having good solution in order to find the optimal solution.

4.1 Ant System

Ant system was the first algorithm proposed under ACO to solve TSP problem [8]. In this algorithm all the ants update their pheromone values after completing a solution. In the construction of a solution an ant chooses next node to be visited using a stochastic mechanism. An ant k at city i has not visited set of cities S_p then P_{ij} be the probability to visit edge k after edge i.

$$P_{ij}^{k} = \begin{cases} \frac{\tau_{ij}^{\alpha}\eta_{ij}^{\beta}}{\sum_{j\epsilon S_p}\tau_{ij}^{\alpha}\eta_{ij}^{\beta}} & if\ j\epsilon S_p \\ 0 & \end{cases} \qquad (1)$$

S_P represents the set of cities which has not been visited yet and to be visited again so that the probability of the ant visiting a city which has already visited becomes 0. Where τ_{ij} is the pheromone content on the edge joining node i to j . η_{ij} represents the heuristic value which is inverse of the distance between the city i to j, which is given by:

$$\eta_{ij} = \frac{1}{d_{ij}}$$

Where d_{ij} is the distance between the city i to j. α and β represents the dependency of probability on the pheromone content or the heuristic value respectively. Increasing the value of α and β may vary the convergence of ACO.

After solution construction we have to update the pheromone accordingly, as follows:

$$\tau_{ij} \leftarrow (1-\rho).\tau_{ij} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k}$$

Where ρ is the evaporation rate, *m* is the number of ants, and $\Delta\tau_{ij}^{k}$ is the quantity of pheromone laid on edge(i,j) by an ant k:

$$\Delta\tau_{ij}^{k} = \begin{cases} {}^{Q}/_{L_k} & if\ ant\ k\ uses\ edge\ (i,j) in\ its\ tour, \\ 0 & otherwise \end{cases}$$

Where Q is a constant and L_k is the length of the tour constructed by an ant k.

5. PARALLEL IMPLEMENTATION OF ACO ON TSP

The main purpose of this section is to show parallel implementation of ant system for TSP. Biologically ants use parallel approach in search of their food. Ants perform task based parallelism to search their food. All the ants search their food parallel simultaneously and synchronize with the help of the pheromone content in the ground similarly we can use this approach in artificial ants in ACO [12]. Parallel model used in ACO is a master/worker paradigm. Where master controls the workers by communicating and capturing the global knowledge where as worker implements the search. In this model same copies of the ant system algorithm are simultaneously and randomly executed using different random source.

ACO is an iterative approach where at each iteration master shares the global knowledge of pheromone to its worker ants to construct a solution. When 1000 of ants perform the search operation then the solution construction becomes comparatively fast as compared to sequential implementations. Parallelism where large number of threads can be executed simultaneously can be done using GPGPU (general purpose graphical processing unit). GPU [9] consist of hierarchy of processing elements and their memory. An AMD GPU consist of more than one SIMD (single instruction multiple data) computation engine. Where each computation engine consists of multiple thread processor which executes same instruction all the time simultaneously but data items may vary. Where each thread processor have their own L1 cache. Each thread processor is a four or five way VLIW (very large instruction word) processor consisting of four or five ALUs respectively. Parallelism can be attained at both the level of thread processor and ALUs.

The two main steps of the ACO solution construction and pheromone updating are thoroughly discussed.

5.1 Solution construction Kernel

In solution construction task based parallelism approach is used as each ant performs their task independent of each other to find the best tour. As we have discussed earlier in this phase ants are allocated the source node randomly and they have to visit each node exactly once and have to reach back to their source node. On each iteration they have to choose their next node using probabilistic stochastic mechanism. This phase has inbuilt parallelism at the level of each ant as the biological ant find their tour. Each ant can be identified as a thread to construct the solution.

```
SOLUTION_CONSTRUCTION(weight_a,  pheromone_p)
Source=get_global_id(0)
Length=0
Initialize all the nodes unvisited;
I=source
Starting from source while all the nodes visited do
        For every unvisited node j from the current node i
                Calculate the node with the max probability using (1)
        Visit the node j with max probability
        Length=length +weight_a_{ij;}
        Mark j as the node traversed
        Enter j in the tour
        i=j
Enter source node in to the tour
Length = length + $a_{j\ source}$
```

Solution construction kernel calculate the heuristic information to visit city j from the city i. computationally it is expensive to construct a solution a with a order of time complexity (n^2). However this kernel has memory related issues to maintain the ant memory for the tour constructed, visited node, weight matrix and pheromone matrix. This type of approach is basically suitable for the problems having large no. of cities. Maximum number of threads can be produced in this problem is equal to the no. of cities. Problem having less no. of cities will have less threads and less parallelism which leads to improper utilization of GPU resources.

