January - June, 2011 Vol. 3 No. 1 ISSN 0973-5658

BVICAM's IJIT

BVICAM's International Journal of Information Technology

Special Issue on "Mobile Ad-Hoc Networks"

CONTENTS

BHARATI VIDYAPEETH PUNE

Bharati Vidyapeeth's
Institute of Computer Applications and Management
A-4, Paschim Vihar, Rohtak Road, New Delhi-63

Email : bijit@bvicam.ac.in, Website : http://www.bvicam.ac.in

Volume 3, Number 1

January - June, 2011

Special Issue on "Mobile Ad-Hoc Networks"

BVICAM's International Journal of Information Technology (BIJIT) is a bi-annual publication of Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063.

ISSN 0973 – 5658

Address for Correspondence:

Prof. M. N. Hoda
Chief Editor – BIJIT
Director, Bharati Vidyapeeth's
Institute of Computer Applications and Management,
A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063 (INDIA).
Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at www.bvicam.ac.in

Published and printed by Prof. M. N. Hoda, Chief Editor – BIJIT and Director, Bharati Vidyapeeth's Institute of Computer Applications and Management, A-4, Paschim Vihar, New Delhi – 63 (INDIA).
Tel.: 91 – 11 – 25275055, Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at www.bvicam.ac.in

BVICAM's
International Journal of Information Technology (BIJIT)

BIJIT is a bi-annual publication of

Bharati Vidyapeeth's

Institute of Computer Applications and Management

A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063 (INDIA)

Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in

Visit us at www.bvicam.ac.in

Editorial

It is a matter of both honor and pleasure for us to put forth the fifth issue of BIJIT; the BVICAM's International Journal of Information Technology. This issue has been dedicated as a Special Issue on "Mobile Ad-Hoc Networks". It presents a compilation of ten papers that span a broad variety of research topics in various emerging areas of Information Technology and Computer Science. Seven papers are included under the special issue on "Mobile Ad-hoc Networks" and remaining three papers are on general theme. Some application oriented papers, having novelty in application, have also been included in this issue, hoping that usage of these would enrich the knowledge base and facilitate the overall economic growth. This issue shows our commitment in realizing our vision "*to achieve a standard comparable to the best in the field and finally become a symbol of quality"*.

As a matter of policy of the Journal, all the manuscripts received and considered for the Journal by the editorial board are double blind peer reviewed independently by at-least two referees. Our panel of expert referees posses a sound academic background and have a rich publication record in various prestigious journals representing Universities, Research Laboratories and other institutions of repute, which, we intend to further augment from time to time. Finalizing the constitution of the panel of referees, for double blind peer review(s) of the considered manuscripts, was a painstaking process, but it helped us to ensure that the best of the considered manuscripts are showcased and that too after undergoing multiple cycles of review, as required.

The ten papers that were finally published were chosen out of more than eighty papers that we received from all over the world for this issue. We understand that the confirmation of final acceptance, to the authors / contributors, is delayed, but we also hope that you concur with us in the fact that quality review is a time taking process and is further delayed if the reviewers are senior researchers in their respective fields and hence, are hard pressed for time.

We wish to express our sincere gratitude to our panel of experts in steering the considered manuscripts through multiple cycles of review and bringing out the best from the contributing authors. We thank our esteemed authors for having shown confidence in BIJIT and considering it a platform to showcase and share their original research work. We would also wish to thank the authors whose papers were not published in this issue of the Journal, probably because of the minor shortcomings. However, we would like to encourage them to actively contribute for the forthcoming issues. A very special thanks to the Guest Editor; Dr. D. K. Lobiyal and Joint Editor; Mrs. Umang for having taken pain and finalized the papers of the special issue.

The undertaken Quality Assurance Process involved a series of well defined activities that, we hope, went a long way in ensuring the quality of the publication. Still, there is always a scope for improvement, and so we request the contributors and readers to kindly mail us their criticism, suggestions and feedback at bijit@bvicam.ac.in and help us in further enhancing the quality of forthcoming issues.

Editors

C O N T E N T S

Hash Security for Ad hoc Routing

Ashwani Kush[1] and **C. Hwang**[2]

Submitted in June 2010; Accepted in November 2010

Abstract - ***A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. The ad hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. An attempt has been made to review some of the existing protocols. Finally a new scheme based on Hashing has been proposed to secure an existing protocol. One-way hash chain is used to protect hop-by-hop transmission. The scheme has been incorporated using AODV as base protocol and results have been explained using NS.***

Index Terms - Security, Ad hoc networks, Routing protocols, Key Management, AODV

1.0 INTRODUCTION

An Ad hoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the Ad Hoc environment. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defence. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. Rest of the paper is designed as: Section 2 discusses Security Challenges, Survey of various protocols is given in Section 3, Section 4 describes new scheme and Conclusion has been made in Section 5.

[1]*Department of Computer Science, University College, Kurukshetra University, Haryana, INDIA*
[2]*Department of Computer Science and Engineering, Texas State University, San Marcos, Texas, USA*
E-Mail: [1]*akush20@gmail.com and* [2]*cjhwang@txstate.edu*

2.0 SECURITY CHALLENGES

All layers in network are prone to some security threats. Table 1 highlights a few of them

Layer Name	Attack
Physical Layer	Jamming, Interception Eavesdropping
Data Link Layer	Traffic analysis, monitoring, MAC disruption, WEP weakness
Network Layer	Routing attacks (DSR, AODV) like Wormhole, location disclosure, impersonation, blackhole, flooding, Cache overflow, route table overflow
Transport Layer	TCP ACK Storm Attack, Session takeover, SYN flooding
Application Layer	Malicious code like Virus, spyware, Trojan horse, lack of cooperation

Table 1: Layer attacks

In this paper, the prime concern is with the attacks targeting the routing protocols for Ad hoc Networks. These attacks [2,3,4,5] can be broadly classified into two main categories as: Passive attacks, Active attacks

2.1 Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. The nature of attacks varies greatly from one set of circumstances to another.

2.2 Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream. It is quite difficult to prevent active attacks absolutely, as this would require physical

protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. Figure 1 is a description of active and passive attacks.

There are various types of attacks that can be categorized on ad hoc network as:

2.2.1 Location Disclosure: This attack targets the privacy requirements of an ad hoc network.

2.2.2 Black Hole: In a black hole attack a malicious node gives false route replies to advertise itself as having the shortest path to a destination.

2.2.3 Replay: An attacker that performs a replay attack into the network routing traffic that has been captured previously.

2.2.4 Wormhole: The wormhole attack is one of the most powerful ones since it involves the cooperation between two malicious nodes that participate in the network.

2.2.5 Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender.

2.2.6 Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network.

2.2.7 Rushing Attack: Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols.

2.2.8 Masquerading: During the neighbor acquisition process, an outside intruder joins illegally in the routing protocol do main by compromising authentication system.

2.2.9 Passive Listening and traffic analysis: The intruder could passively gather exposed routing information. Such a attack can not effect the operation of routing protocol, but it is a breach of user trust to routing the protocol.

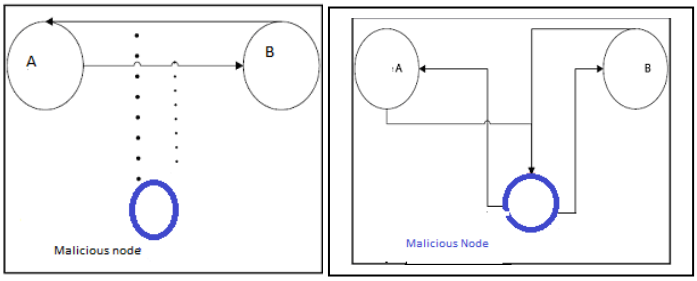


Figure 1: (a) Passive Attack (b) Active Attack

3.0 SECURE ROUTING PROTOCOLS

In this section some of the popular secured protocols have been analyzed. Efforts have been made to use same metrics for all and be bias less.

3.1 ARAN [6] : Dahill et al. proposed ARAN[6], It assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request, reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Authenticated Routing for Ad-hoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment [7].

Characteristics:

(i) ARAN is able to take care of Replay attacks
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does not secure for Denial Of service
(vi) ARAN is loop free
(vii) It is based on Online trusted certification authority

3.2 SEAD [9]: This Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network [9]. To support use of SEAD with nodes of limited CPU processing capability and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, it uses efficient one-way hash functions. It is based on DSDV. It has been designed to protect routing update packets.

Characteristics:

(i) SEAD is able to take care of Replay attacks
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does secure for Denial Of service
(vi) SEAD is table driven
(vii) It is based on Clock synchronization
(viii) It is loop free and uses Distance as route metric

3.3 SRP [9] : Secure Routing Protocol [9] (Lightweight Security for DSR[16]), which one can use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP doesn't attempt to secure ROUTE ERROR packets but instead delegates the route-maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. SRP uses a sequence number in the REQUEST to ensure freshness, but this sequence number can only be checked at the target.

SRP requires a security association only between communicating nodes and uses this security association just to authenticate ROUTE REQUESTS and ROUTE REPLYS through the use of message authentication codes. At the target, SRP can detect modification of the ROUTE REQUEST, and at the source, SRP can detect modification of the ROUTE REPLY. It defends against attacks that disrupt the route discovery process. It is used with DSR, ZRP. It uses mechanism of secure certificate server.

Characteristics:

(i) SRP is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole, Worm hole and invisible node attacks
(v) It does secure for Denial Of service
(vi) SRP is loop free and uses Distance as route metric
(vii) It uses existence of security association between each Source and Destination

3.4 SECURE AODV [10] : The SAODV [10] implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust. The AODV[15] protocol is comprised of two basic mechanisms, route discovery and maintenance of local connectivity. The SAODV protocol adds security features to the basic AODV mechanisms, but is otherwise identical. A source node that requests communication with another member of the MANET referred to as a destination D initiates the process by constructing and broadcasting a signed route request message RREQ.

Characteristics:

(i) SAODV is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does not secure for Denial Of service
(vi) SAODV uses Online key management scheme for acquisition and verification of keys
(vii) It is loop free and uses Distance as routing metric

3.5 SLSP [11]: The Secure Link State Protocol (SLSP) [11] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within *R* hops, which is termed as their *zone*. Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (*LSU*) packets from malicious alteration, as they propagate across the network.

Characteristics:

(i) SLSP is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does secure for Denial Of service
(vi) SLSP is table driven, Loop free
(vii) It assumes that Nodes must have their public keys certified by a Trust party
(viii) It uses Distance as Routing metric

3.6 ARIADNE [12]: A Secure On Demand Routing Protocol for Ad Hoc Networks (ARIADNE) using the TESLA[13] broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication. Adding a MAC (computed with a shared key) to a message can provide secure authentication in point-to-point communication; for broadcast communication, however, multiple receivers need to know the MAC key for verification, which would also allow any receiver to forge packets and impersonate the sender. Secure broadcast authentication thus requires an asymmetric primitive, such that the sender can generate valid authentication information, but the receivers can only verify the authentication information. It is used with DSR. It is prone to selfish node attack. It prevents attackers from tampering uncompromised routes.

Characteristics:

(i) ARIADNE is able to take care of Replay attacks and immune to wormhole attack.
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole.
(v) It does secure for Denial Of service
(vi) It uses TESLA keys distributed to participating nodes
(vii) It is loop free and uses Distance as Routing metric.

3.7 SAR [14]: Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into adhoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. We assume that the base protocol is an on demand protocol similar to AODV or DSR. In the original protocol, when a node wants to communicate with another node, it broadcasts a Route Request or RREQ packet to its neighbors. It is used with AODV. It uses sequence number and time stampings to stop replay attacks. In this route discovered may not be the shortest one.

Characteristics:

i) SAR is loop free
ii) It uses Security requirement as Routing metric
iii) SAR uses Key distribution or secret sharing mechanism
iv) SAR is not loop free, it depends upon selected security requirement
v) It is able to take care of Replay attacks

vi) It is not able to eliminate Rushing attacks
vii) It does not effectively deals with location disclosure
viii) It does secure for Denial Of service

4.0 PROPOSED PLAN

When a source node S needs to discover a route to a destination node D, it initiates a route request (RREQ) message, which includes the source (S) node and Destination (D) node, a request sequence number, and an initial hash value. The initial hash value is computed as H0 = Hash [n] , where n is a random number. The source node S appends the computed initial hash value H0 , and then broadcast the RREQ packet. The neighbor node, receiving this RREQ packet, would check the validity of source node. If any checking process fails, the node discards the packet, otherwise, rebroadcasts. Any intermediate node, say 1, receiving the packet checks whether it has already seen this packet by recognizing the combination of (source node, request sequence number) . If it has, discards the packet, as in regular AODV, otherwise it adds its address to the node list, replaces the hash value field with Hash(1, previous hash value) and rebroadcasts the packet.

S : H_0 = Hash [n]
S -> RREQ, S, D, Seq#,{ } ,H_0

H_1 = Hash [1, H_0]
1-> RREQ, S , D, Seq#,{1} , H_1

H_2 = Hash [2, H_1]
2-> RREQ, S , D, Seq#,{1,2} , H_2

D: [D, S , { 2,1 } , Seq#]

D->2 : RREP, D,S, {1,2} , Seq#
2-> 1 : RREP, D,S, {1,2} , Seq#
1->S : RREP, D,S, {1,2} , Seq#

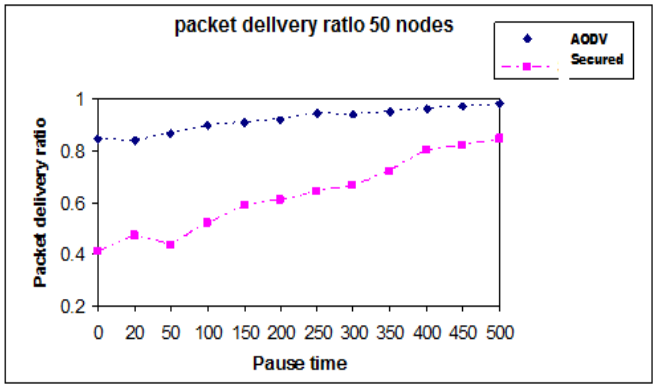
Figure1: Packets exchanged between nodes during RREQ phase.

When the destination node receives the RREQ, it performs a sequence of checking processes. It first unscrypts the received ciphertext and compare the result with the routing message received. If the comparison indicates a match, node D gets the initial hash value H_0. It would further verify the source node S. If the sequence number is greater than the last received sequence number from S, it checks the hash chain field is equal to

H [N_n, H[N_{n-1},H[.. H[N_1,H_0] ..]]]

If any step of the above checking process fails, the authentication fails, and the destination node discards the RREQ packet; otherwise, the destination node prepares the RREP packet. It first copies the accumulated node list from the RREQ packet, reverses it, and puts it to the source route.

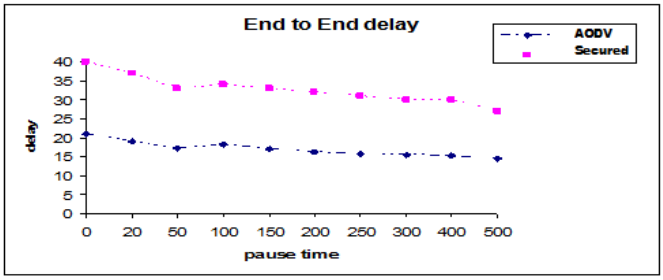
As is evident from proposed scheme, the format size will be increased with inclusion of Hash key generation. The routing load will increase due to incorporation of security. It is also clear that the scheme affects the packet delivery fraction and end-to-end delay. The packet delivery fraction will be marginally reduced. Also chances of packets drop may increase due to delay produced in route reply case. This could be improved by having higher timeouts for packets buffered for route discovery.



Graph 1: PDF using pause time

Simulation study has been carried out to study the performance study of proposed protocol. Simulation Environment used for this study is NS-2 [20]. Area selected is 1 × 1 KM and 50 nodes have been taken. Pause time is varied from 0 to 500 sec. Pause time 500 means minimum movement and 0 means maximum movement. TCP packets are used.

Graph 1 show the packet delivery ratio based on pause time. The packet delivery ratio is the fraction of successfully received packets, which survive while finding their destination. This performance measure determines the completeness and correctness of the routing protocol. Pause time of 0 means very fast moving nodes and 500 shows minimum movement.



Graph 2: End to end delay

As the graph indicates 'Secured' has less number of packets delivered, but this reduction in delivery is due to Hash keys calculations and evaluations. Graph 2 represents the end to end delay with respect to pause time. Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. More end to end delay is observed in this case for 'Secured'. The reason is again the more calculation part involved for hash key estimation. It should be noted here that only trusted packets are delivered, so some packets does fall because of this reason also.

The reduction in packet delivery ratio and increase in end to end delay does not show the effectiveness of the proposed scheme. This change will be obvious as more packets are

sacrificed to keep them secured. Security is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of Hash key

5.0 CONCLUSION

The proposed authentication scheme, in essence, is still an asymmetric key based approach, except it shows some properties of lower computational cost and reduced communication overhead comparing with the traditional PKI supported schemes. An attempt has been made to present an overview of the existing security scenario in the Ad-Hoc network environment. Hash Key management has been proposed as one of the best options for security, though other options can also be considered depending upon need of security. As hash key chain is configured as a recursive chain so these keys are noted in route table. Important function is that the routing protocol functions very similar to the existing one when there are no external attacks. Whenever an attack occurs additional packets need to be sent to change the routes established by the malicious control packets. This increased traffic size will have its impact on overhead. The overhead is bound to increase with it, but keeping in view of the better secured routing this will have to be done to achieve desired results. Efforts are on to simulate the proposed scheme with different topologies, more metrics and to compare it with existing secured routing schemes. Proposed scheme is expected to work better in dense environments as selection of path becomes easy in case of failures. Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. Several protocols for secured routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The current security mechanisms, each defeats one or few routing attacks. It is still a challenging task to design routing protocols resistant to multiple attacks.

FUTURE SCOPE

More simulations will be carried out using speed as a function as well. DSR and TORA will also be compared with proposed scheme and implementing this concept into them. Dense environment has been used in this scheme. Efforts are on to make the scheme robust for sparse medium as well.

REFERENCES

[1]. A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and secure source authentication for multicast", In Network and Distributed System Security Symposium (NDSS'01), Feb. 2001.

[2]. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication 800-48, November 2002.

[3]. William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall New Jersey 2003

[4]. Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking(MOBICOM'00), pp. 275– 283, Aug 2000.

[5]. A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3. pp 1793-1799,

[6]. B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[7]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine October 2002.

[8]. Y.-C. Hu, D. B. Johnson, and A. Perrig., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, pp 3-9. IEEE Computer Society, 2002.

[9]. P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[10]. M. Guerrero Zapata. "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing". IETF MANET Mailing List, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2004.

[11]. P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks" Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.

[12]. Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, Dec. 2001.

[13]. A. Perrig, R. Canetti, D. Tygar, and D. Song, "TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories)", Vol 5, No 2, Summer/Fall 2002, pp. 2-13.

[14]. R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.

Continued on page no. 280

ACBRAAM: A Content Based Routing Algorithm using Ant Agents for MANETs

Ramkumar K. R.[1], Sakthivel K.[2] and **Ravichandran C. S.[3]**

Submitted in July 2010; Accepted in November 2010

Abstract - ***A mobile ad hoc network (MANET) is a temporary network which is formed by a group of wireless mobile devices without the aid of any centralized infrastructure. In such environments, finding the identity of a mobile device and maintaining the paths between any two nodes are challenging tasks, in real time the limited propagation range of mobile devices restrict its identity only to its neighbors and a new host enters in to a MANET does not know the complete details of that instantaneous MANET. This paper analyses the possibility of content based route discovery and proposes a framework for request based route discovery and path maintenance using ant agents. The ant agents fetch routing information along with content relevancy which will have a major influence on pheromone value. The pheromone value is used to find the probability of goodness. The proposed framework consists of ant structures and algorithms for route discovery and path maintenance.***

Index Terms - MANETS, ANT, Request Based Path Setup

1.0 INTRODUCTION

A Lot of research work is going on the development of routing algorithms for MANETs. The swarm intelligence based routing algorithms are Antnet [5], ARA [3] and AntHocNet [4] The categorization will be in general either as *proactive* or *reactive routing.* Proactive routing algorithm updates routing tables constantly but reactive routing algorithms update routing information when required. In path maintenance phase the ants' exploratory behavior is limited around the current optimal path. The basic design behind ACO algorithms for routing is the consciousness of routing information through path sampling using ant agents. These ant agents are generated concurrently and independently by the source nodes, with the task to try out a path to an assigned destination. Assigned destination is an assumption in all existing algorithms ie) the user has to mention source and destination addresses manually. In the range limited networks there is no standard approach to identify the destination node. The general algorithms are working as forward ants always attempts to discover newer routes and the backward ants update path quality and maintain pheromone values. The pheromone value is a measure of probability of goodness going over that neighbor on the way to the destination.

In this paper the content based route discovery is proposed, the precise number of forward ant generations and implementation of heuristic routing methodology are given as algorithms. The rest of the paper is organized as follows. In Section II, the different types of forward ants and backward ants which ensure the content based route discovery and guaranteed data transaction are discussed. The timer introduced here is to reduce the number of backward ants in heavily loaded or congested path .The XML privileges are taken in to account to maintain the consistent forward ant and back ward ant functionalities. Next In Section III the proposed algorithms for forward ants, in section IV path updating algorithms are discussed and in section V the simulation and results are explained.

[1,2]Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, INDIA
[3]SSK College of Engineering and Technolgy, Coimbatore, INDIA
E-Mail: [1]ram@svce.ac.in, [2]sakthivel87@gmail.com and [3]eniyanravi@gmail.com

2.0 ANT AND HOST PROFILE

A FORWARD ANT WITH CONTENT TAG

When a source node needs some information or content from an existing MANET, it first checks the cache for existing routes, when no routes are known, it broadcasts forward request ants with content tag and it is propagated through the network till it reaches maximum hop count. The forward ant carries the content to be searched, when a relevant content is found then forward ant is converted in to backward ant, at the same time the forward ant continues its travel for more relevant contents till it reaches maximum hop count. A forward ant at each intermediate node selects next hop using the information stored in the routing table of that node or by rebroadcast. The timer attribute is used to find out congested path for load balancing. The forward ant initializes the timer value to zero and increments the value by milliseconds till it reaches destination. When a forward ant finds the relevant content from an authenticated node, then backward ant is generated as in AntHocNet[4] which takes same path but in opposite direction. The backward ant updates pheromone value as it moves on its way to source node. The content relevancy and availability ratio decides *pheromone* value, more relevant content increases pheromone value. The definition of forward ant is given in XML format to acquire all benefits of XML in data delivery. XML could be easily combined with DTD [Document Type Definition], XML Schema for integrity checking and SOAP, XML RPC for accessing remote methods and devices, and also it could be benefited from the XML Security.

2.1 Schema definition

```
<?xml version="1.0"?>
 <xsi:schema
xmlns:xsi="http://www.w3.org/2001/XMLSchema">
<xsi:element name="fwdant">
<xsi:complexType>
 <xsi:sequence>
```

```
        <xsi:elementname="fwd" type="xsi:integer"/>
         <xsi:element name="req" type="xsi:integer"/>
         <xsi:element name="payload"type="xsi:integer"/>
        <xsi:element name="hopcount" type="xsi:integer"/>
        <xsi:element name="maxhopcount"
type="xsi:integer"/>
        <xsi:element name="timer" type="xsi:integer"/>
        <xsi:element name="srcaddr" type="xsi:integer"/>
         <xsi:element name="destaddr" type="xsi:integer"/>
         <xsi:element name="content" type="xsi:string"/>
         <xsi:element name="path">
        <xsi:complexType>
        <xsi:sequence>
        <xsi:element name="n1"
          type="xsi:integer"maxOccurs="unbounded"
        minOccurs="0"/>
 </xsi:sequence>
</xsi:path>
 </xsi:complexType>
 </xsi:element>
 </xsi:sequence>
 </xsi:attribute>

 </xsi:complexType>
 </xsi:element> </xsi:schema>
```

2.2 Forward ant structure

The forward ant structure could be combined with XML Schema and explored to all its neighbors to discover content and new routes.

```
<fwdant id = no>
<fwd>1</fwd>
 <req>1</req> <payload>0</payload>

<hopcount>CurrentHopCount</hopcount>
<maxhopcount>Theory Standards  </maxhopcount>
<timer>00:00:00:00</timer>
 <srcaddr>Address </srcaddr>
 <nexthop>Neighbor Address<nexthop>
   <destaddr>Empty</destaddr>
    <content>Content To be searched</content>
    <path>
        <n1>Neighbor1</n1>
        <n2>Neighbor2</n2>
              ……..

        <nN>NeighborN</nN>
   </path>
</fwdant>
```

B NODE PROFILE

It is been assumed that user sets profile for his device which participates in MANET. Profile states the nature of content it has and defines access rights. A forum could be constituted to define profile format. If a node wishes to contribute or distribute its data then it can tag the content's availability in various categories. First one is public content which could be accessed by any node in that network, data movement and ant movement will not be sensed by the user of that device, in other terms the public contents will be delivered without human intervention. Second content type is categorized as protected data, protected data also will be shown for public view, content tag could be identified by any node but content delivery has to be authenticated by the user of that target host. Proper certification method and security algorithms will provide a secured way of protected data transaction. Third is categorized as private content, which cannot be accessed by other hosts.