5.2 Pheromone Update Kernel

It is a data parallelism approach where all the threads are performing the same task on different data sets. Pheromone update consist of pheromone evaporate and pheromone update. Pheromone evaporation can be done simultaneously to each edge parallel as data parallelism with respect to other edge as there is no relevance in evaporation. For pheromone evaporation we call N no. of thread for each row of our pheromone matrix and the pheromone is evaporated parallel. The work group for pheromone evaporation is of size N. Whereas pheromone is updated using a kernel where the tour of the ant is passed and the length of the tour so for every node the pheromone content is updated. Size of the workgroup for the pheromone update is also of size N.

```
Pheroemene_update(pheromone_p,length,tour)
Q=1/length
for(k=0;k<N;k++)
        i=tour[k]
        j=tour[k+1]
        pheromone_$p_{ij}$=pheroemene_$p_{ij}$*Q
```

However this kernel has synchronization related issues which can be handled using barriers such as pheromone can be updated by an ant after the construction of solution only, no ant can update the pheromone before construction of solution.

6. COMPARATIVE ANALYSIS AND PERFORMANCE EVALUATION

We implemented the algorithm sequential as well as parallel to check the speedup of the algorithm to find the solution. We have also parameterized all the parameters using different values so as to find the best parameters for our solution.

6.1 Comparison of different values for the parameters

ACO depends directly or indirectly on differne parameters such as α,β,ρ etc. these parameters affect the probability of the stochastic mechanism in finding the next node to be visited.

Parameter α shows the dependency of the pheromone to find the next city to visit. If the value of α is too high then it shows the dependency of the algorithm on the pheromone value which may lead to an suboptimal result as the new ant will follow the path followed by the previous ants leads to the initial stagnation. Whereas very low value of α shows the low dependency of the algorithm on the pheromone content which may lead to follow the path with the nearest neighbor. Acc. experiment we concluded that the value of α should be nearly equivalent to 1 as shown in figure.

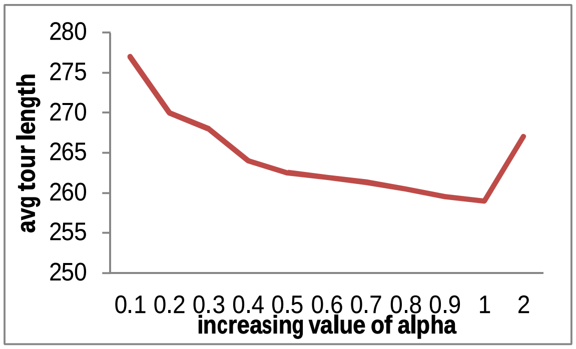


Fig 2 Graph showing the avg. tour length on increasing value of α.

Parameter β shows the dependency of the algorithm on the heuristic value. Similarly if the value of β is too high than it shows that the algorithm depends upon the heuristic value and it will choose the next city with a minimum distance where as if it is too low than only pheromone amplification is at work. Acc. to experiment we concluded that the value of α should be nearly equivalent to 5 as shown in figure as it is giving the best tour length.

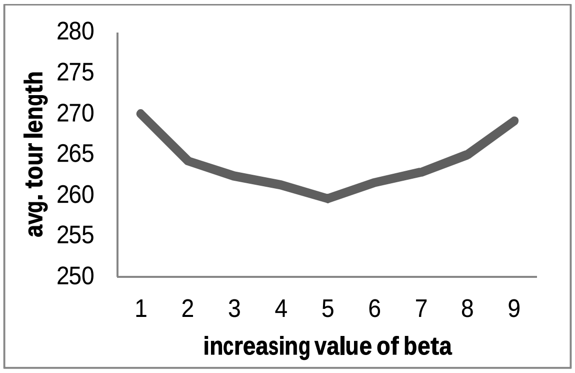


Fig 3 Graph showing the avg. tour length on increasing value of β.

ρ is the evaporation rate of the pheromone. Pheromone evaporation is necessary in ACO as if we will not evaporate the pheromone content than it may lead to the problem of stagnation. As the initial pheromone update may lead to the suboptimal solution. High pheromone evaporation rate (ρ) doesn't affect the pheromone content as the change is too less. Whereas lower value of ρ leads to the negative affect for the pheromone content as it becomes too low to be recognized.