2.3. Node profile

```
<node>
<address>Nodeip</address>
<public>

<contenttag>Tagname[JAVA]
        <filename>Name of the file<filename>
 </contenttag>
 <contenttag>Tagname[C++]

         <filename>Name of the file</filename>
</contenttag>

</public>
<protected>

   <contenttag>Tagname[Photos]
   <filename>Name of the file</filename>

   </contenttag>
   </protected>
</node>
```

3.0 ALGORITHMS FOR ROUTE DISCOVERY

The basic structure is taken from ARA [3], the attributes like timer value; content tag and content relevancy are updated. The standard stack structure to hold the path information is changed as path variable since XML format is used for forward ants. The XML schema is used to check integrity. So the corrupted forward ants could be discarded.

Route discovery is the process of finding possible paths between source and destination which seizes required content. The result of route discovery process is the generation n of multiple backward ants with updated paths to relevant content holder targets.

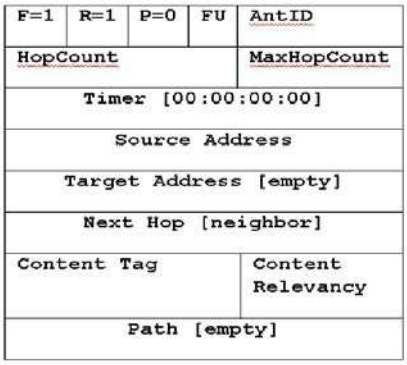


Figure 3.1: Forward ant Structure

Algorithm 1: Generation of forward ant with content

Input: f_{ant}: forward ant attributes, a_f:forward/backward, a_r:request/reply, a_p:payload/empty, a_{id}: request id,

a_{nhop}:neighbour host
a_{hc}:current hopcount,

a_{mhc}:maximumhopcount limit,
a_{timer}: timervalue,a_{src}:sourceaddress,
a_{dst}:destination address,
a_{ctag}:Contenttag, a_{crel}:contentrelevancy,
a_{path}:ant path n_{list}: neighbor list

Output: f_{ant}:forward ant

//Construct a forward ant with all initial parameters.
a_{id}=unique id ,
a_{ctag}= Requestedcontent
a_{crel}=0.0, a_{mhc}=maximum hopcount

a_{dst}=null,a_f=1,a_r=1,a_p=0,a_{hc}=0
a_{timer}=00:00:00:00,a_{nhop}=null a_{path}=null
f_{ant}=construct_Fi(a_f,a_r,a_p,a_{id},a_{hc},a_{mhc},

atimer,asrc,anhop,adst,actag,acrel,apath)
forward(f_{ant},n_{list});

end

Algorithm 2: Routediscovery (f_{ant},n_{list})

Input : f_{ant} :forward Ant, n_{list} :neighbor list
Output: Route discovery and table updating
//Constitute a route discovery process from Source to destination
if a_{hc}=0 || a_{id} is new then
if a_{hc}<=a_{mhc} then
for a_{nhop} Є n_{list} do
if *actag* Є *nctaglist* **&&** n_{ctag}=*public* || *protected* then
f_{ant}=updateandgenerate(a_{hc},a_{nhop},a_{path})

Converttobackwardant(f_{ant})
end
else

Routediscovery(f_{ant},n_{list})

end
else
discard(f_{ant})
end

Generation of backward ant is a simple process of changing the addresses and setting proper timer values.Backward ant structure given below changes some flag bits and content relevancy is filled with the help of ranking algorithms.

Figure 4.2: Backward ant structure with content relevancy

Algorithm 3: Generation of backward ant

Input : f_{ant}: forward ant
Output: b_{ant}:backward ant
copy b_{ant}=f_{ant}

swap $b_{ant}.a_{src}$ with $b_{ant}.a_{dst}$
bant.atimer=fant.atimer * α [α = 2]
bant.amhc=fant.ahc
unicast(b_{ant})

4.0 PATH UPDATION

4.1 Backward Ant from Destination

The backward ants are used to update the discovered path. Existing algorithms states that backward ants calculates pheromone values using queuing delay and MAC delay as in AntHocNet[4] in turn pheromone values are used to calculate the probability of goodness. The content relevancy is also included to calculate pheromone value. New pheromone value will be calculated as

Γnd = α * Γnd + (1-α) * Γnd *Cr ---------- (1).

Γ_{nd} – New Pheromone value for the neighbor.
α – 0.7 taken from standards[good probability]
Cr- Content Relevancy.

Content Relevancy ranges from [0,1] which will have direct impact to pheromone value. This pheromone value is updated to the node table of every node by backward ants.
The backward ant travels back to source by following path information and updates pheromone value which also includes content relevancy ratio, content relevancy will have a major impact to retrieve relevant content. The timer value will be trailed automatically to discard longer waiting backward ants. If a backward ant is unable to reach the source on time then it clearly indicates that the path is more congested and data delivery will not be fruitful. So better the backward ant could be discarded in the intermediate node itself so that path could be avoided for data delivery.

Algorithm 5: unicast(b_{ant})

Input : b_{ant}:backward ant

Output: *m*:updated path
// find content relevancy and assign it to Cr.
$b_{ant}.a_f$=0,$b_{ant}.a_r$=0,$b_{.ant}.a_p$=0 *bant.acrel=Cr*
if $b_{ant}.a_{dst}$==*currentNodeIP* then

$\Gamma_{nd} = \alpha * \Gamma_{nd} + (1-\alpha) * \Gamma_{nd} * C_r$
start new unicast request from $b_{ant}.a_{src}$
to *bant.adst*
end
else if $b_{ant}.a_{dst}$!=*currentNodeIP* then
if $b_{ant}.a_{hc} < b_{ant}.a_{mhc}$ &&
$b_{ant}.A_{timer} > 00:00:00:00$ then

pickup next node from $b_{ant}.a_{path}$ and

unicast(b_{ant})
$b_{ant}.a_{hc} = b_{ant}.a_{hc} - 1$
autodecrement $b_{ant}.a_{timer}$
// update pheromone value based on content
relevancy
else
discard(b_{ant})
end
end

The free function will free up memory space which is allocated to a particular ant. A node can delete a forward ant which crossed maximum hop count and time exhausted backward ants. The discard algorithm is used to control flooded forward and backward ants where ever is possible to reduce the congestion and collision.

Algorithm 4: discard (f_{ant} // b_{ant})

Input : f_{ant}: forward ant or b_{ant}: backward ant

Output : null
free(f_{ant});

4.2 Working Ants

Once the content discovery and path establishment is over then the data transaction thread has to be started. The data transaction thread follows a sequence, first sending a unicast request from source to destination to confirm data delivery, the destination node starts data delivery after receiving confirmation, the payload is accompanied with a backward ant to update path while transferring payload. In case of route failure during payload delivery the backward ant will be detached and converted as forward ant to discover new routes as in HPRAAM [1].

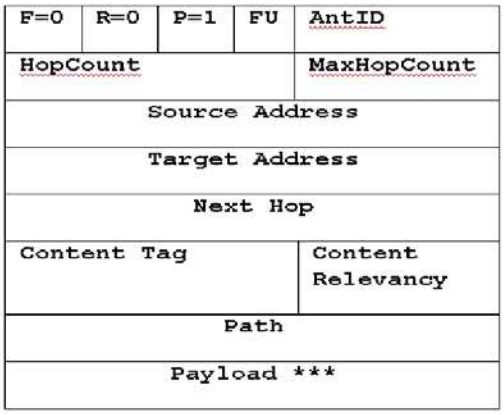


Figure 4.3: Backward ant with payload

5.0 SIMULATION AND RESULTS

The simulation is tried with 60 nodes moving at random way point model with different speed and different pause time. Contents and content relevancies are distributed randomly among all nodes. Simulation is executed for random times ranges from 20 to 200 seconds and requests are made for different contents from different nodes. The proposed algorithm is compared with ARA [3] and it outperforms in searching relevant content in a short period.

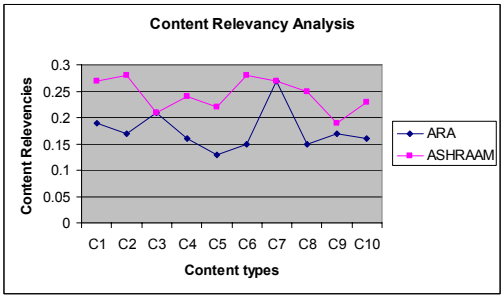


Figure 5.1: Content relevancy analysis

ASHRAAM gathers more relevant results while searching content in MANET. ARA only chooses the minimum hop

count destination to retrieve contents which may be irrelevant. So it has to perform route discovery process again and again which will create more congestion and flooded ants in MANET. ASHRAAM initiates only one route discovery process; to get all destinations and content relevancies for the content.

6.0 CONCLUSION

In this study a new proposal for content based routing using ant agents has been made as a framework. The proposed framework can reduce the congestion in MANET, and also it can diminish the number of retransmissions of forward and backward ants. The timer concept decides the life time of a backward ant, a backward ant which is trapped by a heavily congested network will be dropped automatically after a period of time. The long waiting backward ants brings out unreliable paths to the source node, with the help of timer
concept the problem is completely avoided. This framework will create a new path towards the content based route discovery and XML based ant generations to leverage the benefits of both.

REFERENCES

[1]. Ramkumar. K. R, GaneshKumar. M, Hemachandar. N, ManojPrasadh. D"HPRAAM: Hybrid Parallel Routing Algorithm Using Ant Agents for MANETS" IJET ,ISSN:1793-8244,1793-8236,March 2009.

[2]. Ramkumar. K. R, GaneshKumar. M, Hemachandar. N, ManojPrasadh. D,Nisha. M"ARRAAM:A Reliable Routing Algorithm Using Ant Agents For MANET", ISSN:1865-0929,1865-0937,ISBN: 978-3-642-02341-5 ,March 2009

[3]. M. Guine,, U. Sorges, and I. Bouazzi, "ARA-the ant-colony based routing algorithm for MANETs," in Proc. of IWAHN 2002, pp. 79-85, August 2002.

[4]. G. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: An Adaptive Nature-Inspired Algorithm for Routing in Mobile Ad Hoc Networks," Tech. Rep. No. IDSIA-27-04-2004, IDSIA/USI-SUPSI, Sep.2004.

[5]. Gianni Di Caro, Marco Dorigo, "AntNet: Distributed Stigmergetic Control for Communications Networks" Journal of Artificial Intelligence Research 9 317-365. Aug'1998

Continued from page no. 275

[17]. D. B. Johnson et al., "The dynamic source routing protocol for mobile ad hoc networks (DSR)", Internet Draft, MANET working group, Feb 2002.

[18]. L. Lamport, "Password Authentication with Insecure Communication", Comm. of ACM, 24 (11), pp. 770-772, Nov. 1981

[19]. A.Kush, C.Hwang, "Proposed Protocol For Hash-Secured Routing in Ad hoc Networks", MASAUM JOURNAL OF COMPUTING (MJC) Volume: 1 Issue: 2 Month: September 2009 , pp 221-226

[20]. A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3. pp 1793-1799.

[21]. NS Notes and Documentation, available at www.isi.edu/vint

[22]. Hongmei Deng, Dharma P. Agrawal TIDS: threshold and identity-based security scheme for wireless ad hoc networks Elsevier journal of adhoc networks, Vol 2 (2004), pp 291-307

MANEMO for Fishing Trolleys in Deep Sea

Sulata Mitra[1], Sumanta Pyne[2] and **Arkadeep Goswami[3]**

Submitted in May 2010; Accepted in November 2010

Abstract - The present work considers a fleet of fishing trolleys. The MANEMO is the integration of mobile ad-hoc network technology and mobile network technology for maintaining the uninterrupted connectivity among the fishing trolleys in deep sea. It provides local connectivity among the fishing trolleys for offshore help using mobile ad-hoc network and global connectivity among the fishing trolleys for onshore help using mobile network. Each fishing trolley works as a separate node in case of local communication whereas all the fishing trolleys form a mobile network in case of global communication. The routing algorithm in MANET environment selects an optimal route for a session before starting transmission of data packets associated with that session. It uses route maintenance algorithm to detect whether a trolley associated with an existing route is going out of the communication range during the ongoing session in advance before the existing route fails completely. Such consideration helps to reduce the data packet loss. If the local communication among trolleys fails due to the change in network topology the rest of the communication can be maintained globally which helps to provide the uninterrupted connectivity to the fishermen in the deep sea. The performance of the proposed scheme is evaluated on the basis of initial path set up time and average packet delay.

Index Terms - MANET, MObile NEtwork, Basic POSANT routing algorithm, WLAN, WiFi / WiMAX

1.0 INTRODUCTION

In today's society many people spend a lot of time in vehicle. They need network connectivity for various safety and non-safety applications. The MObile NEtwork technology (NEMO) and Mobile Ad-hoc NETwork (MANET) technology are integrated in MANEMO to maintain global and local connectivity among vehicles. The vehicles can communicate using MANET when they are close enough. They can communicate using NEMO for getting help like weather forecast, accidents, and attack from intruder etc. They also use NEMO for communication in case the MANET technology fails to maintain local communication due to the change in network topology.

Several such integration schemes have been reported so far. The mobile routers (MRS) [1] deployed in car not only provide external communication access but also manage the mobility of the whole network transparently. In [2] the MANET routing protocol is used to achieve multi hop communication between a MANET node and an attachment point in case the attachment point is within the coverage area of MANET. The multi hop path between a MANET node and an attachment point is established through NEMO in case the attachment point is out of the coverage area of MANET. In this scheme NEMO environment provides infrastructure connectivity whereas the MANET environment deals with routing issues internally to a mobile network. The authors did not present any simulation results. A vehicular network integration of VANET with NEMO is proposed in [3]. In this scheme the receive on most stable group path and link expiration time threshold are used to find the most stable link in the VANET environment. But the proposed VANET routing is unable to offer best throughput. The in vehicle router system to support network mobility is proposed in [4]. This scheme is the combination of Mobile IPv6, Interface switching and Prefix Scope Binding update to achieve end to end permanent connectivity and migration transparency. A post-disaster network is formed in [5] by integrating NEMO and VANET to support streaming video, VoIP and short message equipped with global positioning system (GPS) to view the location of vehicles in Google map. The integration of NEMO and MANET is proposed in [6] to form rescue team communication and the experiment is conducted over a mountain rescue team. Tsukada et al. described the co-operation between MANET and NEMO [7] to support route optimization and multi homing. The authors used the optimized link-state routing (OLSR) algorithm for the MANET environment. But the transmission of control packets is required for route existence verification if the data packets are transmitted at a slow speed which increases the overhead of the OLSR algorithm. They mainly focused in defining the architecture and the purpose of integration. The authors did not consider the detailed usage of combination and their utility experimentally.

The present work considers a fleet of fishing trolleys as vehicle. All the fishing trolleys belong to the same fishing harbor, which is their home network associated with a Home Agent (HA). A MR is associated with each trolley. Each MR works as an individual node in case of local communication using MANET interface. All MRs form a mobile network which is connected with the HA through Internet. They communicate globally with HA through Internet using NEMO interface and MR-HA tunnel. One of the trolleys works as a special fixed node (SFN) for MANET and as a local fixed node (LFN) for NEMO. It maintains the optimal route (OR) information for both MANET and NEMO. It is not taking any part in communication. The access router (AR) installed in the

[1, 2,3] *Department of Computer Science and Technology,* Bengal Engineering and Science University, Shibpur, West Bengal, INDIA
E-Mail: [1]*sulata@cs.becs.ac.in*

island forms a foreign network for the fishing trolleys and is considered as Island Side Unit (ISU).The AR installed in the shore forms a foreign network for the fishing trolleys and is considered as Shore Side Unit (SSU). The ISU maintains connectivity between the fishing trolleys and the HA through Internet in case the fishing trolleys are closer to the Island. The SSU maintains connectivity between the fishing trolleys and the HA through Internet in case the fishing trolleys are closer to the shore.

The WLAN is preferred for MANET due to its lesser communication range and power consumption [8] whereas WiFi/WiMAX is preferred for NEMO due to its higher communication range and power consumption [8]. The cost and power consumption of maintaining local communication among trolleys is reduced by using WLAN for MANET in the present work. Moreover such communication among trolleys is secured as it does not need Internet access. So the communication among trolleys is maintained locally in most of the cases. But the route failure may occur in MANET during local communication among trolleys due to the change in network topology. In such a situation the rest of the communication among trolleys can be maintained through HA using MR-HA tunnel if it is not possible to select an alternative route in MANET. So the integration of MANET technology and NEMO technology in the present work helps to maintain the uninterrupted connectivity among the fishermen in the deep sea.

2.0 ROUTING ALGORITHMS FOR MANET

Two different routing algorithms for MANET are proposed in the present work. The algorithms are considered for discussion in the following sections.

2.1 HA Posant Routing Algorithm

The HA is equipped with Google Map [9] and each trolley is equipped with GPS. A source node (S_id) sends route request message (RRM) (as discussed in section 2.1.1) to HA for the initiation of a session with a destination node (D_id). The HA triggers route selection algorithm (as discussed in section 2.1.2) to select an OR in response to RRM and sends the OR to S_id using route found message (RFM) (as discussed in section 2.1.1). The HA assigns a unique session identification (SS_id) to each session after selecting an OR for it. After receiving RFM, S_id generates Type 0 packet (T0 as discussed in section 2.1.3). The Route field of T0 contains the identification of all the nodes which are associated with OR as mentioned in the Route field of RFM by HA. S_id sends this packet to D_id through all the nodes which are identified in the Route field of T0. Each node maintains a routing table (RT) (as discussed in section 2.1.4) and inserts a record in RT after receiving T0. Both S_id and D_id associated with a particular session generate Type 1 packet (T1 as discussed in section 2.1.3) and send this packet to each other to maintain the bidirectional transmission of packets corresponding to a particular session among them using OR which is mentioned in RFM. The HA maintains a session table (ST) (as discussed in section 2.1.5) to store the information of all the ongoing sessions among nodes in MANET. The HA inserts a record in ST after selecting an OR. As soon as an ongoing session is over S_id associated with this session sends session over message (SOM) (as discussed in section 2.1.1) to HA. The HA searches ST for the record who's SS_id attribute matches with the SS_id field as mentioned in SOM and deletes that record from ST. The HA executes the route maintenance algorithm (as discussed in section 2.1.6) to detect node(s) which is associated with an existing route(s) and is going out of the communication range from its neighboring node associated with the same route during the ongoing session. In such a case the HA considers the existing route(s) as faulty and executes route selection algorithm for the selection of an alternate OR(s) to replace the faulty existing route(s). It sends the alternative OR to S_id(s) using route maintenance message (RMM) (as discussed in section 2.1.1). After receiving RMM, S_id(s) generates Type 2 packet (T2 as discussed in section 2.1.3). The N_Route field of T2 contains the identification of all the nodes which are associated with the alternative OR as mentioned in the N_Route field of RMM by the HA. S_id sends T2 to D_id through all the nodes which are identified in the N_Route field of T2 for necessary insertion or modification in their RT.

2.1.1 Message Exchange among Various Nodes

RRM contains S_id and D_id fields. RFM contains S_id, D_id, SS_id and Route fields. SOM has SS_id and F_flag fields. The F_flag field of SOM is set to indicate the end of session which is identified in its SS_id field. RMM has SS_id, S_id and N_Route fields.

2.1.2 Route Selection Algorithm

The GPS detects the current location in terms of longitude and latitude of each node. The GPS sends this information of each node to HA as soon as the current location of any node changes. The HA uses Vincenty's inverse equation [10] to calculate the distance between two neighboring nodes from their current location which is provided by GPS. The longitude and latitude of the fishing area is provided by the fishing authority to HA. The Google Map in HA shows the real time image of each node within the fishing area using the information provided by the GPS and the information provided by the fishing authority. The HA maintains a graph of nodes using their real time image which is provided by the Google Map continuously and creates a rectangular boundary around the graph of nodes. If any intruder node crosses the rectangular boundary from outside HA sends a special security signal to the node(s) closer to the intruder node. After receiving RRM the HA applies depth first search to the graph and finds all possible routes from S_id to D_id. The HA counts the number of nodes in each possible route and selects the route having minimum number of nodes as the best route. The HA uses basic POSANT [11] algorithm to determine OR in case of multiple best routes.

2.1.3 Type of Packets

T0 contains SS_id, S_id, D_id, Type and Route fields. T1 contains SS_id, Node_id, S_No, Type and PAYLOAD fields. The Node_id field is S_id in case the packet is generated by S_id and D_id in case the packet is generated by D_id. The S_No field indicates the sequence number of the packet. The PAYLOAD field contains the data corresponding to the session which is identified by SS_id. T2 has SS_id, S_id, D_id, S_No, Type, N_Route and PAYLOAD fields. The Type field in T0, T1 and T2 indicates their type.

2.1.4 Routing Table (RT)

Each record in RT has 5 attributes as shown in TABLE-1.

S_id	D_id	SS_id	SN_NH	DN_NH
S	D	s	T	E

Table 1

Let TABLE-1 is RT which is maintained by j^{th} node and it shows a record for s^{th} session. S_id and D_id which are associated with the s^{th} session are identified as S and D respectively in TABLE-1. T indicates the next hop of the j^{th} node in case of transmission from S to D and E indicates the next hop of the j^{th} node in case of transmission from D to S in TABLE-1. After receiving T0 the j^{th} node inserts a record in TABLE-1. After receiving T1 the j^{th} node searches TABLE-1 for the existing record whose SS_id attribute matches with the SS_id field as mentioned in T1. Then it compares the S_id attribute and the D_id attribute of the existing record with the Node_id field as mentioned in T1. If the Node_id field in T1 matches with the S_id attribute of the existing record the j^{th} node forwards the packet to T and if the Node_id field in T1 matches with the D_id attribute of the existing record the j^{th} node forwards the packet to E. After receiving T2 the j^{th} node searches RT for the existing record whose SS_id attribute matches with the SS_id field as mentioned in T2. If found it updates the record by replacing the old route attribute by the new route attribute as mentioned in T2. Otherwise, it inserts a new record in RT. When a node is not participating in packet transmission corresponding to a particular session, it deletes the corresponding record from RT.

2.1.5 Session Table (ST)

Each record in ST has 3 attributes as shown in TABLE-2. The Route attribute is identical to Route field in RFM. The number of records in ST depends upon the number of ongoing sessions.

SS_id	S_id	Route

Table 2

2.1.6 Route Maintenance Algorithm

The HA computes the distance between the two neighboring nodes continuously using the information provided by GPS and using the Vincenty's inverse equation. The HA considers a node as MOVE_NODE in case its distance from the neighboring node crosses a threshold. The threshold distance is computed during simulation as discussed in section 4.1.2. As soon as HA detects such a node, it searches the Route attribute of all the records in ST. It selects the record(s) whose Route attribute contains the identification of the MOVE_NODE. If found it retrieves the selected record(s). It executes route selection algorithm for the selection of an alternative OR(s) before the existing route(s) fails completely. Such advance selection of an alternative route helps to reduce packet loss of a session. The HA updates the selected record(s) by replacing the old route attribute by the new route attribute in ST.

The installation of Google Map along with GPS increases the cost of the system. Moreover the GPS may not be able to work properly in situations such as underwater conditions e.g. within submarines. In such a situation radio detection and ranging (RADAR) works well. The RADAR POSANT routing algorithm is considered for discussion in section 2.2.

2.2 Radar Posant Routing Algorithm

Each node is equipped with two antennas, one at the front end and one at the rear end of the node. Both the antenna can work as transmitter as well as receiver to achieve bidirectional transmission of packets corresponding to a particular session.

S_id triggers route selection algorithm (as discussed in section 2.2.1) by forwarding ant packet towards D_id for the initiation of a session as in basic POSANT routing algorithm. D_id selects an OR and sends it to SFN (SFN_id) using D_to_SFN message (as discussed in section 2.2.2). The SFN sends OR to S_id using SFN_to_S message (as discussed in section 2.2.2). The SFN assigns a unique SS_id to each session after receiving OR from D_id. After receiving SFN_to_S message S_id generates T0 (as discussed in section 2.1.3). The Route field of this packet contains the identification of all the nodes which are associated with OR as mentioned in the Route field of SFN_to_S message by SFN. S_id sends T0 to D_id through all the nodes which are identified in the Route field of T0. Each node maintains RT (as discussed in section 2.1.4) and inserts a record in RT after receiving a T0. Both S_id and D_id associated with a particular session generate T1 (as discussed in section 2.1.3) and send T1 to each other to maintain the bidirectional transmission of packets corresponding to a particular session among them using OR as mentioned in SFN_to_S message. The SFN maintains a ST (as discussed in section 2.1.5) to store the information of all the ongoing sessions among nodes in MANET. The SFN inserts a record in ST after receiving D_to_SFN message. As soon as an ongoing session is over S_id associated with this session sends SOM (as discussed in section 2.1.1) to SFN. The SFN searches ST for the record who's SS_id attribute matches with the SS_id field as mentioned in SOM and deletes that record from ST. Each node associated with an existing route executes route maintenance algorithm (as discussed in section 2.2.3) to detect whether its neighboring node associated with the same route is going out of the communication range during the ongoing session and sends an alarming signal to the neighboring node. In response the neighboring node sends its identification to SFN. In such a case the SFN considers the existing route as faulty and sends SFN_ALT_ROUTE message (as discussed in

section 2.2.2) to S_id which is associated with the faulty route for the execution of the route selection algorithm. S_id executes route selection algorithm for the selection of an alternative OR to replace the faulty existing route. After selecting the alternative OR S_id generates T2 (as discussed in section 2.1.3). The N_Route field of T2 contains the identification of all the nodes which are associated with the alternative OR as selected by S_id. S_id sends T2 to D_id through all the nodes which are identified in the N_Route field for necessary insertion or modification in their RT.