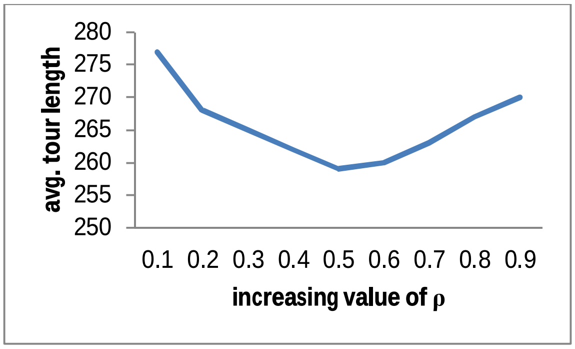


Fig 4 Graph showing the avg. tour length on increasing value of ρ.

6.2 Speedup Comparison

OpenCL parallel implementation on CPU and GPU are tested on the following hardware specifications:-:

AMD Radeon HD 6450(GPU): 2 Compute units, 625 MHz clock, 2048MB Global Mem., 32KB Local Mem., 256 work group size on a system having Intel Core i5 CPU 650 @ 3.2 GHz and 2048MB RAM with AMD APP SDK v2.8.

We have implemented ACO sequentially on the above given hardware specification with a randomly generated graph with different no. of nodes as well as some standard graphs to compare our results. Comparative analysis of the speed up of graph is shown with the sequential, CPU parallel and GPU parallel. In GPU parallel we have considered only the kernel execution time.

Fig 5 shows the speedup between sequential, CPU parallel and GPU parallel. In CPU parallel we have used OpenCL platform to rum the algorithm on CPU parallel. In GPU parallel same program is implemented on GPU. With respect to that we are able to achieve 3.11 times speed up in CPU and up to 7.21 times speed up in GPU.

7. CONCLUSION AND FUTURE WORK

All the parameters of ACO in ant system is been investigated to their best values as α=1, β=5 and ρ=0.5. parallel implementation is done on CPU and GPU using OpenCL. Where GPU parallelization has given best results with a speed up of . we will look for hybrid implementation of ACO on GPU with overcoming the limitation of GPU by utilizing the resources properly with data fragmentation and to optimize our algorithm to gain more speedup.

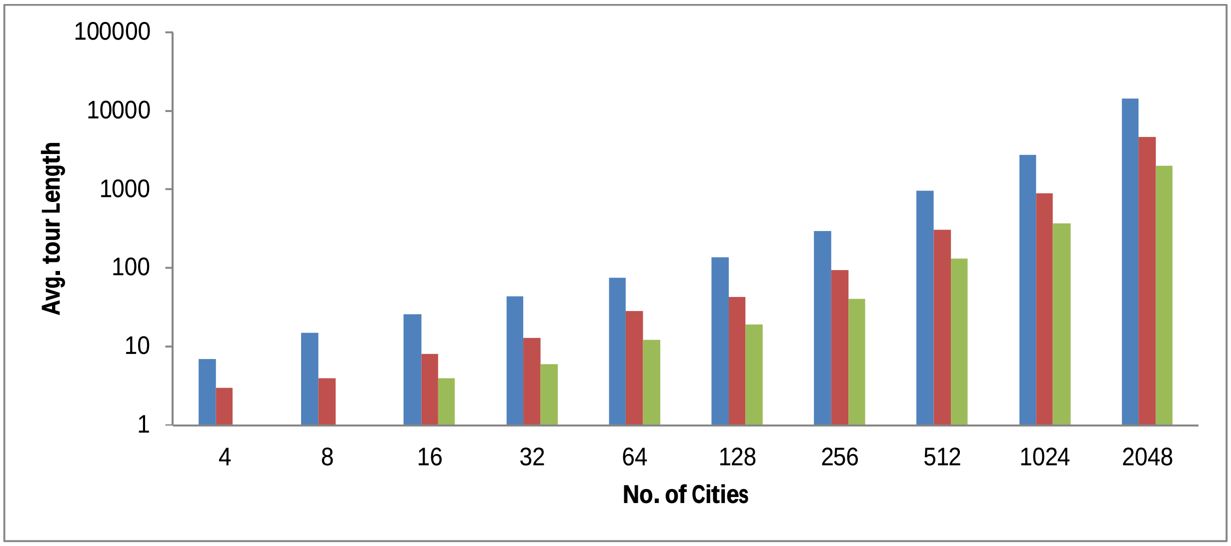


Fig 5 Shows the speed up between sequential, CPU parallel and GPU parallel

8. REFERENCES

[1] E.Lawler, J.Lenstra, A.Kan, and D.Shomsys Wiley New York, 1987 The Travelling Salesman Problem

[2] M.Dorigo and T.Stizzle : Bradford Company 2004. Ant Colony Optimization.

[3] C.Blum. Physics of life reviews, vol. 2, no.4, pp. 353-373, 2005. Ant colony optimization: Introduction and recent trends.

[4] Y-S. You. Genetic and Evolutionary computation, 2009. Parallel ant system for Travelling Salesman Problem.

[5] K.D. boese , A.B. Kahng, and S.Muddu .Operations Research letters ,16:101-113,1994. A new adaptive multistart technique for combinatorial global optimization.

[6] M. Dorigo. PhD thesis, Politecnico di Milano, 1992. Optimization, Learning, and Natural Algorithms

[7] T. Stizzle and H. H. Hoos. Future Generation Computer Systems, vol. 16, no8, pp. 889–914, 2000. MAX–MIN ant system

[8] M. Dorigo and T. Stizzle, A Bradford Book,2004. Ant Colony Optimization.

[9] Ying Zhang. PHD Thesis 2006. Performance and power comparisons between fermi and cypress GPUs.

[10] A. Munshi, B. R. Gaster, T.G. Mattson, J. Fung, D. Ginsburg, Addison-Wesley pub., 2011. OpenCL Programming Guide.

[11]] G. Reinelt, ORSA Journal on Computing, vol. 3, pp. 376–384, 1991. Tsplib–a traveling salesman problem library.

[12] M. Manfrin, M. Birattari, T. Stizzle, and M. Dorigo. 5th International Workshop on Ant Colony Optimization and Swarm Intelligence, vol. LNCS 4150. Springer-Verlag, 2006, pp. 224–234. Parallel ant colony optimization for the traveling salesman problem.

Design and Implementation of Refresh and Timing Controller Unit for LPDDR2 Memory Controller

Sandya M.J
Dept. of Electronics and communication
BNM Institute Of Technology
Bangalore,India

Chaitra .N
Dept. of Electronics and communication
BNM Institute Of Technology
Bangalore,India

Ramudu B
Graphene Semiconductor India Pvt Ltd
Bangalore,India

Abstract: this paper presents a “Implementation of “Refresh And Timing Controller” unit for low power double data rate 2 memory controller (LPDDR2 MEMORY CONTROLLER). “Refresh and Timing Controller” unit plays a vital role for LPDDR2 memory controller .It maintains different timing parameters to handle various commands for memory like refresh, read and write operations and also performs Memory Initialization. Since it is low power DDR2 the maximum duration in power-down mode and deep power down mode is maintained by “Refresh and Timing Controller” unit. The refresh rate period is programmable using the Refresh Period Register. It supports “All Bank Refresh”. The unit has timers to accommodate Refresh, Read/Write, and Power down modes. The RTL is done using the System Verilog. The design is simulated

Keywords: LPDDR2 MC; Design; Device initialization**;** Refresh requirement;Timing parameters

1. INTRODUCTION

Embedded systems usually have a limited amount of memory available; this is because of cost, size, power, weight or other constraints imposed by the overall system requirements. It may be necessary to control how this memory is allocated so that it can be used effectively. Handheld device like mobile, tablet etc are battery operated. For long time battery lasting better power optimization is required in those devices. Nowadays the devices are having multiple masters and share common memory for their applications. LPDDR2 is better fit for these kinds of devices. LPDDR2 memories consume low power. LPDDR2 memory controller accepts write/read commands from multiple masters and generates memory related commands. Functions of memory controller are

□ solves different bandwidth requirement issues
□ handles the “refresh” cycle for Memory.
□ handles read and write operations with bank/row/column addressing.

Since these memories are made with capacitors, charge will leak continuously so refreshing is required memory controller will generate refresh commands as specified in JEDEC specification. For each refresh in a LPDDR2 row, the stored information in each cell is read out and then written back to itself as each LPDDR2 bit read is self-destructive. The refresh process is inevitable for maintaining data correctness, unfortunately, at the expense of power and bandwidth overhead.