2.2.1 Route Selection Algorithm

S_id forwards the ant packet through all the possible routes between S_id and D_id associated with a particular session as in basic POSANT routing algorithm. The ant packet deposits pheromone value to each link. The maximum pheromone value is deposited to the link having smallest length. The ant packet has 6 fields as shown in Fig.1.

S_id	D_id	A_F	T_S	Route	P_C

Figure 1: Format of ant packet

The A_F field is set to indicate the type of the packet as ant. Let i^{th} node receives an ant packet from k^{th} node and j^{th} node is the successor of the i^{th} node. The i^{th} node mentions the current time stamp in the T_S field of the ant packet and forwards it to the j^{th} node. The i^{th} node adds its identification in the Route field of the ant packet. The i^{th} node computes the difference in time stamp (Diff_time) between the current time stamp corresponding to the time of receiving the ant packet by it and the time stamp in the T_S field of the ant packet as mentioned by the k^{th} node. The i^{th} node also computes its distance from the k^{th} node (D_{ik}) by multiplying Diff_time and the speed of electromagnetic signal {mt./sec}(as packets constitute of digital bits and are sent using electromagnetic signals). The bit error rate increases rapidly when the distance between the two neighboring nodes in the WLAN environment is greater than 45 meters [12]. So in the present work the pheromone value of the link between the i^{th} node and the k^{th} node (P_value_{ik}) is assumed as 20 if $D_{ik}<45$ otherwise it is assumed as 1. The i^{th} node also multiplies the value in the P_C field of the ant packet as mentioned by the k^{th} node by P_value_{ik}. At i^{th} node the value in the P_C field of the ant packet indicates the pheromone concentration of the route from S_id up to the i^{th} node.

The D_id receives multiple ant packets through all possible routes between S_id and D_id. It compares the P_C value of all the received ant packets. The route field in the ant packet having maximum P_C value is selected as OR.

2.2.2 Message Exchange among Various Nodes

D_to_SFN message contains S_id, SFN_id and Route fields. SFN_to_S message contains SS_id, S_id, SFN_id and Route fields. SFN_ALT_ROUTE message has S_id, SFN_id and SS_id fields.

2.2.3 Route Maintenance Algorithm

Each node associated with an existing route computes its distance from the neighboring node which is associated with the same route using mono-static equation [13]. The mono-static equation used by the RADAR antennas in this scheme is as follows:

$P_r = 10 \log_{10}[(P_t G_t G_r \lambda^2 \sigma)/((4\pi)^3 R^4)]$

$= 10 \log_{10}[P_t G_t G_r \{(\sigma c^2)/((4\pi)^3 f^2 R^4)\}]$

where, P_r = Received peak power, P_t = Transmitted peak power, G_t = Gain of transmitter antenna (dBi), G_r = Gain of receiver antenna (dBi), λ = Transmitted wavelength (m, cm, in, etc.), σ = Radar cross-section of target - RCS (m^2, cm^2, in^2, etc.), R = Range (m, cm, in, etc.), c = speed of light. The parameter values of the mono-static equation are assumed as follows: P_t = 20 dbm, $G_t = G_r$ =16 dbi, λ = 15 cm, σ = 2.5 m^2 and c = 3* 10^8 meter/sec. The parameter R indicates the distance between the two neighboring nodes. P_r is measured at the receiving antenna and R is computed using the mono-static equation using the known value of all the other parameters.

Each node associated with an existing route also computes its angle with the neighboring node which is associated with the same route using Pythagoras theorem. In ΔABC (Fig.2) the vertex B and the vertex C represent the location of the front end and rare end antenna in a node. The vertex A represents the location of the neighboring node. In ΔABC the side AB (=c) represents the distance between the neighboring node and the front end antenna. P_r is measured at the front end antenna and c is computed using mono-static equation. The side AC (=b) represents the distance between the neighboring node and the rare end antenna. P_r is measured at the rare end antenna and b is computed using mono-static equation. The side BC (=a) represents the length of the node (trolley). AP (=h) is perpendicular to BC.

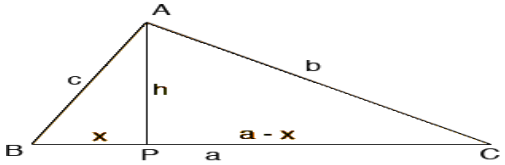


Figure 2: Triangular representation of the angle calculation process.

The angle between the two neighboring nodes (angle C) is $C= \cos^{-1}\{(a^2+b^2-c^2)/ 2ab\}$ using Pythagoras theorem. A node sends an alarming signal to its neighboring node (RECEIVED_NODE) in the direction of the angle as computed by the Pythagoras theorem in case its distance from the RECEIVED_NODE crosses a threshold. The threshold distance is computed during simulation as discussed in section 4.1.2. The RECEIVED_NODE sends its Node_id to SFN. The SFN searches the Route attribute of all the records in ST. It selects the record(s) whose Route attribute contains the identification of the RECEIVED_NODE. If found it retrieves the selected record(s) and sends SFN_ALT_ROUTE message to S_id(s) associated with the selected record(s) to execute route selection algorithm for the selection of an alternative OR(s) before the existing route(s) fails completely. Such

advance selection of an alternate route helps to reduce packet loss of a session. S_id forwards the ant packet towards D_id. D_id selects an alternative OR and sends it to SFN. The SFN sends the alternative OR to S_id. The SFN updates the selected record(s) by replacing the old route attribute by the new route attribute in ST.

2.3 COMPARISON OF ROUTING ALGORITHMS

The performance of ANTNET, GPSR, ANTHOCNET and basic POSANT routing algorithms are compared on the basis of delivery rate, convergence time and algorithm overhead in [11]. In this section the basic POSANT routing algorithm [11], HA POSANT routing algorithm and RADAR POSANT routing algorithm are compared on the basis of storage requirement, RT searching time and time complexity of the algorithm.

2.3.1 Storage Requirement

In basic POSANT routing algorithm each node maintains a forward RT to send packets from S_id to D_id and a backward RT to send packets from D_id to S_id. Each record in RT has 3 attributes as shown in TABLE-3. Let TABLE-3 is the forward RT at j^{th} node. The Node_Address attribute is the address of D_id in case of forward RT. The Next_Hop attribute is the address of the next hop node from j^{th} node towards destination which is identified by the Node_Address attribute. The Pheromone_Value attribute indicates the pheromone value corresponding to the next hop node which is indicated by the Next_Hop attribute. The Node_Address attribute and the Next_Hop attribute are 128 bit IPv6 address. The maximum pheromone value which is deposited to a link is 20 as discussed in the section 2.2.1 and the number of bits require to represent the maximum pheromone value is 5. So the length of each record in the forward RT at any node is 261 bits. The number of records in the forward RT at j^{th} node for a single session depends upon the number of possible next hop nodes from j^{th} node towards destination. So the storage requirement per forward RT is (261*number of possible next hop towards D_id) bits.

Node_Address (128 bits)	Next_Hop (128 bits)	Pheromone_Value (5 bits)

Table 3

Let TABLE-3 is the backward RT at j^{th} node. The Node_Address attribute is the address of S_id in case of backward RT. The Next_Hop attribute is the address of the next hop node from j^{th} node towards source which is identified by the Node_Address attribute. The number of records in the backward RT at j^{th} node for a single session depends upon the number of possible next hop nodes from j^{th} node towards source. The storage requirement per backward RT is (261*number of possible next hop towards S_id) bits. So the storage requirement for each bidirectional session is 261*(number of possible next hop towards destination + number of possible next hop towards source) bits.

In HA POSANT routing algorithm and RADAR POSANT routing algorithm each node maintains a single RT as shown in TABLE-1. The S_id, D_id, SN_NH and DN_NH are 128 bits IPv6 addresses. Now for 1000 number of different bidirectional sessions the number of bits requires to represent SS_id is 10. So the length of each record in RT is 522 bits. There is a single record for each bidirectional session in RT and so the storage requirement for each bidirectional session is 522 bits. The storage requirement for each bidirectional session in basic POSANT routing algorithm is greater than the storage requirement in HA POSANT routing algorithm and RADAR POSANT routing algorithm if the number of next hop nodes from j^{th} node towards S_id or D_id is greater than unity in TABLE-3.

2.3.2 Rt Searching Time

Let in case of basic POSANT routing algorithm the number of forward ongoing session through j^{th} node as an intermediate node is m and the number of next hop from j^{th} node towards D_id is n. So at j^{th} node the forward RT contains m*n number of records and the time complexity to select the desired record from the forward RT is $O(\log_2 m*n)$. The j^{th} node compares the pheromone value of all the n number of next hops and selects the optimal next hop having the maximum pheromone value. The link between j^{th} node and the selected optimal next hop is considered as the optimal outgoing link towards D_id. The time complexity to select the optimal outgoing link from the forward RT at j^{th} node is $O(n^2)$. So the total time complexity at j^{th} node for the selection of an optimal outgoing link is $O(\log_2 m*n+n^2)$.
In case of HA POSANT routing algorithm and RADAR POSANT routing algorithm RT at j^{th} node contains m number of records and the time complexity to select the desired record from RT is $O(\log_2 m)$.
So the time complexity of searching RT is higher in basic POSANT routing algorithm than in HA POSANT routing algorithm and RADAR POSANT routing algorithm.

2.3.3 TIME COMPLEXITY OF THE ALGORITHM

In case of basic POSANT routing algorithm RT at each node contains the possible next hop and their pheromone value. During the ongoing session RT at each node is searched for the selection of an optimal outgoing link. In case of HA POSANT routing algorithm and RADAR POSANT routing algorithm RT at each node contains OR. During the ongoing session RT at each node is searched for OR. So OR is selected during the ongoing session in basic POSANT routing algorithm which increases its time complexity than the HA POSANT routing algorithm and RADAR POSANT routing algorithm. The time complexity of the HA POSANT routing algorithm is higher due to the time complexity of the depth first search than the time complexity of the RADAR POSANT routing algorithm

3.0 ROUTING ALGORITHM FOR NEMO

The LFN inside the mobile network uses route optimization algorithm [14] for the selection of an OR to maintain global communication among trolleys in NEMO.

4.0 SIMULATION

The simulation experiment is performed in two different phases. The performance of the basic POSANT [11] routing algorithm, HA POSANT routing algorithm and RADAR POSANT routing algorithm are compared in Phase 1. The performance of MANEMO has been studied in Phase 2. The simulation experiment is conduced for 1280 number of packets and 6 numbers of trolleys in both the phases. The MANET in the proposed scheme is the combination of some interconnected processing units. The processing units are HA, S_id and intermediate nodes associated with OR in case of HA POSANT routing algorithm. The processing units are SFN, S_id, D_id and intermediate nodes associated with OR in case of RADAR POSANT routing algorithm. The NEMO in the proposed scheme is the combination of some interconnected processing units such as MNN, LFN and MR. Each processing unit in MANEMO is treated as thread and the MANEMO is considered as a producer-consumer problem in a large scale. In HA POSANT routing algorithm the send request thread at S_id sends RRM to HA. The receive request thread at HA searches for RRM. If found it selects OR and sends RFM. The receive route thread at S_id searches for RFM. If found the forward packet thread at S_id forwards packet to the ingress interface of its associated MR. The transfer packet thread at each node transfers the packet from the ingress interface to the egress interface of the associated MR. In RADAR POSANT routing algorithm the source request thread at S_id forwards ant packet towards D_id. D_id selects OR and sends D_to_SFN message using route send thread. The SFN send thread at SFN searches for D_to_SFN message. If found it sends SFN_to_S message. The receive route thread at S_id searches for SFN_to_S message. If found the forward packet thread at S_id forwards packet to the ingress interface of its associated MR. The transfer packet thread at each node transfers the packet from the ingress interface to the egress interface of the associated MR. The processing units and the corresponding threads in NEMO are discussed in [14].

4.1 Experimental Results for Phase 1

The simulation experiment is conducted to compare the performance of the three routing algorithms for MANET.

4.1.1 Initial Path Set Up Time

It is the time to set up an OR for the initiation of a session. Fig.3 shows the plot of initial path set up time for all the three routing algorithms. The basic POSANT routing algorithm needs the transmission of forward ant packets and backward ant packets for route selection. The HA POSANT routing algorithm needs the transmission of RRM and RFM among nodes for route selection instead of the transmission of forward ant packets and backward ant packets which reduces the initial path set up time of HA POSANT routing algorithm than basic POSANT routing algorithm. The RADAR POSANT routing algorithm needs the transmission of forward ant packets for initial route selection which increases the initial path set up time of RADAR POSANT routing algorithm than HA POSANT routing algorithm. But the transmission of backward ant packets is not required in RADAR POSANT routing algorithm which reduces the initial path set up time of RADAR POSANT routing algorithm than basic POSANT routing algorithm. It can be observed from Fig.3 that the initial path set up time of basic POSANT routing algorithm is higher and of HA POSANT routing algorithm is lesser. The initial path set up time of RADAR POSANT routing algorithm is higher than HA POSANT routing algorithm but lesser than basic POSANT routing algorithm.

4.1.2 Average Packet Delay

Fig.4 shows the plot of average packet delay vs. simulation time for all the three routing algorithms. It can be observed from Fig.4 that the average packet delay is higher in basic POSANT routing algorithm as it selects OR during the ongoing session than the other two routing algorithms.

Fig.5 shows the plot of average packet delay vs. the number of packets received for all the three routing algorithms. The speed of the node is assumed as 6 km/hr. If a node associated with OR of a particular session starts to move in the opposite direction of another node associated with the same route, their relative velocity becomes 12 km/hr. The communication range of WLAN is assumed as 100 m. So the failure occurs in the existing route when the two neighbouring nodes associated with the same route go out of the communication range with relative velocity 12 km/hr after 30 sec. It can be observed from Fig.3 that the initial path set up time for HA POSANT routing algorithm is 120 msec and for RADAR POSANT routing algorithm is 150 msec. The two neighbouring nodes having relative velocity 12 km/hr covers a distance of 0.4 m (≈ 1 m) in 120 msec for HA POSANT routing algorithm and .5 m (≈1 m) in 150 msec for RADAR POSANT routing algorithm. So the packet loss and average packet delay of an ongoing session can be minimized by triggering the route maintenance algorithm in advance when the two neighbouring nodes associated with the same OR are at a threshold distance of 99 m (100 m-1 m) from each other. During simulation it has been observed that the time requires to transmit a single packet using basic POSANT routing algorithm is 40 msec whereas the time requires for transmitting a single packet using HA POSANT routing algorithm and RADAR POSANT routing algorithm is 30 msec. So the number of packets that can be transmitted using basic POSANT routing algorithm in 30 sec is 700 whereas the number of packets that can be transmitted using HA POSANT routing algorithm and RADAR POSANT routing algorithm in 30 sec is 950 before the failure occurs in the existing route.

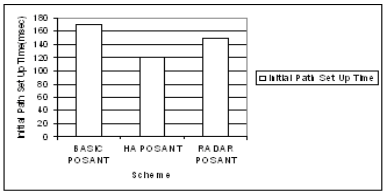


Figure 3: Initial path set up times

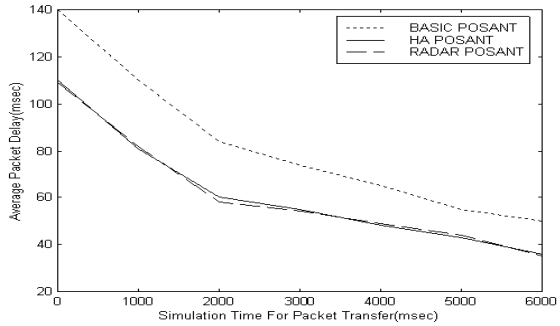


Figure 4: Average packet delay vs. Simulation time

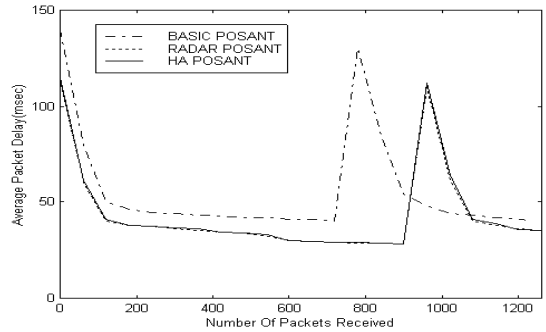


Figure 5: Average packet delay vs. Number of packets received

It can be observed from Fig.5 that the initial average packet delay is higher in basic POSANT routing algorithm due to its higher initial path set up time as discussed in section 4.1.1 than the other two routing algorithms. The new route is selected in basic POSANT routing algorithm after the transmission of 700 packets. The new route is selected in HA POSANT routing algorithm and RADAR POSANT routing algorithm after the transmission of 950 packets. The average packet delay in the new route for basic POSANT routing algorithm is also higher due to its higher initial path set up time than the other two routing algorithms.

4.1.3 Percentage of Successfully Delivered Packets

TABLE-4 shows the percentage of successfully delivered packets for the 3 routing algorithms. The new route discovery process starts after the failure occurs in the existing route in basic POSANT routing algorithm. So the data packets that are generated during the time interval between the occurrence of route failure and finding out a new route are lost. The route maintenance algorithm selects an alternative OR in advance before the failure occurs in the existing route in HA POSANT routing algorithm and RADAR POSANT routing algorithm. So the percentage of successfully delivered packets is lesser in basic POSANT routing algorithm than the other two routing algorithms.

Scheme	Packet generated	Packet delivered	% of successfully deliver packets
13	1280	1203	94%
HA	1280	1280	100%
RADAR	1280	1280	100%

Table 4

4.2 Experimental Results for Phase

The simulation experiment is conducted to find the path set up time and average packet delay in MANEMO.

4.2.1 Path Set Up Time

Fig.6 shows the path set up time in MANEMO. When a S_id wants to initiate a session with D_id, MANEMO searches MANET for the selection of an OR. If found, OR is selected otherwise it searches NEMO for the selection of an OR. If the selected OR in MANET fails due to the change in network topology, MANEMO searches MANET again for the selection of an alternative OR. If found the alternative OR is used to maintain the rest of the communication. Otherwise NEMO is searched for the selection of the alternative OR. It can be observed from Fig.6 that the path set up time in NEMO is higher due to the Internet access overhead than the path set up time in MANET.

4.2.2 Average Packet Delay

Fig.7 shows the plot of average packet delay vs. the number of packets received in MANEMO. The maximum number of packets that can be transmitted using HA POSANT routing algorithm and RADAR POSANT routing algorithm for MANET is 950 as discussed in section 4.1.2. In the worst case no alternative route is found in MANET and the rest of the packets are transmitted using the alternative route in NEMO. It can be observed from Fig.6 that the initial path set up time in MANET is 150 msec and in NEMO is 191 msec. So the total time required to set up an alternate route is 341 msec. The two neighboring nodes having relative velocity 12 km/hr as discussed in section 4.1.2 covers a distance of 1 m in 341 msec. So the packet loss and average packet delay of an ongoing session can be minimized by triggering the route maintenance algorithm in advance when the two neighboring node associated with the same OR are at a threshold distance of 99 m from each other. But at heavy load the initial path set up time in both MANET and NEMO increases which needs a reduction in threshold distance to minimize packet loss and average delay in communication. So the threshold distance is assumed as 95 m during simulation. It can be observed from Fig.7 that the initial average packet delay is higher in NEMO due to its higher initial path set up time as discussed in section 4.2.1 than in MANET. The new route is selected in NEMO after the transmission of 950 numbers of packets using MANET which can also be observed from Fig.7.

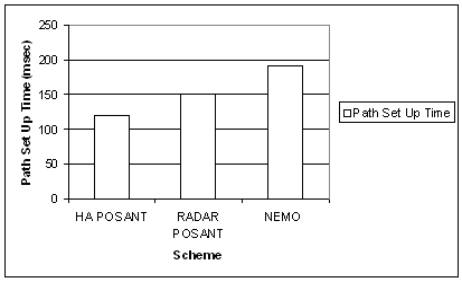


Figure 6: Path set up times for MANET (using HA MANET and RADAR MANET) and NEMO.

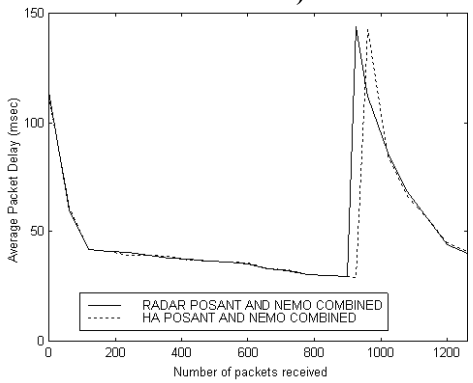


Figure 7: Average packet delay vs. Number of packets received in MANEMO

It can be observed from Fig.5 that the initial average packet delay is higher in basic POSANT routing algorithm due to its higher initial path set up time as discussed in section 4.1.1 than the other two routing algorithms. The new route is selected in basic POSANT routing algorithm after the transmission of 700 packets. The new route is selected in HA POSANT routing algorithm and RADAR POSANT routing algorithm after the transmission of 950 packets. The average packet delay in the new route for basic POSANT routing algorithm is also higher due to its higher initial path set up time than the other two routing algorithms.

8.0 CONCLUSION

The proposed work integrates MANET and NEMO technology to maintain the uninterrupted connectivity among fishing trolleys in deep sea. Two different routing algorithms are proposed for MANET and their performances are compared with the basic POSANT routing algorithm. Several such integrated schemes have already been proposed so far but most of the researchers define the architecture and the purpose of integration. They did not present any simulation results. But the proposed integrated scheme has been simulated to observe the initial path set up time and average packet delay. The performances of the proposed routing algorithms are evaluated considering only the data class of traffic. It can be extended by considering other traffic classes during simulation.

REFERENCES

[1]. T. Taleb, E.Sakhaee, N.Kato, Y.Nemoto and A.Jamalipour, "A Stable Routing Protocol to Support ITS Services in VANET Networks", IEEE Transaction on Vehicular Technology, vol.56. No 6, November 2007.

[2]. R.Baldessari, A.Festag and J.Abille, “NEMO meets VANET: A Deploy ability Analysis of Network Mobility in Vehicular Communication”, pp.375-380, ITST, July 2007.

[3]. C-S. Li**,** U. Lin and H-C. Chao,“Vehicular Network Integration of VANET with NEMO Consideration", 2008 International Computer Symposium (ICS2008).

[4]. K. Mitsuya, K. Uehara and J. Murai, “The In-vehicle Router System to support Network Mobility”, LNCS vol. 2662, pp. 633-642, October 2003.

[5]. K.Kanchanasut, T. Wongsaardsakul, M. Chansutthirangkool, A.Laouiti, H.Tazaki and K.R.Arefin, “DUMBO II: A V-2-I Emergency network”, AINTEC’08, November 18-20, 2008, Bangkok, Thailand.

[6]. B. McCarthy, C. Edwards and M. Dunmore, “The Integration of Ad-hoc (MANET) and Mobile Networking (NEMO): Principles to Support Rescue Team Communication”, ICMU, 2006.

[7]. M.Tsukada, O.Mehani and T.Ernst, “Simultaneous Usage of NEMO and MANET for vehicular communication”, WEEDEV 2008 Innsbruck, Austria.

[8]. Wikipedia.org: WLAN, WiFi and WiMAX.

[9]. K.R.Arefin, T.Wongsaardsaku and K.Kanchanasut, “Vehicle-to-Infrastructure MANET with group mobility for emergency multimedia communication”, Asian Internet Engineering Conference Bangkok, Thailand pp. 46-54, 2009, ISBN: 978-1-60558-614-4.

[10]. Wikipedia.org: Vincenty’s Equation

[11]. S. Kamali and J. Opatrny, “A Position Based Ant Colony Routing Algorithm for Mobile Ad-hoc Networks”, Journal of Networks, vol.3, no.4, April 2008.

[12]. J-P. Ebert, S. Aier, G. Kofahl, A. Becker, B. Burns, and A. Wolisz, “Measurement and Simulation of the Energy Consumption of an WLAN Interface”, TKN Technical Report TKN-02-010, Technical University Berlin, Telecommunication Networks Group, Berlin, June 2002.

[13]. http://www.rfcafe.com/references/electrical/radar-eqn.htm, Radar Equation, 2-way.

[14]. S.Mitra and S.Pyne, “Fuzzy Logic Based Route Optimization in a Multihomed Mobile Networks", Wireless Network, Springer Netherland, vol.17, no.1, 2011.