This paper is organized as follows. The brief introduction to **“Refresh And Timing Controller”** “is given in section 2 describes top module of**“ Refresh And Timing Controller”**, section 3 describes the implementation of **“Refresh And Timing Controller”** for LPDDR2 memory controller. Section 4 describes the result and analysis.

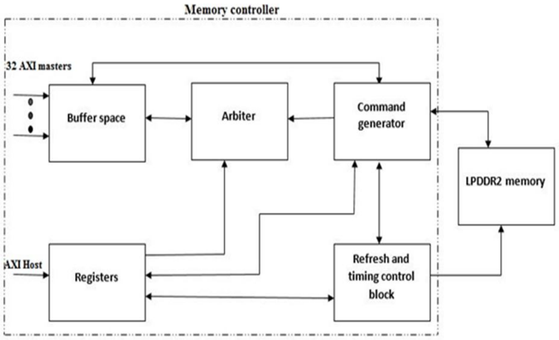


Figure 1: LPDDR2 Memory controller

See figure 1 the LPDDR2 memory controller,LPDDR2 MC’s are used to drive DDR2 SDRAM, where data is transferred on the rising and falling access of the memory clock of the system without increasing the clock rate or increasing the bus width to the memory cell. The masters reading/writing from/to the memory are AXI complaint. LPDDR2 MC follows the JESD209-2F specifications. It can also be configured to power down and deep power down modes.

There are 32 read/write AXI masters, the 33rd master is the host AXI master.

The host will configure all the registers, and the device initialization of the memory will take place and then the actual read/write operation will happen. The buffer space will store all the master requests like address, data and control information, the arbiter will arbitrate the different master requests and gives grant to one master. The command generation will issue different commands to the memory like activate, read, write, precharge, refresh, power down, deep power down which is in synchronization with the refresh and timing control block.

In this paper the LPDDR2 MC Supports SDRAM S2 and S4 devices which can be configured to 4 or 8 banks, and the capacity is 64Mb to 8 GB. The operating frequency of the memory is between 100 MHz to 533MHz.

This paper descries about the "Refresh And Timing Controller Unit" which is part of Memory controller and performs three important operations:

- □ Device initialization of memory device
- □ Refresh Control of memory device
- □ Timing Control for various memory related command.

2. TOP MODULE OF REFRESH AND TIMING CONTROLLER UNIT

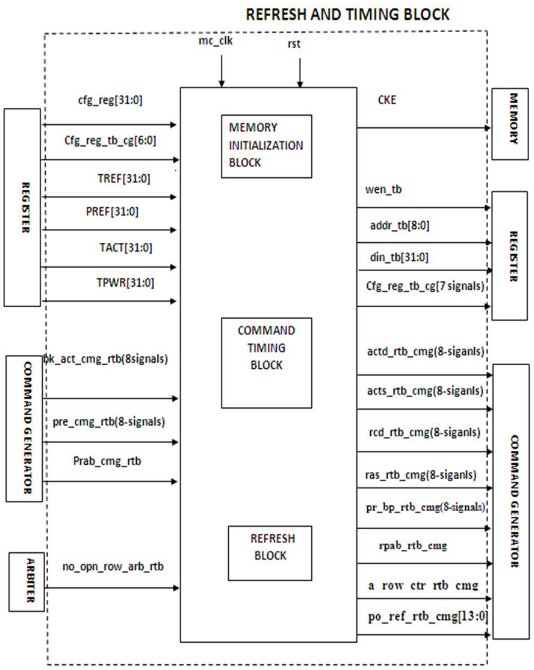


Figure 2: Top module of "Refresh And Timing Controller" unit for LPDDR2 memory controller

See Figure 2 the top module of the **"Refresh And Timing Controller" unit for LPDDR2 memory controller** , the left side signals which are input to "Refresh And Timing "block from the Registers, Arbiter and Command Generator. The right side signals which are output from "Refresh And Timing " block to the Memory, Registers and Command Generator.

There are 5 input from registers are: cfg_reg[31:0], cfg_reg_tb_cg[7:0],TACT[31:0],TPWR[31:0],TREF[31:0],PREF [31:0] ,3 inputs from command generator: bk_act_cmg_rtb(8signals),pre_cmg_rtb(8signsls),prab_cmg_rtb (1signal) , 1 input from arbiter: no_opn_row_arb_rtb and1 CKE output to memory,4 output to register wen_tb, addr_tb[8:0],din_tb[31:0],cfg_reg_tb_cg_in[7:0],

8 different output to command generator acts_bk_rtb_cmg(8signal),actd_bk_rtb_cmg(8signal),rcd_rtb_cmg(8signal),ras_rtb_cmg(8signal),pre_bp_rtb_cmg(8signal),rpab_rtb_cmg,po_ref_rtb_cmg[12:0].

3. IMPLEMENTATION OF REFRESH AND TIMING CONTROLLER UNIT

3.1 Device initialization of memory device FSM

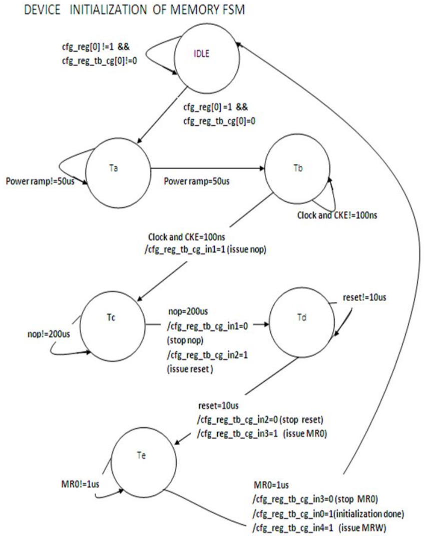


Figure 3: Device initialization of memory device FSM

See Figure 3 initialization of memory device FSM. First step in device initialization is power ramp duration minimum 50us (Ta state).Beginning (Tb State), CKE remain low for at least 100 ns. After which it is asserted high. Clock is stable at least 5 x tCK prior to the first low to high transition of CKE. While keeping CKE high, NOP commands (Tc state) is issued for at least 200 us. .After 200us is satisfied, a MRW (Reset Td-state) command is issued at least 1us is waited, while keeping CKE asserted. After 1us is satisfied(Te state) the MRR command is issued to poll the DAI-bit to acknowledge when Device Auto-Initialization is complete or the memory controller will wait for a minimum of 10us before proceeding. MRW commands is used to properly configure the memory. The LPDDR2 device will now be in IDLE state and ready for any valid command.

3.2 Refresh Control of memory device FSM

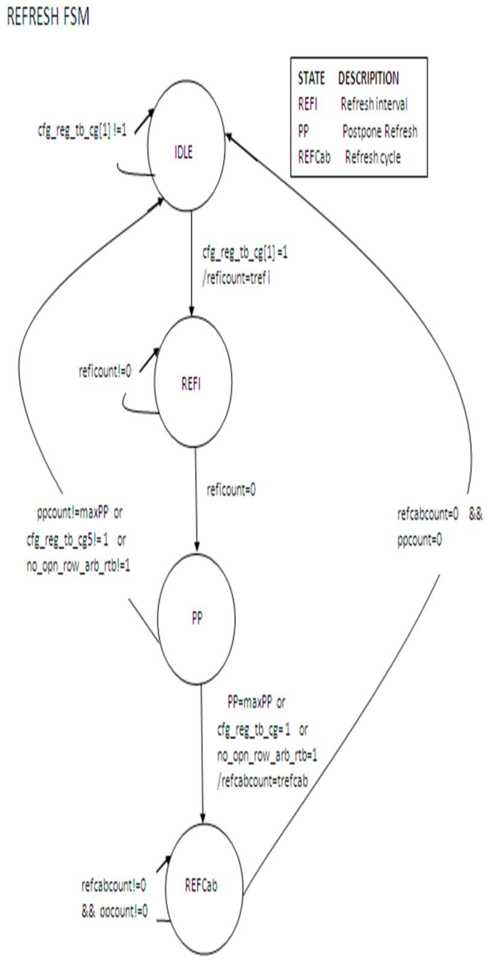


Figure4: Refresh Control of memory device FSM

See Figure 4 the refresh control of memory device FSM. Once device initialization is over it goes from idle state to refresh interval state(REFI state) in which refresh interval duration is maintied,postpone refresh is incremented each time when refresh interval is expired(PP state).When maximum postpone is reached conditional refresh is issued and refresh cycle duration is maintied(REFcab state)for number of postponed refresh.when there is no open row(no request from master to read/write) a conditional refrseh is issued.Refresh ineterval,maximum postpone duration and Refresh Cycle duuration is shown in below table 1for different memory densities.