Dynamic Data Updates for Mobile Devices by Using 802.11 Wireless Communications

B. V. Ramanamurthy[1], K. Srinivas Babu[2] and **Mohammed Sharfuddin[3]**

Submitted in May 2010; Accepted in December 2010

Abstract - Mobile devices are used for conveying important information. Opportunity exist to introduce users to different application of resource constraint mobile device Currently, the client is forced to continuously poll for updates from potentially different data sources, such as, e-commerce, on-line auctions, stock and weather sites, to stay up to date with potential changes in content. We employ a pair of proxies, located on the mobile client and on a fully-connected edge server, respectively, to minimize the battery consumption caused by wireless data transfers to and from the mobile device. The client specifies his interest in changes to specific parts of pages by highlighting portions of already loaded web pages in her browser. The edge proxy polls the web servers involved, and if relevant change have occurred, it aggregates the updates as one batch to be sent to the client. The proxy running on the mobile device can pull these updates from the edge proxy, either on-demand or periodically, or can listen for pushed updates initiated by the edge proxy. We also use SMS messages to indicate available updates and to inform the user of which pages have changed.

Index Terms - Mobile wireless communication, proxy Process, caching, pre fetching, energy measurement.

1.0 INTRODUCTION

In these we introduce an automated and efficient approach for browsing HTML pages with dynamically changing content on mobile devices. Following the fluctuations of the favorite currency, stock value, or auction currently requires the user to reload all the pages in order to capture any changes to the data. The costs of these data transfers to the user come in many forms, including slow data access, excessive battery consumption on the device and inconvenience due to the user's active involvement in constant data reload to be seamlessly updated only when content of interest to the user changes. Our approach greatly reduces the costs of updates by: i) allowing the users to mark the parts each page that are of interest to them, ii) off loading the task of Determining when those parts have changed to a resource-rich proxy and iii) leveraging the proxy for batching those updates and sending them to the user's device periodically. We expect that our system will be useful in two kinds of browsing situations: Our first target is providing seamless low-cost content updates during active client web browsing. Imagine a user browsing dynamic content on her PDA during her daily commute or at an airport terminal waiting for her flight. We leverage our resource-rich proxy to save data Transfers for both the case where the user wants to keep up to date with rapidly changing content for her favorite pages as well as for the case of browsing to random pages.

Our target scenario is automatic periodic content refresh for the user's favorite content, for subsequent browsing while disconnected. This scenario corresponds to a user carrying a handheld device in her pocket, and having her preferred content (news, weather, stocks, etc) automatically updated. We deployed an actual proxy in our lab from which our mobile device can connect using two alternative wireless networking capabilities: 802.11 and cellular communication over GPRS. Each of these networking capabilities offer different trade-offs in terms of data download costs. Specifically, access to content over cellular networks is ubiquitous and low power, but is relatively slow. On the other hand, transfers over Wi-Fi (802.11) are fast, but have high energy costs. Indeed, an 802.11 card can reduce the battery lifetime of a PDA by up to a factor of six when in continuously active mode and by a factor of nearly two when in power saving mode. We measure the data transfer and energy savings for several dynamic content refresh schemes. Specifically, we implement and compare a poll-based scheme, where the mobile proxy periodically polls the edge proxy for updates, and a push-based approach, where the edge proxy pushes updates to the device based on a schedule.[1][2].

2.0 OUR FRAMEWORK

The client interaction with many of today's web servers is repetitive in nature, such as, constantly polling an EBay auction to check the status of a bid, or refreshing a page that contains stock quotes to track the changing values of a stock. While browser caches support "get if modified since" mechanisms, this typically fails to save any data transfers due to frequent updates to parts of the page that are largely irrelevant to the user. These changes include ad banners or the time of day, and although the user may not be interested in them, they usually result in the page being reloaded almost every time

2.1 Client Interface

The user specifies her interest in changes to specific parts of each page by highlighting portions of the web page on her device screen, as illustrated in Figure 1. The end points of a highlighted region serve as the start and end points of an annotation that the system captures.

[1,2,3]*Department of Compute Science and Engineering, Guru Nanak Engineering College, Ibrahimpatnam, R. R Dist, Andhra Pradesh, INDIA*
E-Mail: [1]drbvrm@gmail.com and [3]sharfuddin_se@yahoo.com

To keep track of the mobile client's interest in specific page regions even while the content changes, we use a well documented tree technique for maintaining robust HTML Document locations . This technique has been shown to robustly keep track of a location within a web document, in the face of typical value changes to dynamic content and even in the case of structural changes to the document, such as paragraph reordering or deletion.

2.2 Architecture Components

There are two main components of our system: The mobile device proxy and the edge server proxy. The mobile proxy resides on the mobile device. It consists of a proxy that intercepts client web requests, a cache for storing the responses to previous requests, and a hardware manager which controls the state of the wireless connections available on the device. The mobile proxy's main job is to communicate with the edge server proxy and process any cache updates. The hardware manager on the mobile device is responsible for determining which wireless interface the inter proxy communication should use. The hardware manager makes its decision based on user defined preferences. The user can choose to prefer GPRS-only, WiFi-only or an adaptive GPRS/WiFi hybrid with the goal of optimizing energy consumption automatically. In the hybrid case, the hardware manager bases its decision on which interface to use on the size of the data to be transferred. A long download of a large update on GPRS may consume more energy overall than the equivalent transfer over 802.11,even if the GPRS connection uses relatively less power.

2.2.1 Mobile Device Components

1) Mobile device web browser
2) Mobile proxy
3) Cache
4) Hardware Manager

2.2.2 Edge Server Components

1) Edge server proxy
2) Cache Manager
3) Update Manager
4) Cache

The edge server proxy is placed on any well connected computer. The edge server proxy consists of four components: proxy process, cache manager, cache, and update manager. The proxy process is an event driven server which interacts with multiple clients and serves their requests either from the cache or by directly connecting to the web servers in question. The cache manager consists of an interface to the cache and a thread pool. The cache manager's responsibility is to keep the cache up to date. Each thread periodically polls the web servers that a particular cache entry references, checking for any changes. The cache stores the interest profiles for all the mobile devices that registered their interest with the edge proxy. When a cached page is changed, the update manager adds a reference to the changed content to the update batch of each mobile device that has registered interest in that particular page [2] [7].

2.3 Operation

When a mobile device first joins the system, it registers with the edge server proxy. The edge server proxy assigns each device a unique id so that it can subsequently differentiate between devices in the system. Differentiating based on IP address is not a sufficient means, since a mobile device may change IP addresses several times each day. When a request is issued by the web browser on the device, the mobile proxy checks its cache. If the cache contains the corresponding response (local cache hit), the response is returned immediately to the web browser and no wireless communication occurs. If the response is not found in the cache (local cache miss), the mobile proxy forwards the request to the edge server proxy. The edge server proxy, in turn, checks its cache for the response and returns it from its cache if it is there. Otherwise the request is forwarded to the actual web server. If the response is a HTML page, the edge server proxy pre fetches all the embedded objects within that page and batches them with the response to be delivered to the mobile client in one transmission. Any pending cache updates are also included in the batch transfer. Upon receiving the response from the edge server, the mobile proxy caches the response and updates its cache with any other additional files included in the transfer. The response is then returned to the web browser. The client proxy acknowledges the receipt of any updates, such that the edge server proxy can remove those updates from the update manager's list for that device. In our system, the mobile proxy learns that cache updates are available through three alternative means[3][6].

- Polling the edge server.
- Receiving pushed updates.
- Receiving a SMS message from the edge server.

In the polling based scheme, the mobile proxy periodically polls the edge server proxy asking whether any updates are available. This periodic content refresh occurs automatically during active browsing sessions in order to keep the local client cache up to date, and in turn to minimize client perceived staleness and waiting time. Alternatively, for the push based approach, the mobile proxy listens on a particular port for incoming updates initiated by the edge server proxy. In this situation, the edge server proxy requires a valid IP address for the client. [4]

3.1 Proxy-Based Configurations Used For Comparison

In the following section, we describe in detail the various Proxy-based and standalone configurations we use for comparison with our main approach. By gradually introducing some of the features of our main proxy approach, we are able to demonstrate what aspects contribute to the overall wireless communication savings.

3.1.1 Baseline Configuration without Proxy

In our baseline configuration, the browser running on the mobile device polls all web sites periodically for the pages Opened by the client for any change in the content. No proxies

are used in this configuration. However, the browser's cache is fully functional.

3.1.2 Simple Proxy

In this configuration, we run the two proxies, the mobile device proxy and the edge proxy, and we use the edge proxy to poll for any changes to the data occurring at each separate data source. The proxy schedules an update to be sent to the client when there is any change to a web page. The edge proxy aggregates all updates to be sent to the user as described in our main algorithm. The mobile proxy pulls updates both upon a cache miss and periodically with the same interval as that of polling in the baseline configuration.[7]

3.1.3 Intelligent Proxy

The intelligent proxy configuration is our proxy-based approach which filters out any updates to the mobile device if the parts of the page that the client is interested in have not changed. The client specifies interest by highlighting page regions through the interface.

3.1.4 Thresholds Proxy

The thresholds proxy is an enhanced intelligent proxy where the client specifies her regions of interest within a web page, but can also specify a threshold of significant change for each numerical value. All updates for numerical value changes that are below the significant change threshold are filtered out by the edge proxy. We use both a polling based and push-based thresholds proxy in our experiments. One drawback of our experimental setup is that our edge server is operating outside the Rogers GPRS network. As a result, our edge server is unable to create a connection to the device over GPRS as all incoming communication from an external source is blocked by the Rogers firewall. In order to facilitate push-based experiments over GPRS, our mobile proxy creates a persistent TCP connection with the edge server. Updates are then pushed to the mobile device over this connection. [2][5][7]

3.2 Parameters Used In Each Configuration

We use Internet Explorer (IE) as our web browser on the mobile device. However, we use a simple wrapper around it to mimic the user and drive the experiments. All communication uses HTTP/1.1. In our baseline configuration, IE is running alone on the mobile device. The web browser contains a cache of its own, and as a result, after the first round of communication, the majority of the requests consist of if modified since requests from the browser for validating the cached items. The browser is set up to visit the four sites in the trace, once every 4 minutes. This means that over the 3 hour experiment, each of the 4 websites in the trace is loaded 45 times. The period with which the pages are loaded is irrelevant, except for allowing the experiment to complete in a reasonable amount of time and to allow for full download of the respective pages over Wi-Fi or GPRS.[5][6]

3.3 Experimental Setup for Power Measurements

The most commonly used method for automated measurement of power dissipation in a mobile device uses a precision ammeter. In this traditional method, the device is powered by a low-noise constant voltage source. The precision ammeter, equipped with a serial communication interface, is placed in series with the device's power delivery path. Energy is computed as a function of the measured current and supply voltage. This approach can result in very high accuracy, low bandwidth current measurements, but it is not practical for today's low-voltage devices which typically operate from a single Lithium-Ion cell. During startup, the high in-rush current, Iin causes the device's voltage supply, Vin to drop due to the relatively large internal ammeter sensing resistance (5□) and its parasitic inductance. In many cases, this drop causes the internal power management protection circuit included in newer devices to suspend startup.Hence, the traditional power measurement technique becomes infeasible, as we experienced first-hand with our transition from an older device to a more modern version.

Calculated using formula where fs are the oscilloscope sampling frequency [2][8]

$$Etot = 1/fs * \sum_{i=1}^{n} Vin[i].Iin$$

	Transmitted (KB)	Received	Updates	Cache Hits	Misses
Without Proxy	242.4	9238.0	0	0	657
Simple Proxy	39.1	8999.4	220	521	109
Intelligent Proxy	40.2	3211.8	72	512	120
Thresholds Proxy(Poll)	37.5	886.9	11	536	105
Thresholds Proxy(Push)	36.5	886.0	11	530	105

Table 1: Experimental Results for Each Configuration

Cache hits/misses are only for mobile proxy and not the web browser's cache. Updates are the number of page changes that occurred, several updates may be sent in one batched transfer. In contrast to the data transmission graph, As a result, the simple proxy method downloads nearly the entire batch of data each period. The intelligent proxy reduces much of the wireless data received by reducing the number of updates the edge server proxy sends to the mobile client. As we can see from Table 1, [2][7]by only sending updates when parts of the page of interest to the user change, we reduce the total number of updates by a factor of 3. This translates into a 65.2% reduction in the amount of data received when compared to the baseline proxy less approach. Finally, the thresholds proxy reduces the amount of data received over the wireless link.

3.3.1 Energy Consumption

The average energy consumed by the device per download period (i.e., loading each of the 4 web sites in the browser) for the 3 hour, the baseline proxy less configuration using the 802.11 connection and using the GPRS connection, our poll-based thresholds proxy configuration using the 802.11 connection and using the GPRS connection, and our push-based thresholds proxy configuration using the 802.11 connection and using the GPRS connection.

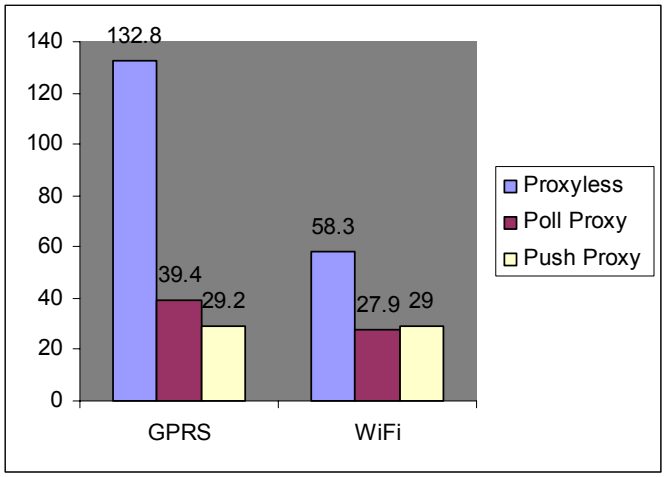


Figure 1: Average Energy Expenditure per Download Period

We can see that all configurations of the thresholds proxy are superior in energy conservation compared to their proxy less counterparts. Our proxy system reduces energy costs by factors of 2.1 and 4.5 when used over the 802.11 and GPRS connection, respectively.

3.3.2 Energy Consumption in Push Versus Poll Proxy

As stated in Fig 1, [2] the differences in energy consumption between the push-based and poll-based proxies are small for both Wi-Fi and GPRS. The push-based proxy using the GPRS connection conserves 7% energy per download period compared to the poll-based proxy. Maintaining a persistent connection with the edge server in the push based configuration is more energy-efficient than requiring the device to create a connection, request an update, and tear down the connection during each period in this case. The push based proxy using the Wi-Fi connection on the other hand, uses 4% more energy per download period than it's polling based counterpart. Constantly listening for incoming communication over the Wi-Fi connection requires more energy than periodically sending update request packets. This push based proxy could potentially save more than the polling approach, if the device used a small listening window for receiving updates [9][10].

4.0 ENERGY CONSUMPTION FOR OFF-LINE UPDATES USING THE HYBRID APPROACH

In this section, we analyze the energy consumption of the SMS based proxy system. The mobile proxy requests an update only when it receives an SMS message specifically informing it that there are updates available. The proxy uses the control information contained in this SMS message to determine the best interface to use for downloading the update. The proxy uses GPRS to download any updates under 30 KB and Wi-Fi for updates over this threshold.

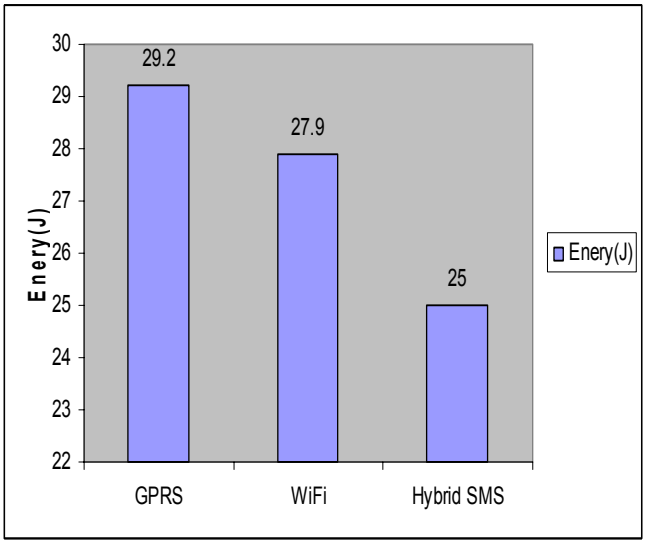


Figure 2: Average Energy Expenditure per Download Period

The average energy consumption of this proxy is stated in Fig 2, [2] along with the best results for the GPRS and Wi-Fi only proxies. The hybrid SMS proxy saves an additional 14% energy over the push based GPRS proxy and 10% over the polling Wi-Fi proxy. The savings are the result of not having to send periodic update requests, or conversely, listening over the wireless channel for incoming updates, and from using the most efficient download method for acquiring the updates when they are available.[7]

4.1 Energy Consumption for New Page Accesses

To determine the energy consumption for the case of visiting new pages i.e., cold cache miss, we ran an experiment where we viewed one of the pages in our trace with an empty browser cache and an empty proxy cache. The age used in this experiment contained 51 embedded files, consisting of dozens of small images, a couple of style sheets, and several JavaScript files. We used a proxy less setup as baseline for comparison. The total energy required to view the selected page in each configuration is Compared to the proxy less approach, the energy expenditure is reduced by 69% when using the GPRS connection in conjunction with our proxy system, gives 15% when using the Wi-Fi connection see fig 3,[2] and 12.8 for proxy system see fig 3[2].

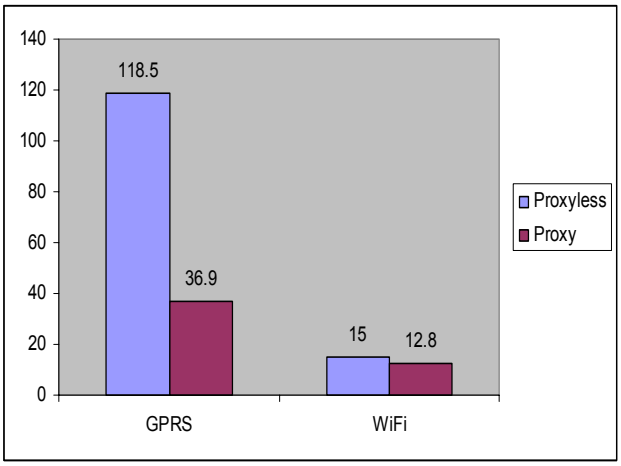


Figure 3: Total Energy Cost for Downloading a Page

5.0 CONCLUSIONS

In these we introduced an automated approach to automatic data refresh for mobile devices. Our approach is centered around a general purpose mechanism for letting the user specify her interest in changes to specific parts of pages. We avoid introducing new languages or complex interfaces that may prevent wide acceptance. Instead, the user loads her favorite pages on her mobile device browser and highlights areas of interest in those pages using the regular browser's cursor. We offload the detection of updates to content that matches the user's interest, onto a fully-connected edge proxy. Subsequently, either while the client is actively browsing or while attending to everyday activities of travel, shopping, work and play, the mobile device performs automatic data refresh transparently to the user.

Our approach is fully implemented using both Wi-Fi and GPRS communication on an actual mobile device and evaluated on real world data traces. Our results show that our general purpose proxy system saves data transfers to and from the mobile device by an order of magnitude and battery consumption by up to a factor of 4.5. These savings are due to the fact that, typically, there are frequent changes to parts of dynamic content web pages that the user is not interested in, such as the time of day or an ad banner. In addition, many changes in the n-th decimal of numerical values can be typically ignored. We have shown that, a Push-based approach provides minimal gains over a poll-based approach. Additionally, we have shown that by using the existing SMS infrastructure to deliver notifications on dynamic content changes, we can offer an energy efficient and user friendly way to keep the clients up to date with their content of interest.

REFERENCES

[1]. E. Shih, P. Bahl, and M. Sinclair, "Wake on wireless: An event driven energy saving strategy for battery operated devices," in IEEE International Conference on Mobile Computing and Networking (Mobicom), 2008.

[2]. Armstrong, T., Trescases, O., Amza, C., de Lara, E. Efficient and transparent dynamic content updates for mobile clients.Proceedings of the 4th international conference on Mobilesystems, applications and service, pages 56-68. 20066]

[3]. Thomas A. Phelps and Robert Wilensky, "Robustintra document locations," in Proceedings of the 9th international World Wide Web conference on Computer networks, Amsterdam, The Netherlands, The Netherlands, 2007, pp. 105-118, North-Holland Publishing Co.

[4]. ResearchinMotion,"Blackberry," http://www.blackberry.com.

[5]. C Perkins, "IP Mobility Support," RFC 2002, Oct. 2005, ftp://ftp.isi.edu/in-notes/rfc2002.txt.

[6]. Barron C. Housel and David B. Lindquist, "Web express: a system for optimizing web browsing in a wireless environment," in MobiCom '96: Proceedings of the 2nd annual international conference on Mobile computing and networking, 2000, pp. 108-116.

[7]. Marcel C. Rosu, C. Michael Olsen, Chandrasekhar Narayanaswami, and Lu Luo, "Pawp: A power aware web proxy for wireless LAN clients." In 6th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 2004.

[8]. Rajiv Chakravorty, Suman Banerjee, Pablo Rodriguez, Julian Chesterfield, and Ian Pratt, "Performance optimizations for wireless wide-area networks: comparative study and experimental evaluation," in MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking, New York, NY, USA, 2004, pp. 159-173, ACM Press.

[9]. R. Agrawal and E. L. Wimmers, "A framework for expressing and combining preferences," in Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, August 2000.

[10]. Mitch Cherniack, Eduardo F. Galvez, Michael J.Franklin, and Stan Zdonik, "Profile-driven cache management," in International Conference on Data Engineering (ICDE), 2003.

Simulation and Proportional Evaluation of AODV and DSR in Different Environment of WSN

Pranav M. Pawar[1], Smita Shukla[2], Pranav Kulkarni[3] and **Adishri Pujari[4]**

Submitted in May 2010; Accepted in November 2010

Abstract - ***Simulation and comparison of the routing protocols for network topology hold a significant position in the performance evaluation of wireless networks. This paper, discusses performance evaluation of Ad-hoc on demand Distance Vector (AODV) and Dynamic Source Routing (DSR), routing protocols for static WSN using NS-2. Energy efficiency, latency, throughput and fairness characteristics in different conditions are investigated under different load conditions on two-hop and multi-hop network. The comparison results reveal that AODV performs better in the network with strict requirement on time, whereas DSR is more adaptable in the networks with high throughputs and energy constraints.***

Index Terms - Wireless Sensor Network (WSN), Dynamic Source Routing (DSR), Ad-Hoc On-demand Distance Vector (AODV), energy efficiency, latency, throughput, fairness, NS-2 (network simulator-2)

1.0 INTRODUCTION

Wireless sensor networking is an emerging technology that has a wide range of potential applications including environment monitoring, smart spaces, medical systems and robotic exploration [6].

Such networks will consist of large numbers of distributed nodes that organize themselves into a multi-hop wireless network. Each node has one or more sensors, embedded processors and low-power radios, and is normally battery operated. Typically, these nodes coordinate to perform a common task. Due to the energy constraints wireless sensor networks have to take energy consumption factor in to consideration while performing various tasks [6]. Hence these are Energy-Aware Wireless Sensor Networks.

While many aspects of WSN have already been investigated, this paper concentrates on the performance characteristics of the routing protocols, in particular on the AODV and DSR protocols.

AODV is a distance vector type routing [3]. It does not require nodes to maintain routes to destinations that are not actively used. The protocol uses different messages to discover and maintain links: Route Requests (RREQs), Route Replies(RREPs), and Route Errors (RERRs). These message types are received via UDP, and normal IP header processing applies. DSR protocol works "ON Demand", i.e. without any periodic updates. Packets carry along the complete path they should take. This reduces overhead for large routing updates at the network. The nodes store in their cache all known routes. The protocol is composed of route discovery and route maintenance [3].

Both the protocols are implemented in the network layer and the MAC layer protocol used is 802.11. The IEEE 802.11 Standard is by far the most widely deployed wireless LAN protocol. This standard specifies the physical, MAC and link layer operation. Multiple physical layer encoding schemes are defined, each with a different data rate. At the MAC layer IEEE 802.11 uses both carrier sensing and virtual carrier sensing prior to sending data to avoid collisions.

The scope of the paper is to simulate the AODV and DSR protocols and analyse their performance based on specific traffic load conditions and scenarios of wireless sensor network and reveal the fundamental tradeoffs of energy, latency, throughput and fairness under steady state simulations by using Network Simulator – 2 (NS-2).

The remainder of the paper is organized as follows: Section 2 and Section 3 recalls the main features of AODV and DSR. Section 4 describes the simulation in multiple environments and result of energy consumption, latency, throughput and fairness.

2.0 THE DSR PROTOCOL

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network: Route Discovery is the mechanism by which a source node (S) sending a packet to a destination node (D) obtains a route to D [3]. It is used only when the route to D is not known. Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D. Route Discovery and Route Maintenance each operate entirely on demand.

When source node S originates a new packet destined to some other node D, it will obtain a suitable source route by searching its Route Cache of routes previously learned, but if no route is found in its cache, it will initiate the Route Discovery process to dynamically find a new route. S transmits a ROUTE REQUEST message as a single local broadcast packet, which is received by all nodes currently within its range. Each ROUTE

[1, 2]Department of Information Technology, [3, 4]Department of Electronics and Telecommunication,
[1, 2, 3, 4]Smt Kashibai Navale College of Engineering, Pune,Maharashtra, INDIA
E-Mail: [1]pranav21684@gmail.com,
[2]smitapatel7122006@gamil.com, [3] prnv_kulkarni@yahoo.co.in and [4]adishripujari@gmail.com

REQUEST message identifies the initiator and target of the Route Discovery, and also contains a unique request id, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. This route record is initialized to an empty list. When a node receives a ROUTE REQUEST, it will add it's ID to the discovered route field and forward the request or if it is the target of the Route Discovery, it returns a ROUTE REPLY message to the source, containing the entire route; when the nodes in the discovered route receive this ROUTE REPLY, they cache this route in their Route Cache for use in sending subsequent packets to this destination. Thus the entire route is stored in the cache of all the intermediate nodes in that route along with the source node [3].

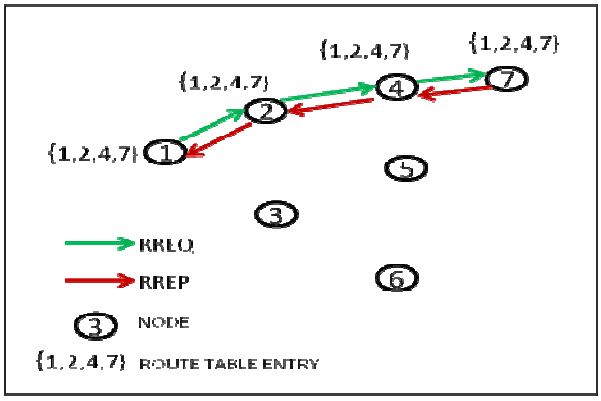


Figure1: DSR Route Discovery Mechanism

3.0 THE AODV PROTOCOL

The AODV routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol: the routes are created and maintained on demand i.e. only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. The distance-vector routing algorithm is used in AODV that keeps the information only about next hops to adjacent neighbors. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified.

Hello messages may be sent to detect and monitor links to neighbors. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected [4]. When a source has data to transmit to an unknown destination, it broadcasts a RREQ to that destination. The number of RREQ messages that a node can send per second is limited. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ [4].

If the receiving node is the destination or has a current route to the destination, it generates a RREP. The RREP is unicast in a hop-by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. Unlike DSR the route table entry in the intermediate nodes on the established path contain only the record of next hop along the route instead of complete route [3].

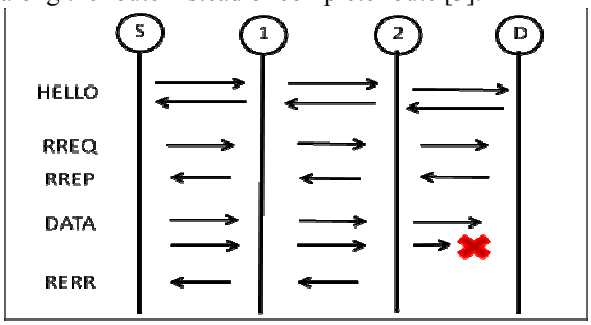


Figure 2: AODV Protocol Messaging.

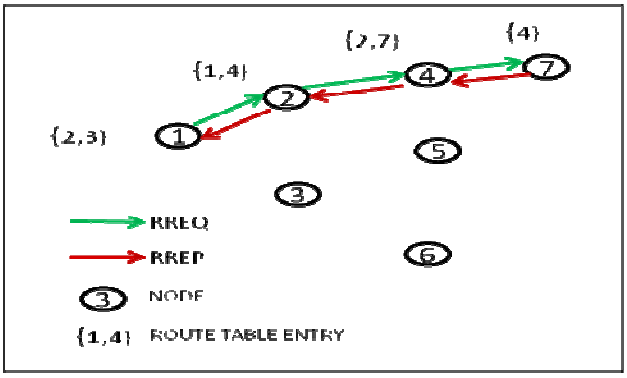


Figure 3: AODV Route Discovery Mechanism.

4.0 RESULTS AND ANALYSIS

The goal of the experimentation is to reveal the fundamental tradeoffs of energy, latency, throughput and fairness in AODV and DSR. All simulations are done using NS-2.27. The radio power values used to compute energy consumption in idle, transmitting, receiving, and sleeping state are in accordance with the RFM TR3000 radio transceiver [7] on Mica Motes.

Simulation parameter and node configuration parameter sets are given in Table 1 and Table 2 respectively.

Simulation Area	2500mx500m
Energy Model	Energy Model
Initial energy	1000J
Transmitting Power	36.00Mw
Receiving Power	14.4mW
Transmission Range	250m

Table 1: Simulation Parameters

Channel Type	WirelessChannel
Radio Propagation Model	TwoRayGround
Antenna Model	OmniAntenna
Network interface type	WirelessPhy
MAC Type	802.11
Interface Queue Type	PriQueue/CMUPriQueue
Buffer size of IFq	50

Table 2: Node Configuration Parameters

4.1. TWO-HOP SCENARIO

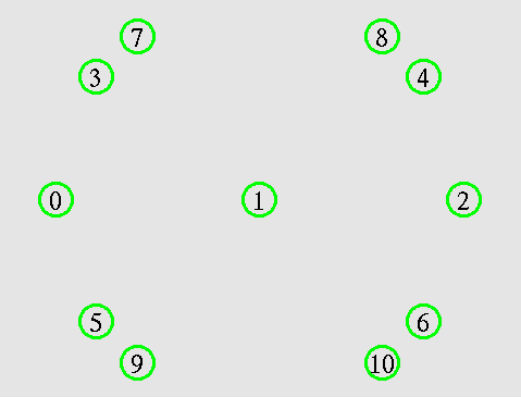


Figure 4: Two-hop Scenario of 11 nodes

The two-hop topology is useful to measure the performance of protocol when hidden terminals are present [8]. As shown in Fig 4, source and sink pairs are arranged around a single intermediate node i.e. node 1. The two-hop topology is of 2500m*500m area.

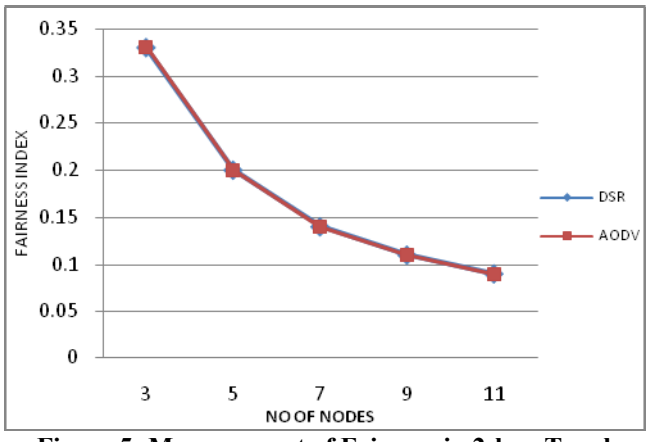


Figure 5: Measurement of Fairness in 2-hop Topology

The Fig 5 shows the measurement of fairness in two hop scenario. The measurement is done by varying the number of nodes. The fairness index values for both the protocols coincide exactly over the entire range. The fairness index reduces significantly with the increase in number of nodes. With increase on network congestion the channel sharing between the nodes becomes unequal, resulting into a drop in fairness index of the network. It is observed that both the protocols respond identically to increasing congestion in the network which gives overlapping graphs.

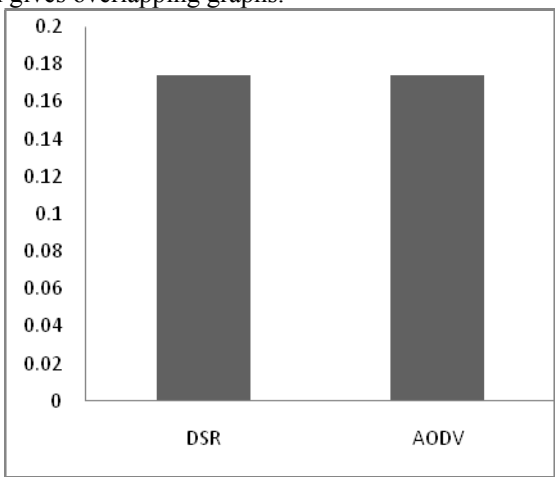


Figure 6: Comparison of average value fairness in 2hop Topology

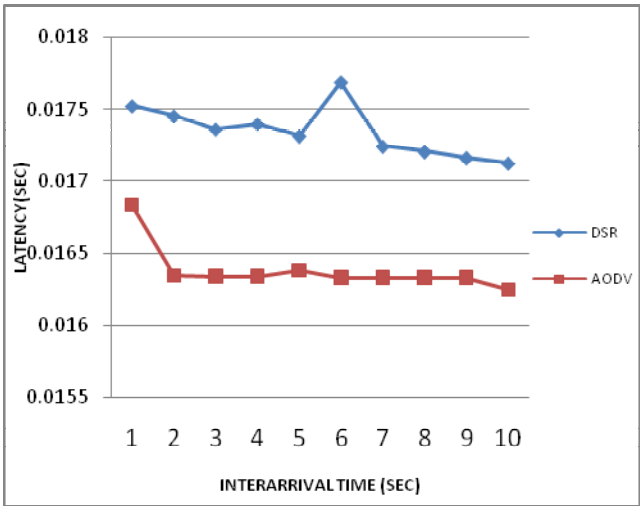


Figure 7: Measurement of Latency in 2-hop Topology

DSR shows higher latency for all values of inter-arrival-time with the respective latency values showing an overall decrease. AODV exhibits a drop at the second value and thereafter remains fairly constant. This may be because in AODV the node replies to the first arrived RREQ packet and discards all those received later thus automatically favoring the least congested path whereas in DSR the node accepts all the RREQ packets and then chooses the shortest path which is comparatively more time consuming [3]. Also DSR requires more time for obtaining routing information, as each node consumes more time for processing any control data it receives, even if it is not the intended receiver.

Throughput for both AODV and DSR reduces with increase in inter arrival time as seen in Fig 7. DSR gives better throughput than AODV over the range. The decrease in throughput is rapid

initially and then becomes gradual. As the inter arrival time increases the time for which the network remains idle increases thus throughput drops in both the cases.

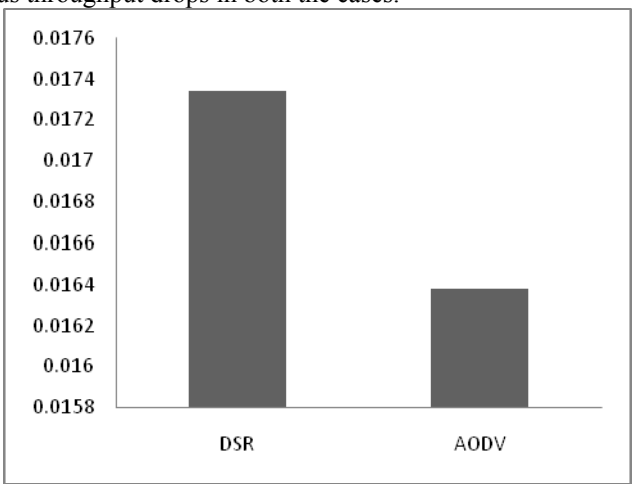


Figure 8: Comparison of Average Latency for 2hop Topology

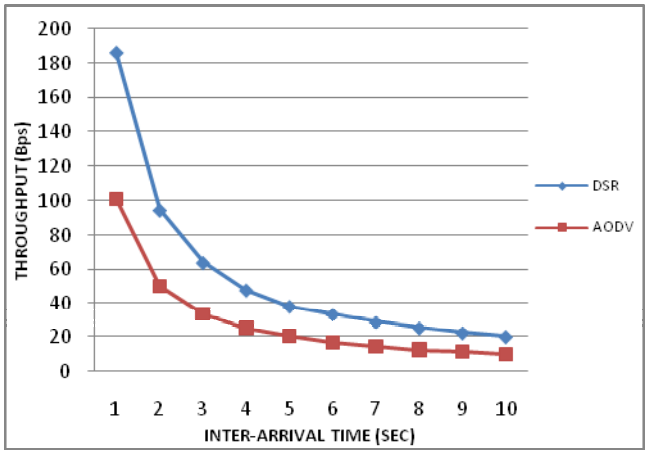


Figure 9: Measurement of Throughput in 2-hop topology.

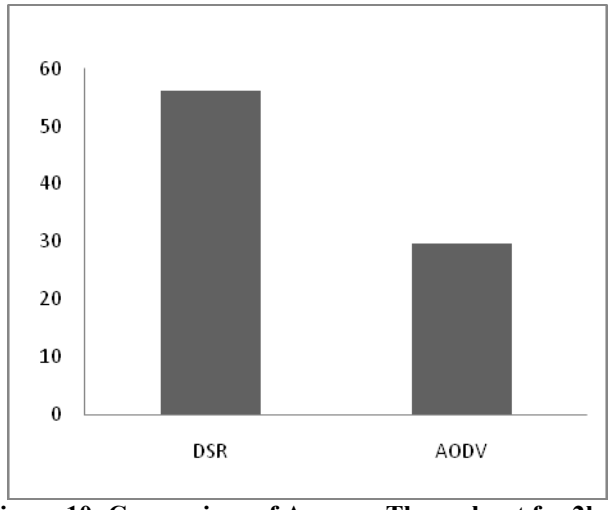


Figure 10: Comparison of Average Throughput for 2hop Topology

This is probably due to the fact that DSR applies the principles of promiscuous listening and caching aggressively which reduces the routing load, thus obtaining higher throughput [5].

4.2. MULTI-HOP CHAIN SCENARIO

The multi-hop scenarios allow the simulations of the complex interactions that more closely approximate the nature of real world WSNs [8]. The multi-hop chain topology can view the system when the sensor nodes are placed equidistant for example on the railway track. [4] The multi-hop chain topology of 11 nodes is as shown in Fig 7. Here, the node 0 is source and node 10 is sink node.

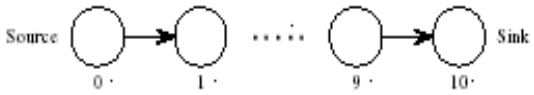


Figure 11: Multi-hop chain (10-hop) Scenario

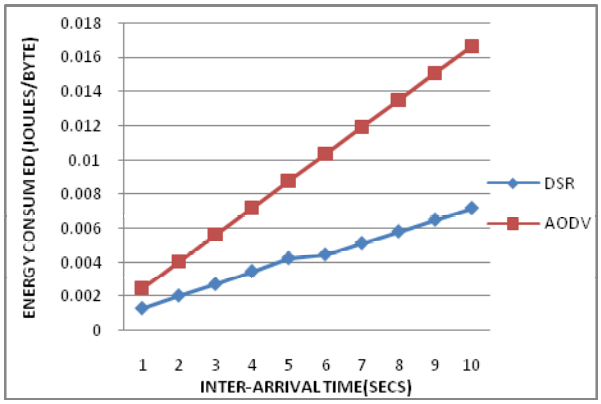


Figure 12: Measurement of Energy Consumption in multi-hop chain topology

Energy consumption in AODV & DSR varies linearly with inter arrival time & is directly proportional to it. It is consistently higher in AODV over the range of inter arrival times and increases at a higher rate than that of DSR. DSR out performs AODV in energy consumption. This may be due to its aggressive approach in promiscuous listening and caching. Because of this the nodes can save a lot of routing procedure as discussed earlier thus saving power [5]. In AODV hello packets are flooded regularly throughout the network. This leads to higher power consumption.

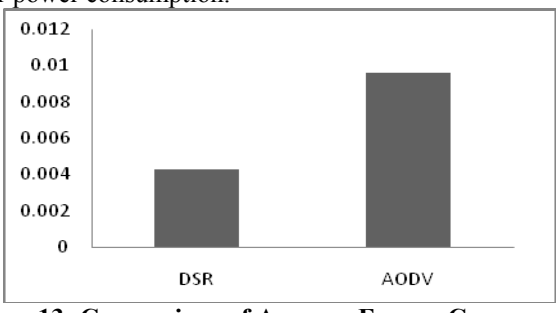


Figure 13: Comparison of Average Energy Consumption for Multi-hop Topology

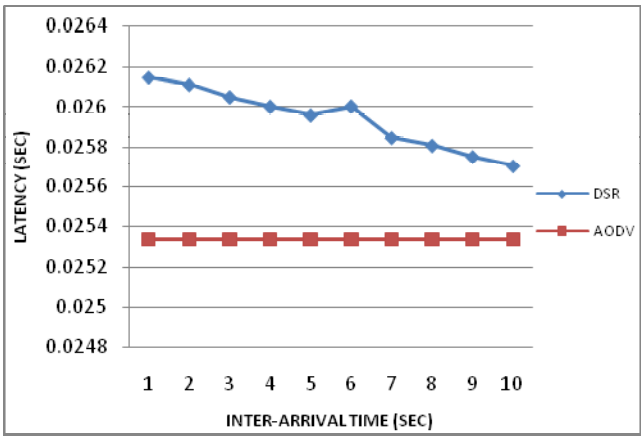


Figure 14: Measurement of Latency in multi-hop chain topology

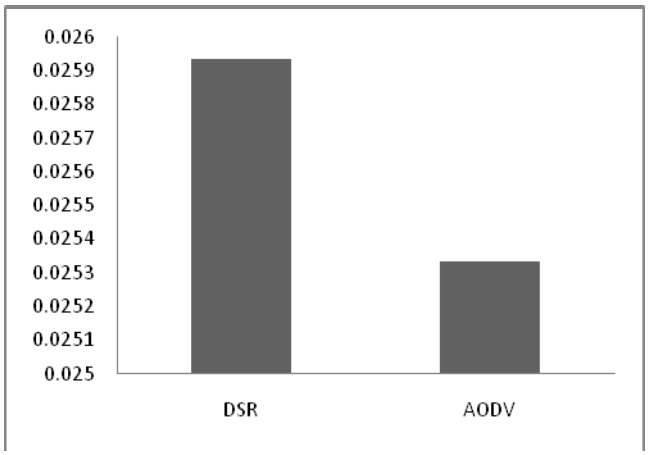


Figure 15: Comparison of Average Latency for Multi-hop Topology

In case of Multi-hop topology also DSR gives higher latency than AODV. This may happen for similar reasons as discussed while considering 2hop topology.

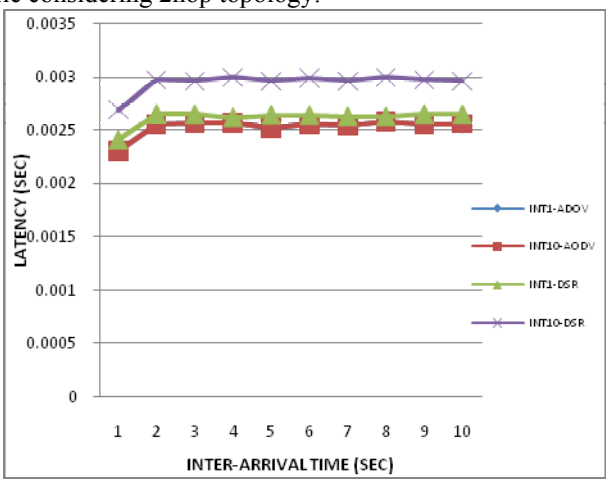


Figure 16: Measurement of Hop-Hop Latency in multi-hop chain topology

Hop to hop latency is the delay required for every hop. It is found to be lesser for the first hop than the rest for whom it is constant. This can be because the source node directly sends the packet to the next node where as the remaining intermediate nodes have to receive the packet, process it, determine the next destination before forwarding.

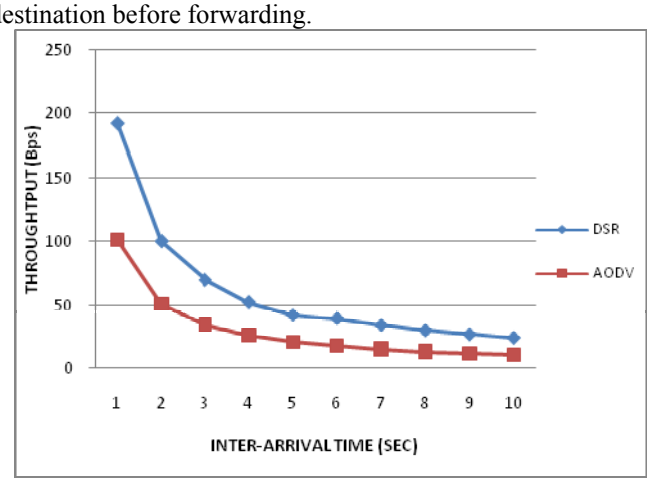


Figure 17: Throughput versus Inter-arrival time for AODV and DSR in multi hop scenario.

The throughput in case of multi-hop topology goes on decreasing in what appears to be an exponential curve, the reasons being same as those mentioned in case of 2hop topology.

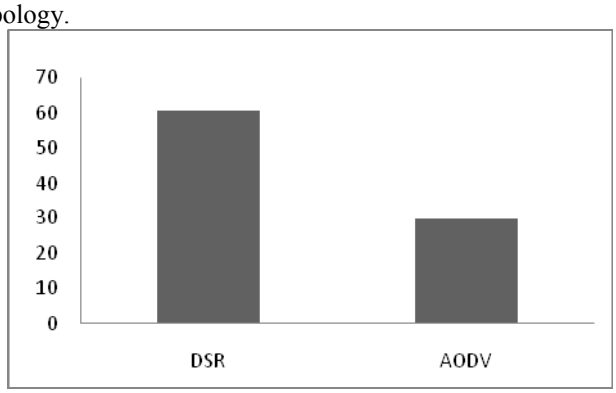


Figure 18: Comparison of Average Throughput for Multi-hop Topology

5.0 CONCLUSIONS

5.1. From the results obtained, DSR proves advantageous with respect to energy consumption with 55.12% lesser average power consumption. Thus DSR is the better choice in networks deployed in remote or inaccessible areas where changing the batteries or replacing the nodes is not practically or economically feasible. Such applications include environment monitoring, animal tracking etc.

5.2. DSR has poor latency as compared to AODV in both multi-hop and 2-hop scenarios. Hence the delay in packet delivery is higher for DSR, thus for time critical applications in which on time delivery of data is of utmost importance AODV is preferable over DSR. Such

applications include various military, disaster warning, health care etc. based applications.

5.3. DSR exhibits nearly 51% higher throughput than AODV. Higher throughput is desirable in case of data intensive applications like industrial process monitoring, urban pollution and traffic monitoring networks etc, which generate a large amount of data that must reach the destination. DSR protocol gives better performance in such cases.

5.4. Both AODV and DSR protocols give identical results with respect to fairness.Thus in topologies with changing node density both protocols behave identically.

REFERENCES

[1] David *B. Johnson David A. Maltz Josh Broch,"* DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*"* Computer Science Department Carnegie Mellon University Pittsburgh, PA,2005.

[2] *Shaily Mittal Prabhjot Kaur "*Performance comparison of AODV, DSR and ZRP Routing Protocols in Manets" International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009.

[3] *Ian. D. Chakeres, Elizabeth M. Belding-Roye* "AODV Routing Protocol implementation Design" Dept. of Electrical & Computer Engineering, University of California Santa Barbara, 2004.

[4] *Juan-Carlos Cano, Pietro Manzoni "*A Performance Comparison of Energy Consumption for Mobile Ad Hoc Network Routing Protocols", EE 360 Class Project Spring 2000-2001.

[5] V. Raghunathan, C. Schurgers, Park.S, and M.B. Srivastava, "Energy-aware wireless microsensor networks," IEEE Signal Processing Magazine, Volume: 19 Issue: 2 , March 2002 Page(s): 40 –50.

[6] ASH transceiver TR3000 http://www.rfm.com/.

[7] D. Corbett, A. Ruzzelli, D. Everitt, G. O'hare, "A Procedure For Benchmarking Mac Protocols Used In Wireless Sensor Networks", Technical Report 593, The University of Sydney, NSW 2006, Australia.