Table 1: LPDDR2-SX : Refresh Requirements By different Device Density

Parameter	Symbol	64Mb	128Mb	256Mb	512Mb	1Gb	2Gb	4Gb	6Gb	8Gb	unit
Refresh Time in ns(tREFCab) for all Banks-	tREFCab	90	90	90	90	130	130	130	210	210	ns
Average time between REFRESH command	tREFI	15.6	15.6	15.6	15.6	7.8	7.8	7.8	3.6	3.6	us
Refresh postpone	tpp (max)	31.26	31.26	31.63	31.63	30	27.7	27.7	25.1	25.1	ms

3.3 Timing Control for various memory related command

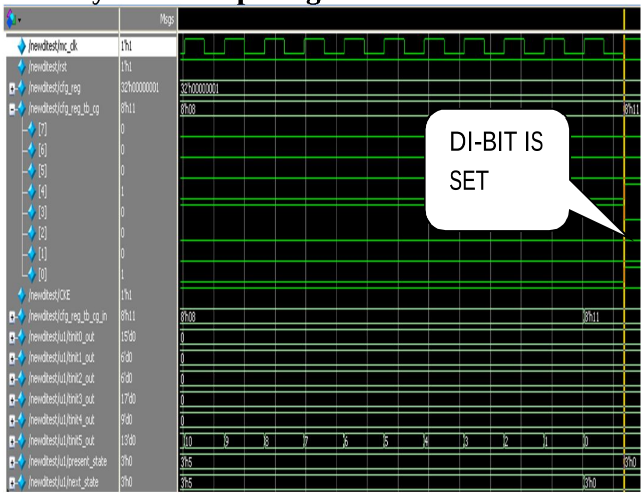
Timing control various memory related command like activate, precharge ,power down, deep power down commands related timing are maintained in refresh and timing block. All timings which are maintained are listed in below table 2

Table 2:Different timing parameters reqiurements by different frequency

Sl.no	Parameter	Symbol	533	466	400	300	266	200	166	Freq in MHz
			1.875	2.15	2.5	3	3.75	5	6	Time period
1	ACTIVE to ACTIVE command period	tRC	tRC=tRAS + tRPab (with all-bank Precharge) tRAS + tRPpb (with per-bank Precharge)							
2	Row Active Time	tRAS	42							ns
3	RAS to CAS Delay	tRCD	18							ns
4	ACTIVE bank A to ACTIVE bank B	tRRD	10							ns
5	Row Active Time	tRAS	42							ns
6	Row Precharge Time(per bank)	tRPab	21							ns
7	Row Precharge Time(single bank)	tRPpb	18							ns
8	Exit power down to next valid command delay	tXP	7.5							ns
9	Minimum Deep Power Down Time	tDPD	500							us

4. SIMULATION RESULTS

4.1 Simulation of Device initialization of memory device as per figure1



	Msgs
/newditest/mc_clk	1'h1
/newditest/rst	1'h1
/newditest/cfg_reg	32'h00000001
/newditest/cfg_reg_tb_cg	8'h11
[7]	0
[6]	0
[5]	0
[4]	1
[3]	0
[2]	0
[1]	0
[0]	1
/newditest/CKE	1'h1
/newditest/cfg_reg_tb_cg_in	8'h11
/newditest/u1/tinit0_out	15'd0
/newditest/u1/tinit1_out	6'd0
/newditest/u1/tinit2_out	6'd0
/newditest/u1/tinit3_out	17'd0
/newditest/u1/tinit4_out	9'd0
/newditest/u1/tinit5_out	13'd0
/newditest/u1/present_state	3'h0
/newditest/u1/next_state	3'h0

Figure 5: shows device initialization is completed by setting cfg_reg_tb_cg[0]=1(DI BIT IS SET)

4.2 Simulation of Refresh

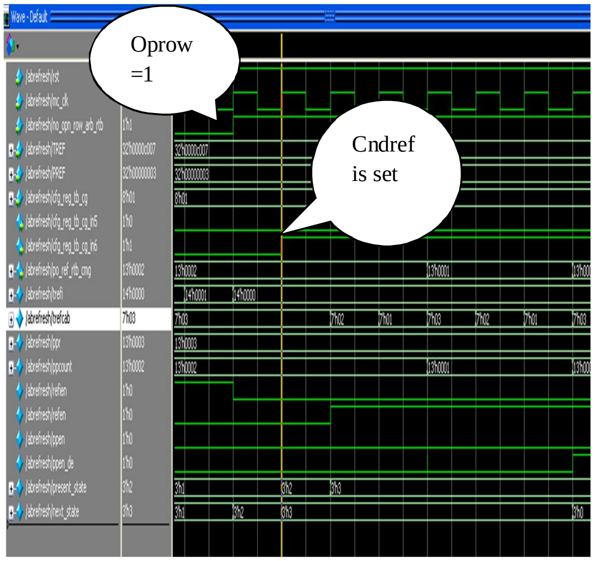


Figure 6: shows conditional refresh is issued in open row condition as per figure 3

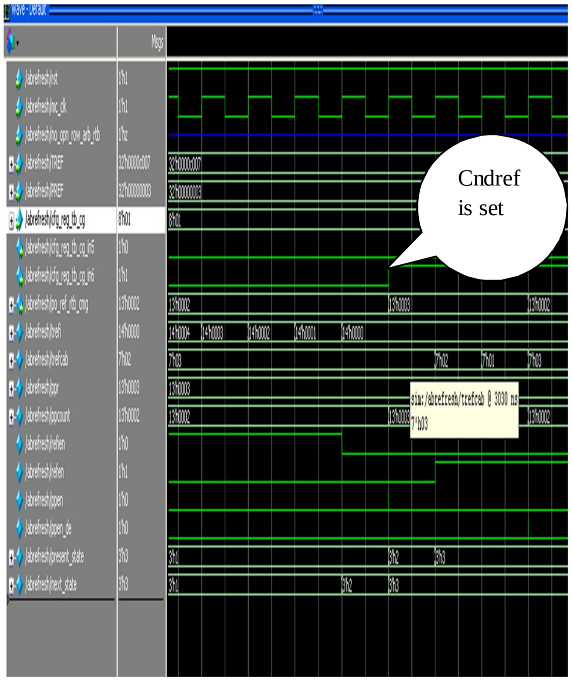


Figure 7: shows conditional refresh (Cndref is set) is issued when maximum pospone is reached as per figure 3

4.3 Simulation of Timing Control for activate command

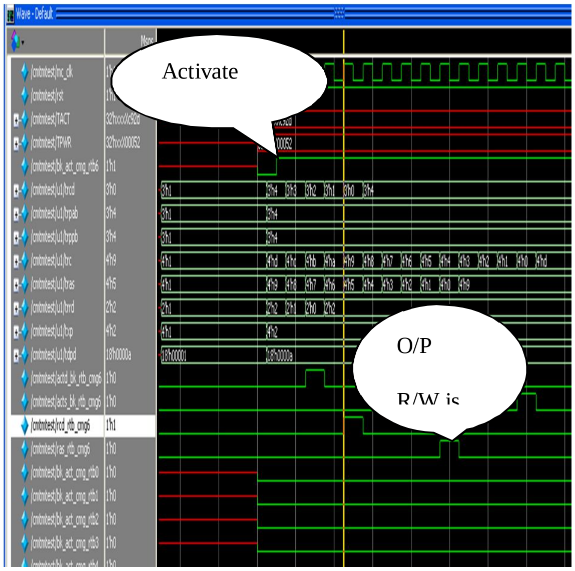


Figure 8: shows when activate command is issued and after some duration read/write bit is set and now memory can go read/write

5. CONCULSION

Device initialization of device are simulated as per JDEC spec. All timing parameters for refresh all bank, activate, precharge, power-down and deep power down command are simulated as per JDEC spec..

6. ACKNOWLEDGEMENT

We sincerely thank the management of BNM Institute of Technology, HOD of ECE department and the project coordinator for the support given to us. We also thank the design and verification engineers at Graphene for giving us the internship opportunity at Graphene Semiconductor Services Private limited and guiding us during our internship there.

7. REFERENCES

[1] “An introduction to SDRAM and memory controllers” by BENNY AKESSON.

[2] “Design and implementation of a memory controller for Real Time Applications” by Markus Ringhofer

[3] “JEDEC Low Power Double Data Rate (LPDDR2) SDRAM Standard,” 209-2F, June 2013. Specification (Rev2.0), ARM Inc.

[4] DDR RAM by Gene Cooperman

[5] “Mobile LPDDR2 SDRAM ‘by Micron technologies, 2010.

[6] ”Verilog HDL, A Guide to Digital Design and Synthesis” by Samir Palnitkar, 2nd edition.