[8] AWK Scripting Tutorial http://www.vectorsite.net/tsawk_1.html#m1

[9] M. Greis. Tutorial for the network simulator-NS. http://www.isi.edu/nsnam/ns/tutorial/index.html

[10] *Per Johansson, Tony Larsson, Bartosz Mielczarek and Nicklas Hedman* "Scenario Performance Analysis of Routing Protocols for Mobile Ad- Hoc Networks", Department of Signals and systems Chalmers University of Technology, Sweden, 2006

Continued from page no. 297

Plain Text	A	S	K	S
Conversion to alpha numeric value	10	28	20	28
Sub key	9	7	2	5
Total	19	35	22	33
Mod 36	19	35	22	33
Cipher Text	j	z	M	x

Table 2: Encryption

Cipher Text	j	z	M	x
Conversion to alpha numeric value	19	35	22	33
Add 36 if less than 9	19	35	22	33
Sub key	9	7	2	5
Subtract	10	28	20	28
Plain Text	A	S	K	S

Table 3: Decryption

Load Balancing in Integrated MANET, WLAN and Cellular Network

Sulata Mitra[1] and **Arkadeep Goswami**[2]

Submitted in June 2010; Accepted in November 2010

Abstract - ***The present work integrates mobile ad-hoc network, wireless local area network and cellular network. It balances the load among the three networks in the integrated heterogeneous environment. It uses a home agent for the selection of the optimal network depending upon the type of session of the mobile nodes. It uses route selection algorithm to select the optimal route in the selected optimal network. Two different position based ant colony routing algorithms are proposed for mobile ad-hoc network in the present work. Both the routing algorithms select an optimal route for a session before starting it. They use route maintenance algorithm to detect whether a node associated with an existing route is going out of the communication range during the ongoing session before the existing route fails completely. Such consideration helps to reduce the data packet loss for both the algorithm. Our previous route selection algorithm is used for route selection in the wireless local area network and cellular network. The performance of the proposed routing algorithms for mobile ad-hoc network are compared with the performance of the existing basic position based ant colony routing algorithm on the basis of initial path set up time, average delay and packet loss. The performance of the three networks is compared on the basis of path set up time and average packet delay in the integrated heterogeneous environment. The performance of the proposed integrated scheme is evaluated in terms of blocking probability.***

Index Terms - MANET, WLAN, Cellular Network, Basic POSANT routing algorithm

1.0 INTRODUCTION

The mobile nodes (MNs) will be equipped with multiple wireless access technology in the future wireless networks. So the future wireless networks are an integrated heterogeneous environment where each MN has multiple network interfaces corresponding to multiple wireless access technology associated with it. The seamless mobility management and load balancing are the challenging issues for such a heterogeneous wireless networks environment.

Such several integration schemes have been reported so far. Nair and Jhu introduced [1] network latency, congestion, battery power, service type as important performance criteria to evaluate seamless vertical mobility.

An end-to-end mobility management system is proposed in [2] to reduce unnecessary handoff and ping-pong effect by using measurement on the condition of different networks.

Nasser et al. proposed a vertical handoff decision method [3] to calculate the service quality for available networks and selects the network with the highest quality. The vertical handoff algorithms in [1,3] are not adequate to coordinate the QoS of many individual mobile users or adapt to newly emerging performance requirements for handoff and changing network status. The vertical handoff decision function for heterogeneous wireless network in [4] is a measurement of network quality. But the authors did not provide any performance analysis. An active application oriented handoff decision algorithm [5] was proposed for multi interface mobile terminals to reduce the power consumption caused by unnecessary handoff and other unnecessary interface activation.

The present work considers the integration of mobile ad-hoc network (MANET), wireless local area network (WLAN) and cellular network. A mobile router (MR) is associated with each MN for maintaining the session in such an integrated heterogeneous environment. Each MN in this integrated environment has three network interfaces. The cellular network has the excellence of wide coverage, seamless roaming support and better quality of service. The WLAN found its application as a low cost high speed solution to cover hot spot like Internet cafes, office buildings, apartment buildings etc. to solve the wideband data access problem and to utilize the existing infrastructure which helps to reduce the implementation cost of the network. The cellular network and WLAN provide single hop communication environment whereas MANET helps to extend this to a multi hop communication environment [6]. The MANET provides multi hop communication environment to the MNs without using any existing infrastructure. Moreover the small, low cost and low powers are suitable for frequent but short duration sessions like making a phone call, checking appointment schedule etc. So low power consumption is an important factor for such application which only can be achieved using MANET environment.

The present work maintains a home agent (HA) to select an optimal network depending upon the type of application of the MNs. When a MN wants to initiate a session it sends session request message to the HA. This message contains MN identification (MN_id) and type of session. The home agent selects MANET as optimal network for the MNs in case of short duration sessions inside the hot spot cells. It selects cellular network as optimal network for the MNs having a session with little data for transmission or reception and long idle period. Though the power consumption of the network interface card (NIC) in MN for upload in cellular network is almost two times than that of WLAN network still it is suitable because using lesser bandwidth of cellular network MNs can transmit or receive only a small amount of data. On the other

[1, 2]*Department of Computer Science and Technology, Bengal Engineering and Science University, Shibpur, West Bengal, INDIA*
E-Mail: [1]sulata@cs.becs.ac.in

hand the WLAN network is suitable for MNs having a session with lot of data due to its high speed, high bandwidth and low cost which helps to complete transmission or reception using the same network which in turn reduces the frequency of vertical handoff. The power consumption of the NIC in MN in case of idle mode is almost 9 times higher in WLAN network in comparison to cellular network. So it would be more advantageous to select the cellular network for mobility management [7] as energy efficient interface in case of idle MN. The HA maintains session_count counter and block_count counter. It increases session_count counter by 1 after receiving a session request message from MN. The home agent increases block_count counter by 1 if it is unable to select an optimal network in response to the session request message of MN within time out. The home agent computes the session blocking probability of the proposed scheme as the ratio of block_count and session_count.

Two different routing algorithms for MANET are proposed in the present work. These algorithms are discussed in section II. The present work uses the route selection algorithm as proposed in [8] for cellular network and WLAN. The HA of the proposed scheme works as the vertical handoff controller as considered in [8] to execute the route selection algorithm.

2.0 ROUTING ALGORITHMS FOR MANET

The routing algorithms for MANET are considered for discussion in the following sections.

2.1 HA Posant Routing Algorithm

The HA is equipped with Google Map [9] and each MN is equipped with global position system (GPS). A source MN (S_id) sends route request message (RRM as discussed in section 2.1.1) to HA for the initiation of a session with a destination MN (D_id). The HA triggers route selection algorithm (as discussed in section 2.1.2) to select an optimal route in response to RRM and sends the optimal route to S_id using route found message (RFM as discussed in section 2.1.1). The home agent assigns unique session identification (SS_id) to each session after selecting an optimal route for it. After receiving route found message S_id generates Type 0 packet (T0 as discussed in section 2.1.3). The route field (Route) of RFM and T0 contains the identification of all MNs which are associated with the optimal route. The S_id sends T0 to D_id through all MNs which are identified in Route of T0. Each MN in the MANET environment maintains a routing table (as discussed in section 2.1.4) and inserts a record in the routing table after receiving a T0. Both S_id and D_id associated with a particular session generate Type 1 packet (T1 as discussed in section 2.1.3) and send T1 to each other to maintain the bidirectional transmission of packets corresponding to a particular session among them using the optimal route which is mentioned in RFM. The HA maintains a session table (as discussed in section 2.1.5) to store the information of all the ongoing sessions among MNs in MANET. The home agent inserts a record in the session table after selecting an optimal route. As soon as an ongoing session is over S_id associated with this session sends session over message (SOM as discussed in section 2.1.1) to HA. The HA searches the session table for the record who's SS_id attribute matches with the SS_id field as mentioned in SOM and deletes that record from the session table. The HA executes route maintenance algorithm (as discussed in section 2.1.6) to detect MN(s) which is associated with an existing route(s) and is going out of the communication range from its neighboring MN associated with the same route during the ongoing session. In such a case the HA considers the existing route(s) as faulty and executes route selection algorithm for the selection of an alternative optimal route(s) to replace the faulty existing route(s). It sends the alternative optimal route to S_id(s) associated with the faulty existing route(s) using route maintenance message (RMM as discussed in section 2.1.1). After receiving route maintenance message S_id(s) generates Type 2 packet (T2 as discussed in section 2.1.3). The new route (N_Route) field of RMM and T2 contains the identification of all MNs which are associated with the alternative optimal route. The S_id sends T2 to D_id through all MNs which are identified in N_Route of T2 for necessary insertion or modification in their routing table.

2.1.1 Message Exchange among Various MNs

RRM contains S_id and D_id fields. RFM contains S_id, D_id, SS_id and Route fields. The MR associated with S_id uses the optimal route as mentioned in Route of RFM for packet transmission corresponding to a particular session which is identified by SS_id field. SOM contains SS_id and F_flag fields. The F_flag field of SOM is set to indicate the end of session which is identified by the SS_id field. RMM contains SS_id, S_id and N_Route fields. The MR associated with S_id uses the alternative optimal route as mentioned in N_Route of RFM for packet transmission corresponding to a particular session which is identified by SS_id field.

2.1.2 Route Selection Algorithm

The GPS detects the current location in terms of longitude and latitude of each MN. The GPS sends this information of each MN to HA as soon as the current location of any MN changes. The home agent uses Vincenty's inverse equation [10] to calculate the distance between two neighboring mobile nodes using their current location which is obtained from GPS. The HA maintains a rectangular boundary around the MNs and the Google Map in HA shows the real time image of each MN within this rectangular boundary using the information provided by GPS. If any intruder MN crosses the rectangular boundary from outside HA sends a special security signal to the MN(s) closer to the intruder MN. The HA maintains a graph of MNs using their real time image which is provided by the Google Map continuously. After receiving RRM the HA applies depth first search to the graph and finds all possible routes from source MN which is identified by S_id to the destination MN which is identified by D_id in RRM. The HA counts the number of MNs in each possible route and selects the route having minimum number of MNs as the best route.

The HA uses basic POSANT [11] algorithm to determine the optimal route in case of multiple best routes.

2.1.3 Type of Packets

T0 contains SS_id, S_id, D_id, Type and Route fields. The Type field indicates the type of the packet as Type 0. T1 contains SS_id, Node_id, S_No, Type and PAYLOAD fields. The Node_id field of this packet is S_id in case the packet is generated by the source MN and D_id in case the packet is generated by the destination MN. The S_No field indicates the sequence number of the packet and Type field indicates the type of the packet as Type 1. The PAYLOAD field contains the data corresponding to the session which is identified by the SS_id. T2 contains SS_id, S_id, D_id, S_No, Type, N_Route and PAYLOAD. The Type field indicates the type of the packet as Type 2.

2.1.4 Routing Table

Each record in the routing table has 5 attributes as shown in TABLE-1. The attributes SN_NH and DN_NH are the source MN next hop and destination MN next hop respectively.

S_id	D_id	SS_id	SN_NH	DN_NH
S	D	s	T	E

Table 1

Let TABLE-1 is the routing table which is maintained by j^{th} MN and it shows a record for s^{th} session. The S_id and D_id which are associated with s^{th} session are identified as S and D respectively in TABLE-1. T indicates the next hop of the j^{th} MN in case of transmission from S to D and E indicates the next hop of j^{th} MN in case of transmission from D to S in TABLE-1. After receiving a T0 the j^{th} MN inserts a record in TABLE-1. After receiving a T1 the j^{th} MN searches TABLE-1 for the existing record whose SS_id attribute matches with the SS_id field as mentioned in T1. It compares the S_id attribute and the D_id attribute of the existing record with the Node_id field as mentioned in T1. If the Node_id field in T1 matches with the S_id attribute of the existing record the j^{th} MN forwards the packet to T and if the Node_id field in T1 matches with the D_id attribute of the existing record the j^{th} MN forwards the packet to E. After receiving T2 the j^{th} MN searches the routing table for the existing record whose SS_id attribute matches with the SS_id field as mentioned in T2. If found it updates the record by replacing the old route attribute by the new route attribute as mentioned in T2. Otherwise, it inserts a new record in the routing table. When a MN is not participating in packet transmission corresponding to a particular session, it deletes the corresponding record from the routing table.

2.1.5 Session Table

Each record in the session table has 3 attributes as shown in TABLE-2. The Route attribute contains the identification of all MNs which are associated with the selected optimal route starting from S_id to D_id for the packet transmission corresponding to a particular session as identified by SS_id. The number of records in the session table depends upon the number of ongoing sessions.

SS_id	S_id	Route

Table 2

2.1.6 Route Maintenance Algorithm

The HA computes the distance between the two neighboring MNs continuously using the information provided by GPS and using the Vincenty's inverse equation. The HA considers a MN as MOVE_NODE in case its distance from the neighboring MN crosses a threshold. The threshold distance is computed during simulation as discussed in section 3.1.2. As soon as HA detects such a MN, it searches the Route attribute of all the records in the session table. It selects the record(s) whose Route attribute contains the identification of the MOVE_NODE. If found it retrieves the selected record(s). It executes route selection algorithm for the selection of an alternative optimal route(s) before the existing route(s) fails completely. Such advance selection of an alternative optimal route helps to reduce packet loss of a session. The HA updates the selected record(s) by replacing the old route attribute by the new route attribute in the session table.

The installation of Google Map along with GPS increases the cost of the system. Moreover the GPS may not be able to work properly in situations such as underwater conditions e.g. within submarines. In such a situation radio detection and ranging (RADAR) works well. The RADAR POSANT routing algorithm is considered for discussion in section 2.2.

2.2 Radar Posant Routing Algorithm

Each MN is equipped with two antennas, one at the front end and one at the rear end of MN. Both the antenna can work as transmitter as well as receiver to achieve bidirectional transmission of packets corresponding to a particular session. One of the MNs works as a special fixed node (SFN). It maintains route information and is not taking any part in communication.

The S_id triggers route selection algorithm (as discussed in section 2.2.1) by forwarding ant packet [11] towards D_id for the initiation of a session as in basic POSANT routing algorithm. The D_id selects an optimal route and sends the optimal route to SFN using D_to_SFN message (as discussed in section 2.2.2). The SFN sends the optimal route to S_id using SFN_to_S message (as discussed in section 2.2.2). The SFN assigns a unique SS_id to each session after receiving the optimal route from D_id. After receiving SFN_to_S message S_id generates T0 (as discussed in section 2.1.3). The route field (Route) of D_to_SFN message, SFN_to_S message and T0 contain the identification of all MNs which are associated with the optimal route. The S_id sends T0 to D_id through all MNs which are identified in Route of T0. Each MN maintains a routing table (as discussed in section 2.1.4) and inserts a record in the routing table after receiving a T0. Both S_id and D_id associated with a particular session generate T1 (as discussed in section 2.1.3) and send T1 to each other to maintain the

bidirectional transmission of packets corresponding to a particular session among them using the optimal route as mentioned in SFN_to_S message. The SFN maintains a session table (as discussed in section 2.1.5) to store the information of all the ongoing sessions among MNs in MANET. The SFN inserts a record in the session table after receiving D_to_SFN message. As soon as an ongoing session is over S_id associated with this session sends SOM (as discussed in section 2.2.2) to SFN. The SFN searches the session table for the record who's SS_id attribute matches with the SS_id field as mentioned in SOM and deletes that record from the session table. Each MN associated with an existing route executes route maintenance algorithm (as discussed in section 2.2.3) to detect whether its neighboring MN associated with the same route is going out of the communication range during the ongoing session and sends an alarming signal to the neighboring MN. In response the neighboring MN sends its identification to SFN. In such a case the SFN considers the existing route as faulty and sends SFN_ALT_ROUTE message (as discussed in section 2.2.2) to S_id which is associated with the faulty route for the execution of the route selection algorithm. The S_id executes route selection algorithm for the selection of an alternative optimal route to replace the faulty existing route. After selecting the alternative optimal route S_id generates T2 (as discussed in section 2.1.3). The N_Route of T2 contains the identification of all MNs which are associated with the alternative optimal route as selected by S_id. The S_id sends T2 to D_id through all MNs which are identified in N_Route of T2 for necessary insertion or modification in their routing table.

2.2.1 Route Selection Algorithm

The S_id forwards the ant packet through all the possible routes between S_id and D_id associated with a particular session as in basic POSANT routing algorithm. The ant packet deposits pheromone value to each link. The maximum pheromone value is deposited to the link having smallest length. The ant packet has 6 fields as shown in Fig.1.

S_id	D_id	A_F	T_S	Route	P_C

Figure.1: Format of ant packet

The A_F field is set to indicate the type of the packet as ant. Let i^{th} MN receives an ant packet from k^{th} MN and j^{th} MN is the successor of i^{th} MN. The i^{th} MN mentions the current time stamp in the T_S field of the ant packet and forwards it to j^{th} MN. The i^{th} MN adds its identification in the Route field of the ant packet. The i^{th} MN computes the difference in time stamp (Diff_time) between the current time stamp corresponding to the time of receiving the ant packet by it and the time stamp in the T_S field of the ant packet as mentioned by k^{th} MN. The i^{th} MN also computes its distance from k^{th} MN (D_{ik}) by multiplying Diff_time and the speed of electromagnetic signal (m/sec). The bit error rate increases rapidly when the distance between the two neighboring MNs in the WLAN environment is greater than 45 meters [12]. So in the present work the pheromone value of the link between the i^{th} MN and the k^{th} MN (P_value_{ik}) is assumed as 20 (any value >1 shows the identical performance) if $D_{ik}<45$ otherwise it is assumed as 1. The i^{th} MN also multiplies the value in the P_C field of the ant packet as mentioned by k^{th} MN by P_value_{ik}. At i^{th} MN the value in P_C field of the ant packet indicates the pheromone concentration of the route from S_id up to i^{th} MN.

The D_id receives multiple ant packets through all possible routes between source and destination. It compares the P_C value of all the received ant packets. The route field in the ant packet having maximum P_C value is selected as the optimal route.

2.2.2 Message Exchange among Various MNs

D_to_SFN message has S_id, SFN_id and Route fields. SFN_id field indicates the identification of SFN. SOM contains SS_id and F_flag. SFN_to_S message contains SS_id, S_id, SFN_id and Route fields. The SFN_ALT_ROUTE message contains S_id, SFN_id and SS_id fields.

2.2.3 Route Maintenance Algorithm

Each MN associated with an existing route computes its distance from its neighboring MN which is associated with the same route using mono-static equation [13]. The mono-static equation used by the RADAR antennas in this scheme is as follows:

$P_r = 10 \log_{10}[(P_tG_tG_r\lambda^2\sigma)/((4\pi)^3R^4)]$

$= 10 \log_{10}[P_tG_tG_r\{(\sigma c^2)/((4\pi)^3 f^2 R^4)\}]$

where, P_r = Received peak power

P_t = Transmitted peak power

G_t = Gain of transmitter antenna (dBi)

G_r = Gain of receiver antenna (dBi)

λ = Transmitted wavelength (m, cm, in, etc.)

σ = Radar cross-section of target - RCS (m^2, cm^2, in^2, etc.) R = Range (m, cm, in, etc.), c = speed of light

The parameter values of the mono-static equation are assumed as follows: P_t = 20 dbm, $G_t = G_r$ =16 dbi, λ = 15 cm, σ = 2.5 m^2 and c = 3* 10^8 meter/sec [14,15,16,17]. The parameter R indicates the distance between the two neighboring MNs. P_r is measured at the receiving antenna and R is computed using the mono-static equation using the known value of all the other parameters.

Each MN associated with an existing route also computes its angle with its neighboring MN which is associated with the same route using Pythagoras theorem. In ΔABC (Fig.2) the vertex B and the vertex C represent the location of the front end and rare end antenna in a MN. The vertex A represents the location of the neighboring MN. In ΔABC the side AB (=c) represents the distance between the neighboring MN and the front end antenna. P_r is measured at the front end antenna and c is computed using mono-static equation. The side AC (=b) represents the distance between the neighboring MN and the rare end antenna. P_r is measured at the rare end antenna and b is computed using mono-static equation. The side BC (=a) represents the length of MN. AP (=h) is perpendicular to BC.

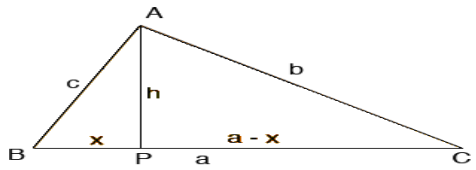


Figure.2: Triangular representation of the angle calculation process.

The angle between the two neighboring MNs (angle C) is $C= \cos^{-1}\{(a^2+b^2-c^2)/ 2ab\}$ using Pythagoras theorem. A MN sends an alarming signal to its neighboring MN (RECEIVED_NODE) in the direction of the angle as computed by the Pythagoras theorem in case its distance from the RECEIVED_NODE crosses a threshold. The threshold distance is computed during simulation as discussed in section 3.1.2. The RECEIVED_NODE sends its Node_id to SFN. The SFN searches the Route attribute of all the records in the session table. It selects the record(s) whose Route attribute contains the identification of the RECEIVED_NODE. If found it retrieves the selected record(s) and sends SFN_ALT_ROUTE message to S_id(s) associated with the selected record(s) to execute route selection algorithm for the selection of an alternative optimal route(s) before the existing route(s) fails completely. After the selection of the alternative optimal route by D_id, SFN receives D_to_SFN message and updates the selected record(s) by replacing the old route attribute by the new route attribute corresponding to the alternative optimal route in the session table.

2.3 Comparison of Routing Algorithms

In this section the basic POSANT routing algorithm [11], HA POSANT routing algorithm and RADAR POSANT routing algorithm are compared on the basis of storage requirement, routing table searching time and time complexity of the algorithm.

2.3.1 Storage Requirement

In basic POSANT routing algorithm each MN maintains a forward routing table to send packets from source MN to destination MN and a backward routing table to send packets from destination MN to source MN. Each record in the routing table has 3 attributes as shown in TABLE-3. Let TABLE-3 is the forward routing table at j^{th} MN. The Node_Address attribute is the address of the destination MN in case of forward routing table. The Next_Hop attribute is the address of the next hop MN from j^{th} MN towards destination which is identified by the Node_Address attribute. The Pheromone_Value attribute indicates the pheromone value corresponding to the next hop MN which is indicated by the Next_Hop attribute. The Node_Address attribute and the Next_Hop attribute are 128 bit IPv6 address. The maximum pheromone value which is deposited to a link is 20 as discussed in the section 2.2.1 and the number of bits require to represent the maximum pheromone value is 5. So the length of each record in the forward routing table at any MN is 261 bits. The number of records in the forward routing table at j^{th} MN for a single session depends upon the number of possible next hop MNs from j^{th} MN towards destination. So the storage requirement per forward routing table is (261*number of possible next hop towards destination MN) bits.

Node_Address (128 bits)	Next_Hop (128 bits)	Pheromone_Value (5 bits)

Table 3

Let TABLE-3 is the backward routing table at j^{th} MN. The Node_Address attribute is the address of source MN in case of backward routing table. The Next_Hop attribute is the address of the next hop MN from j^{th} MN towards source which is identified by the Node_Address attribute. The number of records in the backward routing table at j^{th} MN for a single session depends upon the number of possible next hop MNs from j^{th} MN towards source. The storage requirement per backward routing table is (261*number of possible next hop towards source MN) bits. So the storage requirement for each bidirectional session is 261*(number of possible next hop towards destination + number of possible next hop towards source) bits.

In HA POSANT routing algorithm and RADAR POSANT routing algorithm each MN maintains a single routing table as shown in TABLE-1. The S_id, D_id, SN_NH and DN_NH are 128 bits IPv6 addresses. Now for 1000 number of different bidirectional sessions the number of bits requires to represent SS_id is 10. So the length of each record in the routing table is 522 bits. There is a single record for each bidirectional session in the routing table and so the storage requirement for each bidirectional session is 522 bits. The storage requirement for each bidirectional session in basic POSANT routing algorithm is greater than that in HA POSANT routing algorithm and RADAR POSANT routing algorithm if the number of next hop MNs from j^{th} MN towards source or destination is greater than unity in TABLE-3.

2.3.2 Routing Table Searching Time

Let in case of basic POSANT routing algorithm the number of forward ongoing session through j^{th} MN as an intermediate MN is m and the number of next hop from j^{th} MN towards destination is n. So at j^{th} MN the forward routing table contains m*n number of records and the time complexity to select the desired record from the forward routing table is $O(\log_2 m*n)$. The j^{th} MN compares the pheromone value of all the n number of next hops and selects the optimal next hop having the maximum pheromone value. The link between j^{th} MN and the selected optimal next hop is considered as the optimal outgoing link towards destination. The time complexity to select the optimal outgoing link from the forward routing table at j^{th} MN is $O(n^2)$. So the total time complexity at j^{th} MN for the selection of an optimal outgoing link is $O(\log_2 m*n+n^2)$.

In case of HA POSANT routing algorithm and RADAR POSANT routing algorithm the routing table at j^{th} MN contains m number of records and the time complexity to select the desired record from the routing table is $O(\log_2 m)$.

So the time complexity of searching the routing table is higher in basic POSANT routing algorithm than in HA POSANT routing algorithm and RADAR POSANT routing algorithm.

2.3.3 Time Complexity of the Algorithm

In case of basic POSANT routing algorithm the routing table at each MN contains the possible next hop and their pheromone value. During the ongoing session the routing table at each MN is searched for the selection of an optimal outgoing link. In case of HA POSANT routing algorithm and RADAR POSANT routing algorithm the routing table at each MN contains the optimal route. During the ongoing session the routing table at each MN is searched for the optimal route. So the optimal route is selected during the ongoing session in basic POSANT routing algorithm which increases its time complexity than the HA POSANT routing algorithm and RADAR POSANT routing algorithm. The time complexity of the HA POSANT routing algorithm is higher due to the time complexity of the depth first search than the time complexity of the RADAR POSANT routing algorithm

3.0. SIMULATION

The simulation experiment is performed in two different phases. The performance of the basic POSANT [11] routing algorithm, HA POSANT routing algorithm and RADAR POSANT routing algorithm are compared in Phase 1. The performance of the integrated heterogeneous environment has been studied in Phase 2. The simulation experiment is conduced for 1280 number of packets and 6 numbers of MNs in both the phases.

3.1 Experimental Results for Phase 1

The simulation experiment is conducted to compare the performance of the three routing algorithms for MANET.

3.1.1 Initial Path Set Up Time

It is the time to set up an optimal route for the initiation of a session. Fig.3 shows the plot of initial path set up time for all the three routing algorithms. The basic POSANT routing algorithm needs the transmission of forward ant packets and backward ant packets for route selection. The optimal outgoing link corresponding to the optimal route is decided from the pheromone value in the ant packets. The HA POSANT routing algorithm needs the transmission of RRM and RFM among MNs for route selection instead of the transmission of forward ant packets and backward ant packets. The transmission of RRM and RFM select the optimal route instead of the optimal outgoing link which reduces the initial path set up time of HA POSANT routing algorithm than basic POSANT routing algorithm. The RADAR POSANT routing algorithm needs the transmission of forward ant packets for initial route selection which increases the initial path set up time of RADAR POSANT routing algorithm than HA POSANT routing algorithm. But the transmission of backward ant packets is not required in RADAR POSANT routing algorithm which reduces the initial path set up time of RADAR POSANT routing algorithm than basic POSANT routing algorithm.

3.1.2 Average Packet Delay

Fig.4 shows the plot of average packet delay vs. simulation time for all the three routing algorithms. It can be observed from Fig.4 that the average packet delay is higher in basic POSANT routing algorithm as it selects the optimal route during the ongoing session than the other two routing algorithms.

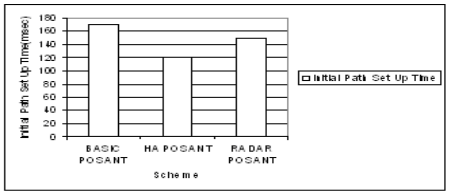


Figure 3: Initial path set up times

Fig.5 shows the plot of average packet delay vs. the number of packets received for all the three routing algorithms. The speed of MN is assumed as 6 km/hr [18,19,20]. If a MN associated with the optimal route of a particular session starts to move in the opposite direction of another MN associated with the same route, their relative velocity becomes 12 km/hr. The communication range of WLAN is assumed as 100 m [21]. So the failure occurs in the existing route when the two neighbouring MNs associated with the same route go out of the communication range with relative velocity 12 km/hr after 30 sec. It can be observed from Fig.3 that the initial path set up time for HA POSANT routing algorithm is 120 msec and for RADAR POSANT routing algorithm is 150 msec. The two neighbouring MNs having relative velocity 12 km/hr covers a distance of 0.4 m (≈ 1 m) in 120 msec for HA POSANT routing algorithm and .5 m (≈1 m) in 150 msec for RADAR POSANT routing algorithm. So the packet loss and average packet delay of an ongoing session can be minimized by triggering the route maintenance algorithm in advance when the two neighbouring MNs associated with the same optimal route are at a threshold distance of 99 m (100 m-1 m) from each other. During simulation it has been observed that the time requires to transmit a single packet using basic POSANT routing algorithm is 40 msec whereas the time requires for transmitting a single packet using HA POSANT routing algorithm and RADAR POSANT routing algorithm is 30 msec. So the number of packets that can be transmitted using basic POSANT routing algorithm in 30 sec is 700 whereas the number of packets that can be transmitted using HA POSANT routing algorithm and RADAR POSANT routing algorithm in 30 sec is 950 before the failure occurs in the existing route.

It can be observed from Fig.5 that the initial average packet delay is higher in basic POSANT routing algorithm due to its higher initial path set up time as discussed in section 3.1.1 than the other two routing algorithms. The new route is selected in basic POSANT routing algorithm after the transmission of 700 packets. The new route is selected in HA POSANT routing algorithm and RADAR POSANT routing algorithm after the

transmission of 950 packets. The average packet delay in the new route for basic POSANT routing algorithm is also higher due to its higher initial path set up time than the other two routing algorithms.

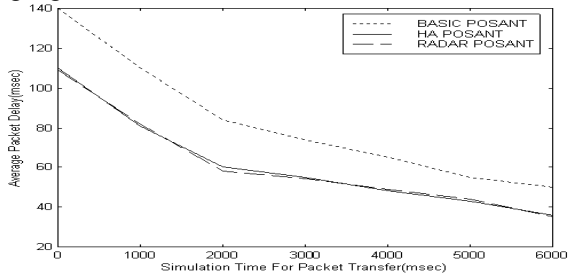


Figure 4: Average packet delay vs. Simulation time

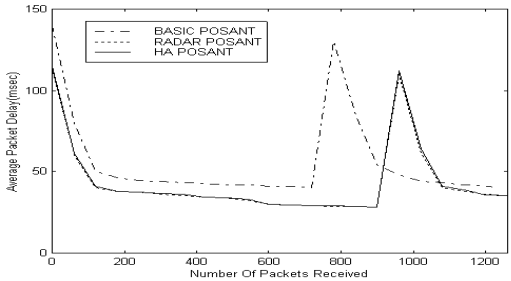


Figure.5: Average packet delay vs. Number of packets received

3.1.3 Percentage Of Successfully Delivered Packets

TABLE-4 shows the percentage of successfully delivered packets for the 3 routing algorithms. The new route discovery process starts after the failure occurs in the existing route in basic POSANT routing algorithm. So the data packets that are generated during the time interval between the occurrence of route failure and finding out a new route are lost. The route maintenance algorithm selects an alternative optimal route in advance before the failure occurs in the existing route in HA POSANT routing algorithm and RADAR POSANT routing algorithm. So the percentage of successfully delivered packets is lesser in basic POSANT routing algorithm than the other two routing algorithms.

Scheme	Packet generated	Packet delivered	% of successfully deliver packets
11	1280	1203	94%
HA	1280	1280	100%
RADAR	1280	1280	100%

Table 4

3.2 EXPERIMENTAL RESULTS FOR PHASE 2

The simulation experiment is conducted to evaluate the performance of the proposed integrated scheme.

3.2.1 Path Set Up Time

Fig.6 shows the path set up time for all the networks in the integrated heterogeneous environment. The path set up time in the cellular network and in WLAN is higher due to the infrastructure access overhead than the path set up time in MANET. The path set up time in cellular network and WLAN are identical as they are using the same route selection algorithm [8].

3.2.2 Average Packet Delay

Fig.7 shows the plot of average packet delay vs. simulation time for all the three networks in the integrated network environment. The average packet delay is lesser in MANET due to its lesser path set up time. The average packet delay of WLAN and cellular network is slightly higher due to higher path set up time and the overhead of executing the route selection algorithm [8] than MANET. But the average packet delay of WLAN is lesser due to its high speed than cellular network.

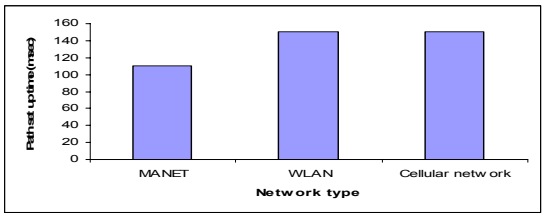


Figure.6: Path set up time for three networks

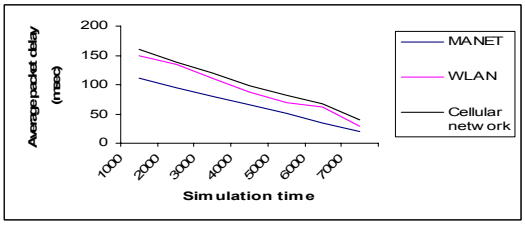


Figure.7: Average packet delay vs. simulation time

3.2.3 Session Blocking Probability

Fig.8 shows the plot of session blocking probability vs. the number of sessions of the proposed scheme. It increases with the number of sessions. The blocking probability in [22] is 90. The maximum session blocking probability of the proposed scheme is 60%.

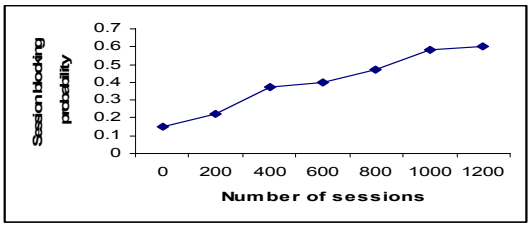


Figure 8: Session blocking probability vs. number of sessions

4.0 CONCLUSION

The proposed work integrates MANET, WLAN and cellular network. It maintains a HA to select an optimal network depending upon the type of session. The route selection algorithm is proposed for all the three networks. The performances of the proposed scheme are evaluated

considering only the data class of traffic. It can be extended by considering other traffic classes during simulation.

REFERENCES

[1]. J.McNair and F.Zhu, "Vertical Handoffs in Fourth-Generation Multinetwork Environments", IEEE Wireless Communications Magazine, June 2004.

[2]. Chuanxiong Guo, Zihua Guo, Qian Zhang and Wenwu Zhu, "A seamless and proactive End-to-End Mobility Solution for Roaming across Heterogeneous Wireless Networks", IEEE Journal on Selected Areas in Communications, vol.22, no.5, pp.834-848, June 2004.

[3]. N.Nasser, A.Hasswa and H.Hassanein, "Handoffs in Fourth Generation Heterogeneous Networks", IEEE Communications Magazine, vol.44, no.10, pp. 96-103, October 2006.

[4]. A.Hasswa, N.Nasser and H.Hassanein, "Generic vertical handoff decision function for heterogeneous wireless networks", Second IEEE/IFIP international conference on wireless and optical communication networks, pp.239-243, March 2005.

[5]. W.T.Chen and Y.Y.Shu, "Active application oriented vertical handoff in next generation wireless networks", IEEE wireless communication and networking conference, pp.1383-1388, March 2005.

[6]. D.Cavalcanti, D.Agrawal, C.Cordeiro, B.Xie and A.Kumar, "Issues in Integrated Cellular Networks, WLANs, and MANETs: A Futuristic Heterogeneous Wireless Networks", IEEE Wireless Communications, pp.30-41, June 2005.

[7]. S.Mitra, "Dynamic Mobility Management for Next Generation All-IP Wireless Network", AsiaCSN 2008.

[8]. S.Mitra, "Resource Management using Route Selection and Vertical Handoff Algorithm in Next-Generation All-IP Wireless Network", IJARITAC, vol.1, issue 2, August 2010.

[9]. K.R.Arefin, T.Wongsaardsaku and K.Kanchanasut, "Vehicle-to-Infrastructure MANET with group mobility for emergency multimedia communication", Asian Internet Engineering Conference Bangkok, Thailand pp. 46-54, 2009, ISBN: 978-1-60558-614-4.

[10]. Wikipedia.org: Vincenty's Equation

[11]. S. Kamali and J. Opatrny, "A Position Based Ant Colony Routing Algorithm for Mobile Ad-hoc Networks", Journal of Networks, vol.3, no.4, April 2008.

[12]. J-P. Ebert, S. Aier, G. Kofahl, A. Becker, B. Burns, and A. Wolisz, "Measurement and Simulation of the Energy Consumption of an WLAN Interface", TKN Technical Report TKN-02-010, Technical University Berlin, Telecommunication Networks Group, Berlin, June 2002.

[13]. www.rfcafe.com

[14]. www.air802.com

[15]. www.radiolabs.com

[16]. www.l-com.com

[17]. www.mwjournal.com

[18]. www.tradekey.com

[19]. www.chinaripu.com

[20]. www.allproducts.com

[21]. www.eurescom.eu: BLTandWLAN.html

[22]. F.Zhu and J.McNair, "Multiservice Vertical handoff Decision Algorithms", EURASIP Journal on Wireless Communications and Networking, pp.1-13, vol.2006.

An Enhanced Genetic Algorithm Approach to ATM Network Design

Susmi Routray

Submitted in February 2010; Accepted in August 2010

Abstract - ***The world of telecommunications is booming the telecommunication infrastructures are becoming more complex, and consequently, interest in developing broadband integrated service of digital network technologies like Asynchronous Transfer Mode (ATM) and Wireless ATM (WATM) are gaining momentum. The changing traffic pattern and the new technologies used in ATM networks make the topological design of ATM network a major research issue. Most of the researchers dealt with the topological design problem suggested solutions based on requirement of expensive exchange based equipments. In this paper we have proposed a cost effective ATM network model. The design of ATM networks entail optimization of the network. We have proposed an Enhanced Genetic Algorithm (GA) based solution for the optimization of ATM network. The results of the study show a major improvement in the solutions generated by Enhanced GA over Simple GA.***

Index Terms - Asynchronous Transfer Mode, Passive Optical Network, Genetic Algorithm (GA), Enhanced GA

1.0 INTRODUCTION

ATM is a packet switched, connection oriented transfer mode based on asynchronous time division multiplexing. ATM is considered to reduce the complexity of the network and improve the flexibility of traffic performance [Raychaudhuri and Wilson, 1994]. In ATM, information is sent out in fixed-size cells. Each cell in ATM consists of 53 bytes. Out of these 53 bytes, 5 bytes are reserved for the header field and 48 bytes are reserved for data field. ATM is Asynchronous as the recurrence of cells sent by an individual user may not necessarily be periodic. ATM integrates the multiplexing and switching functions and allows communication between devices that operate at different speeds [P. Wong and D. Britland, 1993]. The objective of ATM network planning is to design the network structure to carry the estimated traffic and also to minimize the cost of network [Gerla, 1989, Gerla, Kleinrock, 1977, Routray et. al., 2006]. Over the last decade, many programming models have been developed [Kim et. al., 1995, Minoux, 1987] which deals with telecommunication network planning [Liu, 2003]. A large number of network optimization problem do not have any standard algorithm that can guarantee an optimal solution in real time, based on the different constraints. As the models for the design of ATM networks are quite complex, and involve generally a very large number of integer and continuous variable, meta-heuristics like simulated annealing [Rios et. al., 2005] and GA has been used to solve the design problem [Routray et. al., 2005, Davis et. al. 1993, Davis et. al., 1987]. Abuali et. al. (1994) present a GA based algorithm for the capacitated concentrator location problem and develop a permutation-based representation. The resulting algorithm out-performed a greedy heuristic on larger problems. Elbaum & Sidi, 1995 consider the problem of designing local area computer networks which corresponds to the minimum spanning concentrator location problem. Chardaire *et a*l. (1995) also use a GA and apply it to uncapacitated and capacitated versions of SS-CLP. The paper does not describe how they assign end-users if there are capacity constraints. For uncapacitated problems [Balakrishnan et. al., 1989], LR finds better solutions than the GA. However, when tested against capacitated problems, a GA combined with local search performs more consistently than LR across a range of problems.

ATM network planning deals with determination of location for the switches and linking the switches [Hasslinger et. al., 2005]. One of the limiting factors in the design of the ATM network as can be deduced from the literatures cited is the requirement of expensive exchange based equipments. Passive Optical Network is a solution to the problem. It provides a way to gradually introduce fiber optic technology into access networks while still deploying parts of the traditional copper line or co-axial cable systems. These networks allow many different configuration options and as such will place new demands on network planners. Most of the literatures available with respect to PON ATM's pertain to the Steiner tree topology implementation. In this paper we have addressed the comprehensive ATM network planning problem which deals with the backbone network design using the ring topology. Ring architecture is considered cost effective in that they offer high network survivability in the face of node failure and greater bandwidth sharing [Wu, et. al., 1998]. And also the problem of end-user connectivity with the backbone network has been addressed.

2.0 GENETIC ALGORITHM

GA is a non-traditional based optimizing technique [Goldberg, 1991] which can be used to optimize the ATM network. GA operations [Srinivas et. al., 1994] can be briefly described as Coding, Initialization, Evaluation, Reproduction, Crossover, Mutation and Termination. Coding-This step is to represent the variables of the optimization problem in the form of genes. Initialization-Chromosomes with different genes are randomly selected as the initial chromosomes. These random chromosomes constitute the population, the size of which is equal to the random number of chromosomes. Evaluation-Each chromosome in the population is assigned a specific value

Department of Information Technology, Institute of Management Technology, Ghaziabad, UP, INDIA
E-Mail: sroutray@imt.edu

associated with the gene arrangement called fitness. Due to the differences of gene arrangement, the fitness value of the chromosome in the population is used to evaluate the chromosome for its survivability. Reproduction-from Evaluation chromosomes with different gene arrangements have different fitness values. Reproduction is to increase the number of the good chromosomes and decrease the number of the poor chromosomes in the next generation. Crossover-This procedure exchanges genes between the father and the mother chromosomes. Two chromosomes are randomly selected from the population as parent chromosomes. The crossover points are chosen to be less than the number of genes in the chromosome and then the genes are swapped between the crossover points. Two new chromosomes with the genes from both the parent chromosomes are obtained. This procedure is called two-point crossover. Mutation-In order to have a new chromosome which differs from the chromosomes in the population, a mutation operation is used. A chromosome is randomly selected as the mutated chromosome. The mutating gene is randomly selected from the number of genes in the mutating chromosome and then the value of this gene is flipped into another value. The operation repeats until the variation of the mean fitness of the population is very small. Finally, the best chromosome in the population is decoded as the solution of the optimization problem. GA has been used in previous studies with a different perspective and in parts to design ATM network, to optimize the bandwidth [Thompson , 2000, G. Carello et. al, 2003, Routray et. al., 2006]. Comprehensive ATM network planning problem using meta-heuristics has not been dealt with.

Genetic algorithms are based on evolution of genes. GA do not take into consideration the learning generated by cultural evolution. One of the limitations in GA based technique is quick convergence from local optima. Enhanced GA can be used to overcome this limitation. In Enhanced GA local search algorithms are implemented in the steps of GA to generate better solutions. The local search algorithm that has been considered in this paper is Hill climbing algorithm. In hill climbing the basic idea is to always head towards a state which is better than the current one. If such states are available the algorithm searches for those states and if there are no such states available then the algorithm terminates.

3.0 PROBLEM DESCRIPTION

While planning ATM network there are two sets of customers to be considered, the user who would be using the services through the network and the company that will be building the ATM network and maintaining it. Therefore while planning the ATM networks there are two principal objectives to be considered. One, the network should meet the end-users needs in terms of quality of service and cost. Two, for the network operator it should be as cost effective as possible to install and maintain the network. The second objective has traditionally been examined as reducing the first installed cost of the network. Minimizing the total cost is mainly a matter of finding shortest paths between the ATM nodes, as in installing a new network most of the money is spent on digging the cable ducts.

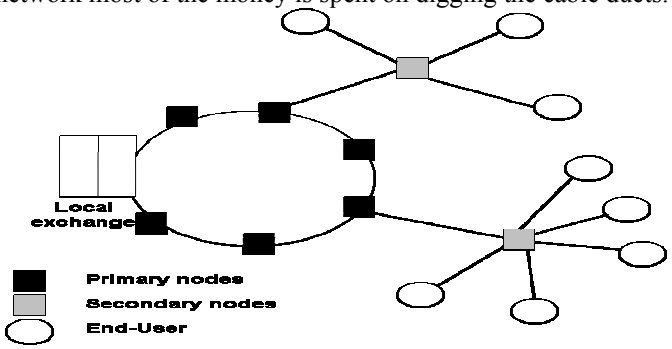


Figure 1: Schematic for a ATM planning

PON ATMs can be implemented in several topologies. One such configuration is a ring structure where the OLT (Optical Line Termination) in the central office can be seen as the root and the ONU (Optical Network Units) as the nodes in the ring. Customer access points are connected to the ONU in a star topology [en.wikipedia.org/wiki/GPON]. These devices take an optical fiber as input and split the signal carried on this fiber over a number of fibers on the output. Signal attenuation constraints require that the signal is only split at a maximum of two points between the exchange and customer. The first splitting point in the network is called the primary node. The second point at which the signal is split is called the secondary node. Typically 32 ONU's [en.wikipedia.org/wiki/GPON] can be connected to one OLT. The diagram [fig.1] shows a ring of fiber connecting the primary nodes and the method of connecting the end-users to these primary nodes. In this paper we have considered the case where there is a single connection from the primary to secondary node and from the secondary node to customer. This is likely to be the most common installation strategy for the ATM network as back-up links are very expensive.

When installing a new network in the access area, the majority of money has to be spent on digging the cable ducts. Thus, minimizing the total cost is mainly a matter of finding the shortest street paths which interconnect all ONUs with the OLT. A city map can be represented by a graph where the streets are the links, and the street junctions together with the ONUs and the OLT make up the nodes. In this paper we have taken the location of the exchange, the location of potential end-users, and a forecast of these end-users' demand in terms of number of lines and year as given. Variables being - Primary and secondary node locations, cable sizes and routes, Duct capacity and routes ,assignment of end-users to secondary nodes ,assignment of secondary nodes to primary nodes. The network must be implemented subject to the constraints of attenuation, maximum distance between a node and a customer and planning rules. The aim of the planner is to satisfy both the network's end-users and the network operator, by producing a reliable cost-effective network.

Objective: The objective of the optimization is to install a minimum net present cost network that satisfies the customer

demand criterion. Let the graph G= (V, E) be a set of V nodes; V= {1,…,n} and a set of E customers as edges; E = {1,…,m}. The objective function [Kratica] used to optimize the backbone network has been taken as:

Objective function = Minimize $\left(\sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} x_{ij} + \sum_{i=1}^{m} f_i y_i \right)$ [1]

subject to,

$$\sum_{i=1}^{m} x_{ij} = 1 \qquad [2]$$

$$\forall j \in J;$$

$$x_{ij} \in \{0,1\}$$

$$yi \in \{0,1\}$$

xij =1 : when end node is connected to concentrator j; otherwise 0

yi = 1 : when secondary node is established else 0

fi = cost of secondary node connected to primary node

$$\text{dij} = \sum_{i=1}^{n} \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2} \qquad [3]$$

Where,

xi, yi = co-ordinates of the ATM nodes

Along with the objective function - to optimize the time at which cable is installed into the network and to create a network that uses, the above allocations, split levels and positioning, a heuristic method has been used to achieve the installation strategy [Routray et. al.].

4.0 METHODOLOGY

The integer value is assigned to the respective link as a pseudo link weight which is not correlated to the real cost value of this edge. The pseudo link weights are only auxiliary parameters. The fitness has been calculated based on objective function given in [Eq.1]. The position of the primary and secondary nodes and the associated split-levels can be represented using a simple bit string. An individual in the population is therefore a combination of two types of genome; a list for representing allocation and a bit string for representing split level and secondary and primary node positions. The two can be evolved in parallel and the fitness score of the individual depends on the performance of both the genomes. Thus the initial problem is solved wherein the primary nodes are optimally connected to the local exchange in the ring topology.

4.1 Encoding Mechanism

The position of the primary and secondary nodes and the associated split-levels can be represented using a simple bit string as in (Fig. 4.2). Standard crossover and mutation operators can manipulate this. An individual in the population is therefore a combination of two types of genome; a list for representing allocation and a bit string for representing split level with secondary and primary node positions. The two can be evolved in parallel and the fitness score of the individual depends on the performance of both the genomes. Thus the initial problem is solved wherein the primary nodes are optimally connected to the local exchange in the ring topology.

The second stage is then to optimize the allocation of end-users to the secondary nodes and assigning secondary nodes to the primary nodes. For encoding the problem, the following methodology has been considered. There are m end-users and p secondary nodes a matrix of p*m is taken. A constant k is chosen based on the condition of fiber optics i.e. the maximum possible distance the signal can be transmitted without getting attenuated. Initially, the Configuration String (CS) is taken at random. The CS is created by the mechanism shown in fig. 2. CS follows the constraint that the distance between the end-node and the secondary node will be less than or equal to k. Also to optimize the time at which cable is installed into the network to create a network that uses the above allocations, split levels and positioning.

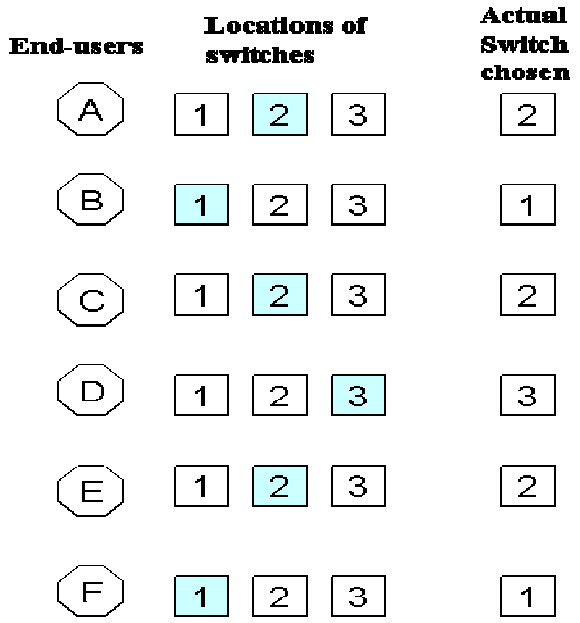


Figure 2: Encoding Mechanism

A heuristic method has been used to achieve this installation strategy. Heuristic used is:

4.1.1 Set year, y=0

4.1.2 For each customer with demand in y, connect it to the secondary nodes to which it is assigned by the shortest route through the duct network.

4.1.3 For each secondary node connected in the previous step connect it to the primary node to which it is assigned.

4.1.4 If y is the final year of the planning period then finish else increment y and go to 2.

This heuristic has been included in the objective function of a genetic algorithm so that iteration is not required between the

two stages. Costing of the installation is based on the net present worth of the plant in the year it is installed.

4.2 Network Optimization Using Ga

The following algorithm is followed for the backbone network:

```
pop = makeRandomPopulation
        while (not done)
         for each p in pop
                  p.fitness = evaluate(p)
                 for i = 1 to size(pop) by 2
                 ## select parents for reproduction
        parent1, parent2] = select two random solutions from pop
        [child1, child2] = crossover (parent1, parent2)
        mutate child1, child2
        replace old population with new population
```

4.2.1 Initial Population

The approach taken is to represent the problem using an ordered list of customers. The first n customers from the list are assigned to the first secondary node, the second n customers to the second node, etc. Fig 4.1 shows an example of this: the first primary node connects to the first four secondary nodes, which in turn connect to the first thirty-two customers in the list. This representation means that the GA cannot generate genomes that correspond to illegal network configurations.

4.2.2 Selection

The selection mechanism chosen is the Roulette wheel selection. In roulette wheel selection individuals are assigned a probability of being selected based on their fitness, $pi = fi / \Sigma fj$, Where pi is the probability that individual i will be selected, fi is the fitness of individual i, and Σfj represents the sum of the fitness of all individuals in the population. Similar to using a roulette wheel, fitness of an individual is represented as proportionate slice of wheel. Wheel is then spun and the slice underneath the wheel when it stops determines which individual becomes a parent.

4.2.3 Crossover

Two standard crossover operators are chosen for manipulating the above representation. These are the edge recombination crossover and the partial match crossover [Goldberg, 1991]. These operators are designed to manipulate permutations.

4.2.4 Mutation

New genetic parameter is introduced by the mutation operator. The values of individual genes are changed and, hence, new solutions are chosen. Mutation becomes important when after some generations the number of different strings decreases because strong individuals start dominating. In a situation of strong dominance of a few strings, the crossover operator alone would not bring any changes and the search for an optimal solution would be ended. To partially shift the search to new locations in the solution space, the mutation operator randomly alters genes. A mutation rate of 0.01 was taken for GA. The number of generations considered in the algorithm was 500.

4.2.5 Terminating Condition

The terminating condition has been taken as a constant with 500 generations.

4.2.6 Enhanced GA

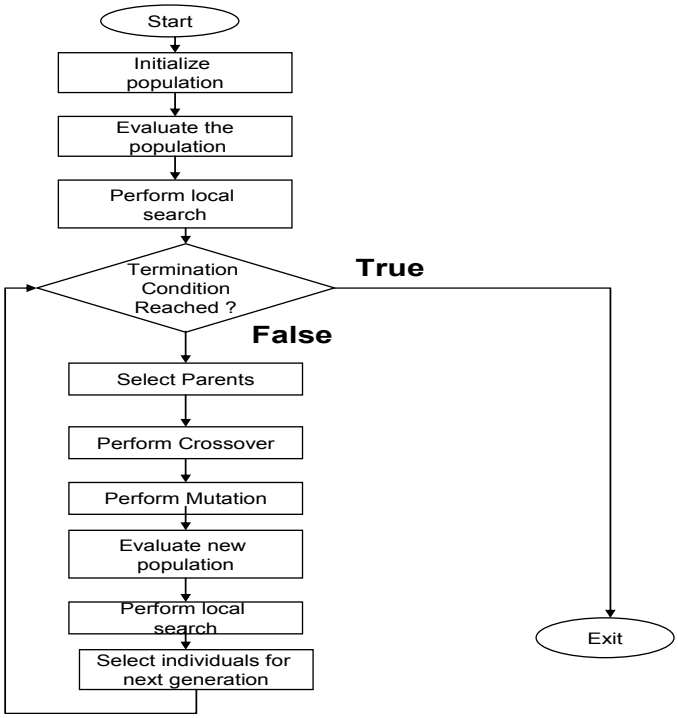


Figure 3: Flowchart of Enhanced GA

Initial Population Generation: Initial population is generated and then local search technique namely Hill Climbing algorithm is used to generate the initial solution string.

5.0 EXPERIMENTAL RESULTS

Enhanced Genetic algorithm has been used to find out an optimum connection using ring topology to connect the ATM nodes and to find end user connectivity. Numbers of experiments were conducted with varying population size. For all the experiments the results were recorded after a fixed number of 500 generations in our experimental data. The objective function in [Eq. 1] has been considered. The crossover rate of 0.6 and a mutation rate of 0.01 have been considered for the base GA. These parameters were established empirically from a series of test runs. The graph [Fig. 4] shows the average normalized cost of the best individual in the population at each generation for each operator. In the first phase with 50 ATM nodes it has been observed, the solutions obtained by Enhanced GA were better than the solutions obtained by GA.

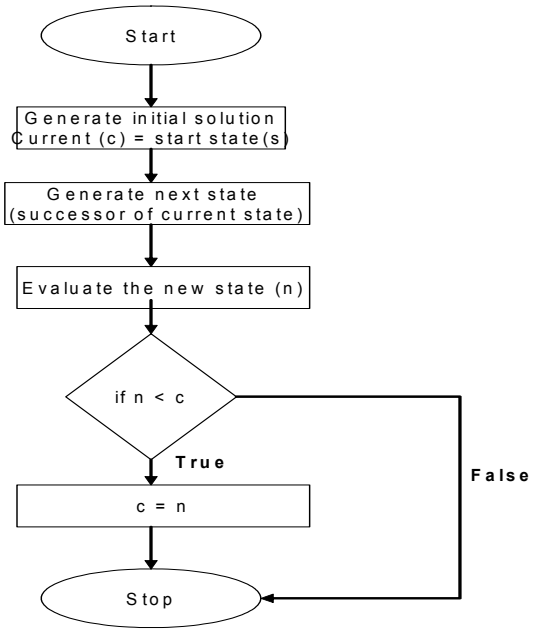


Figure 4: Flowchart of local search method

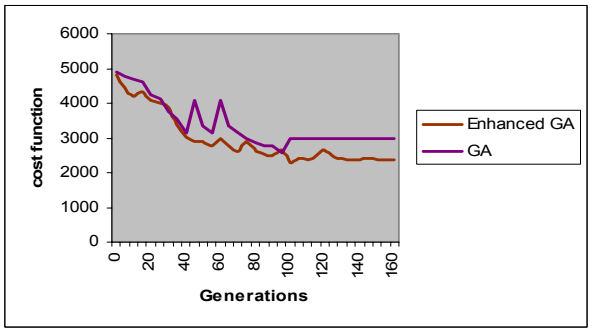


Figure 5

The comparison chart between GA & Enhanced GA for the Best cost average for 50 nodes. The cost of network design using Enhanced GA was 2986.53, which is better than GA. Also the time required to generate the solutions by Enhanced GA was much lesser than the time required by GA. It was also observed that with a smaller network size GA performed better than Enhanced GA but as the network size increased Enhanced GA performed better than GA (Table 1 & 2). The graph (Fig. 5) shows the average normalized cost of the best individual in the population at each generation for each operator. In the first phase with 50 ATM nodes it has been observed, the solutions obtained by Enhanced GA were better than the solutions obtained by GA.

ATM nodes	Time (min)	
	GA	EGA time
30	0.55	1.68
50	1.10	0.98
100	2.25	1.87

Table 1: GA and EGA comparison for connecting primary nodes in ring topology

ATM nodes	**Time min**	
	GA	**EGA**
30	1.25.	2.19
50	2.30	2.65
100	5.10	3.97

Table 2: GA and EGA comparison for network design

It was also observed that the time required to generate the solutions by Enhanced GA was much lesser than the time required by GA. In some cases GA gave better results than Enhanced GA but the time required was very high in GA. In all the cases it was observed that GA was slower than Enhanced GA.

The allocation of end-users to secondary and primary nodes can be treated as an ordering problem. The approach taken is to represent the problem using an ordered list of end-users. The first n end-users from the list are assigned to the first secondary node, the second n end-users to the second node, etc. Unlike many optimization techniques, Enhanced GA work effectively with discontinuous cost functions. The cost of assigning a customer to a node is calculated by finding the shortest path from the customer through the network of ducts to the node. The constraint that has been considered for assigning the end-users to the secondary nodes is that no more than 8 end-users can be connected to a single secondary node. The best results are shown for end-user networks using Enhanced GA [fig. 6].

In the figures a network with 100 end-users has been considered. It can be observed from the resultant network, the majority of the nodes in the network obtained by Enhanced GA supply nearby clusters of end-users. The time taken by GA is considerably higher than the time required by Enhanced GA. So for this specific problem of connecting the end-users with the secondary nodes it can be concluded that Enhanced GA works better than simple GA.

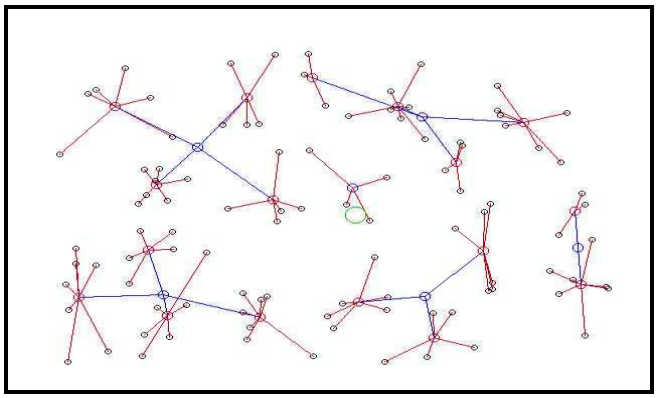


Figure 6: End-users connected to secondary nodes and secondary nodes connected to primary nodes in star topology using Enhanced GA.

6.0 CONCLUSION

An Enhanced GA based optimization system for ATM network has been designed, implemented and tested. In this paper we have designed an ATM network using Enhanced Genetic Algorithm approach. Considering the strategic and financial implications for communications providers, cost is very important factor in network planning. So it is very important that fiber networks are implemented in a cost-effective manner. Minimizing the total cost is mainly a matter of finding shortest paths between the ATM nodes, as in installing a new network most of the money is spent on digging the cable ducts. In this paper we have found the optimal paths to connect the primary nodes in the ring topology and also connected the end-users optimally with the secondary nodes in a star network and then the secondary nodes are connected to the nearest primary node. We have firstly used Enhanced GA to connect the primary nodes in ring topology and have then connected the end-users to the secondary nodes in star topology using Enhanced GA. As the results demonstrates that a Enhanced GA based optimization approach to network planning produces good network plans as compared to simple GA based approach networks. An optimization system such as the one described here will enable a planner to evaluate a large number of scenarios under different conditions.

REFERENCES

[1]. Abuali F.N., Schoenefeld D.A., & Wainwright R.L. (1994), Terminal assignment in a communications network using genetic algorithms. *Proc. 22nd Annual ACM Computer Science Conference (CSC'94)*, Phoenix, Arizona, USA, 74-81.

[2]. Balakrishnan A., Magnanti T., and Wong T. (1989), "A Dual-Ascent Procedure for large scale uncapacitated Network Design", *INFORMS Operation Research*, 37, pp. 716-740.

[3]. Carello G., Della Croce F., Giovanni L. De, Quagliotti M., Tadeo R.(2002) , "Optimal Telecommunication Network Design: problems, methods and applications", *exp*, volume 2, no. 3, 27-31..

[4]. Chardaire P., Kapsalis A., Mann J.W., Rayward-Smith V.J. and Smith G.D., (1995), "Applications of Genetic Algorithms in Telecommunications", In J. Alspector, R. Goodman, T.X. Brown (Eds.), *Proceedings of the 2nd International Workshop on Applications of Neural Networks to Telecommunications*, 290-299.

[5]. Davis L., Cox A., Qiu Y.(1993), "A Genetic Algorithm for Survivable Network Design", *Proc. Fifth International Conference on Genetic Algorithms,* Morgan Kauffman, 1993, pp 408-415.

[6]. Davis L., Coombs S.(1987), "Genetic Algorithm and Communication Link Speed Design: Theoretical Considerations", *Proc. Second International Conference on Genetic Algorithms*, Lawrence Erlbaum, 1987, pp 252-256.

[7]. Elbaum R. & Sidi M. (1995), "Topological design of local area networks using genetic algorithms", *IEEE INFOCOM'95*, Boston, Massachusettes, USA, v1, 64-71.

[8]. Gerla M., Monteiro J. A. S., Pazos R.(1989), "Topology Design and Bandwidth Allocation in ATM Nets", *IEEE. JSAC*, Vol. 7, No. 8, pp. 1253-1262.

[9]. Gerla M., Kleinrock L.(1977), "On the topological design of Distributed Computer Networks", *IEEE Transactions on Communications*, Vol. 25, No. 1, pp.55-67

[10]. Goldberg DE. (1991), Genetic Algorithm in search , optimization and machine learning, NewYork, Addison Wesley,1991.

[11]. Hasslinger, G., Schnitter, S., Franzke, M. (2005), "The Efficiency of Traffic Engineering with regard to Link Failure Resilience", *Telecommunication Systems Journal* 29 , 2005, 109-130.

[12]. Kim S. B., Kim M. J., Lee S. I.(1995), "Mathematical models for Dimensioning of ATM Networks" , *IEEE GLOBECOM'95*, Singapore, 1995

[13]. Kirkpatrick S, Gelatt C. D., Vechhi M. P.(1993), "Optimization by Simulated Annealing" Science, 220, pp 671-680.

[14]. Liu Xian (2003), " Network capacity allocation for traffic with time priorities", *Int. J. Network Mgmt 2003*, vol. 13 pp. 411-417.

[15]. Miguel Rios, Vladimir Marianov, and Cristian Abaroa (2005), "Design of Heterogeneous Traffic Networks Using Simulated Annealing Algorithms", *ICOIN 2005*, LNCS 3391, pp. 520-530.

[16]. Minoux M.(1987), "Network Synthesis and Dynamic Network Optimization." *Annals of Discrete mathematics*, 31:283–324.

[17]. Raychaudhuri D. and Wilson D.(1994), "ATM-Based Transport Architecture for Multiservices Wireless Personal Communication Networks ", *IEEE Journal On Selected Areas In Communications*, vol 12, No 8, pp 1401 – 1413.

Continued on page no. 323

Fuzzy Approach for Selecting Optimal COTS Based Software Products Under Consensus Recovery Block Scheme

P. C. Jha[1], Shivani Bali[2] and **P. K. Kapur[3]**

Submitted in March 2010; Accepted in December 2010

Abstract - The cost associated with development of a large and complex software system is formidable. In today's customer driven market, improvement of quality aspects in terms of reliability of the product is also gaining increased importance. But the resources are limited and the manager has to maneuver within a tight schedule. In order to meet these challenges, many organizations are making use of Commercial Off-The-Shelf (COTS) software. This paper develops a fuzzy multi objective optimization model approach for selecting the optimal COTS software product among alternatives for each module in the development of modular software system. The problem is formulated for consensus recovery block fault tolerant scheme. In today's ever changing environment, it is arduous to estimate the precise cost and reliability of software. Therefore, we develop a fuzzy multi objective optimization models for selecting optimal COTS software products. Numerical illustrations are provided to demonstrate the models developed.

Index Terms - Modular software, software reliability, COTS products, fault tolerance, fuzzy optimization.

1.0 INTRODUCTION

In our modern society, computers are used in diverse areas for various applications, for example, air traffic control, nuclear reactors, aircraft, real time military, industrial process control, and hospital patient monitoring systems. As the functionality of computer operations becomes more essential and complicated and critical software operations becomes more essential and complicated and critical software applications increase in size and complexity, there is a greater need for computer software reliability.

Software reliability is an important attribute of software quality, together with functionality, usability, performance, serviceability, capability, install ability, maintainability, and documentation. Software reliability is hard to achieve, because the complexity of software tends to be high. While any system with a high degree of complexity, including software, will be hard to reach a certain level of reliability, system developers tend to push complexity into the software layer, with the rapid growth of system size and case of doing so by upgrading the software.

[1,3]*Department of Operational Research, University of Delhi, Delhi, INDIA*
[2]*Lal Bahadur Shastri Institute of Management, Delhi, INDIA*
E-Mail: [1]lbsshivani@gmail.com

Commercial off-the-shelf (COTS) components engineering is an emerging paradigm for software development. Benefits of COTS based development include significant reduction in the development cost, time and improvement in the dependability requirement. Commercial off-the-shelf (COTS) components are used without any code modification and inspection. The components, which are not available in the market or cannot be purchased economically, can be developed within the organization. Component Based Software Engineering (CBSE) process model has become a kind of process model of software development project [6,9] Respective developers of the components provide information about their quality normally in terms of reliability. COTS components are received from distributor and are used 'as is'. No changes are normally made to their source codes. Only the code that is necessary to integrate these products is required to be developed in house. Large software systems have modular structures. The advancement of technology has made the use of COTS products as modules a possibility. A component can now be chosen for a module from the number of alternatives available in the market.

This paper proposes fuzzy multi objective optimization models for selecting the best COTS software product for each module. Software whose failure can have severe repercussions can be made fault tolerant through redundancy at module level [1]. Because of our present inability to produce error-free software, software fault tolerance is and will continue to be an important consideration in software systems. For some applications software safety is important and fault tolerance techniques used in those applications are aimed at preventing catastrophes. Multi version software fault tolerance techniques are based on the assumption that software built differently should fail differently and thus, if one of the redundant version fails, at least one of the others should provide an acceptable output. In [3, 4] reliability optimization problems for fault tolerant systems have been discussed. The authors have discussed two reliability models. In this paper, a fault tolerance architecture, which support consensus recovery block Scheme is proposed.

In the existing research in this area it is assumed that a crisp or a constant value of all the parameters is known. Jha et al formulated bi-criteria optimization model for selection of COTS based software system for consensus recovery block scheme by taking crisp estimates of reliability and cost [5]. However, in practice, it is not possible for a management to get precise value of reliability and cost for a software system. Or it may happen that they decide not to set precise levels due to the market considerations and are ready to have some tolerance of their objectives. When the precise values of parameter of the

problem are not known, the problem becomes a fuzzy optimization problem and the solution so obtained is a fuzzy approximation. Gupta et. al proposed a hybrid approach for selecting the optimal COTS software product in the development of modular software system[8].

This paper proposes two fuzzy multi-objective optimization models for selecting the best COTS software product for each module. The first optimization model (optimization model-I) of this paper is a joint optimization problem that maximizes the system reliability with simultaneously minimizing cost. The second optimization model (optimization model-II) considers the issue of compatibility between different alternatives of modules as it is observed that some COTS components cannot integrate with all the alternatives of another module. We assume the existence of virtual versions, apart from available versions, having negligible reliabilities and zero costs. Virtual versions are chosen only when we have insufficient budget. In a situation where this particular version is chosen, the corresponding alternative is not to be added to the system. The rest of the paper is organized as follows. Section 2 proposes notations. In section 3, we develop a crisp model and describe non –linear S-shape fuzzy membership functions in respect of both the chosen objectives, viz. the reliability and the cost. In this section, we also present fuzzy multi-objective optimization models for selecting the best COTS product for each module. Section 4 paper are illustrated with numerical example. Section 5, we furnish our concluding observations.

2.0 NOTATIONS

R : System quality measure

f_l : Frequency of use, of function l

s_l : Set of modules required for function l

R_i : Reliability of module i

L : Number of functions, the software is required to perform

n : Number of modules in the software.

m_i : Number of alternatives available for module i

V_{ij} : Number of versions available for alternative j of module i

c_{ijk} : Cost of version k of alternative j of module i (COTS)

t_1 : Probability that next alternative is not invoked upon failure of the current alternative

t_2 : Probability that the correct result is judged wrong.

t_3 : Probability that an incorrect result is accepted as correct.

Y_{ij} : Event that correct result of alternative j of module i is accepted.

X_{ij} : Event that output of alternative j of module i is rejected.

r_{ij} : Reliability of alternative j of module i

r_{ijk} : Reliability of version k of alternative j of module i

z_{ij} : Binary variable taking value 0 or 1

$$\begin{cases} 1, & \text{if alternative } j \text{ is present in module } i \text{ s} \\ 0, & \text{otherwise} \end{cases}$$

3.0 MULTI-OBJECTIVE OPTIMIZATION MODELS SELECTING COTS PRODUCTS

In this section, we formulate COTS software products selection problem as an optimization problem with multiple objectives. The first optimization model is developed for the following situations, which also holds good for the second model, but with additional assumptions related to compatibility among alternatives of a module.

The following are the assumptions of optimization Models:

3.0.1 There is a specified budget for the development of software system.

3.0.2 A software system consists of a finite number of modules.

3.0.3 A software system is required to perform a known number of functions. The program written for a function can call a series of modules $(\leq n)$. A failure occurs if a module fails to carry out an intended operation.

3.0.4 Codes written for integration of modules don't contain any bug.

3.0.5 Several alternatives are available for each module. Fault tolerant architecture is desired in the modules (it has to be within the specified budget). Independently developed alternatives (primarily COTS components) are attached in the modules and work similar to the recovery block scheme discussed in [3,4].

3.0.6 The cost of an alternative is the development cost, if developed in house; otherwise it is the buying price for the COTS product. Reliability for all the components are known and no separate testing is done.

3.0.7 Different versions with respect to cost and reliability of a module are available.

3.0.8 Other than available cost-reliability versions of an alternative, we assume the existence of a virtual versions, which has a negligible reliability of 0.001 and zero cost. These components are denoted by index one in the third subscript of x_{ijk}, c_{ijk} and r_{ijk}. for example r_{ij1} denotes the reliability of first version of alternatives j for module i, having the above property.

3.1 Multi-Objective Optimization Model I

In the first optimization model it is assumed that the alternatives of a module are in a consensus recovery block [10]. Consensus recovery block requires independent development of independent alternatives of a program, which the COTS

components satisfy and a voting procedure. Upon invocation of the consensus recovery block all alternatives are executed and their outputs are submitted to a voting procedure. Since it is assumed that there is no common fault, if two or more alternatives agree on one output then that output is designated as correct. Otherwise the next stage is entered. At this stage the best version is examined by an acceptance test. If the output is accepted, it is treated as the correct one. However if the output is not accepted, the next best version is subject to testing. This process continues until an acceptable output is found or all outputs are exhausted.

Problem (P1)

$$\text{Maximize } R = \sum_{l=1}^{L} f_l \prod_{i \in s_l} R_i \qquad (1)$$

$$\text{Minimize } C = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \sum_{k=1}^{V_{ij}} c_{ijk} x_{ijk} \qquad (2)$$

Subject to

$$X \in S = \{ X_{ijk} \text{ is binary variable}$$

$$R_i = 1 + \left[\sum_{j=1}^{m_i} \frac{1}{(1-r_{ik})^{z_{ik}}} \left[\prod_{k=1}^{m_i} (1-r_{ik})^{z_{ik}} \right] \left[1 - \left(1-r_{ij}\right)^{z_{ij}} \right] + \prod_{j=1}^{m_i} \left(1-r_{ij}\right)^{z_{ij}} \right] \qquad (3)$$

$$\left[\sum_{j=1}^{m_i} z_{ij} \left[\prod_{k=1}^{j-1} P\left(X_{ik}\right)^{z_{ij}} \right] P\left(Y_{ij}\right)^{z_{ij}} - 1 \right] ; \; i = 1,2,.....n$$

$$P\left(X_{ij}\right) = \left(1-t_1\right)\left[\left(1-r_{ij}\right)\left(1-t_3\right) + r_{ij} t_2\right]$$

$$P\left(Y_{ij}\right) = r_{ij}\left(1-t_2\right)$$

$$r_{ij} = \sum_{k=1}^{V_{ij}} x_{ijk} r_{ijk} \quad j = 1,2,.....,m_i \text{ and } i = 1,2,.....n \qquad (4)$$

$$\sum_{k=1}^{V_{ij}} x_{ijk} = 1, \text{ for } j = 1,2,.....,m_i \text{ and } i = 1,2,.....,n \qquad (5)$$

$$x_{ij1} + z_{ij} = 1; \; j = 1,2,.....m_i \qquad (6)$$

$$\sum_{j=1}^{m_i} z_{ij} \geq 1 \; ; i = 1,2,.....,n \qquad (7)\}$$

Objective function (1) maximizes the system quality (in terms of reliability) through a weighted function of module reliabilities. Reliability of modules that are invoked more frequently during use is given higher weights. Analytic Hierarchy Process (AHP) can be effectively used to calculate these weights and (2) minimize the overall cost of the system.

Constraint (3) estimates the reliability of module i. As it has been assumed that the exception raising and control transfer programs work perfectly, a module fails if all attached alternatives fail.

Constraint (5) ensures that exactly one version is chosen from each alternative of a module. It includes the possibility of choosing a dummy version. Equation (6) and (7) guarantee that not all chosen alternatives of module are dummies. Optimization model-I is a 0-1 Bi-Criterion integer programming problem. An example is solved using software package LINGO.

It is observed that some alternatives of a module may not be compatible with alternatives of another module. The next optimization model II addresses this problem. It is done, incorporating additional constraints in the optimization models. This constraint can be represented as $x_{gsq} \leq x_{hu_t c}$, which means that if alternative s for module g is chosen, then alternative $u_t, t = 1,.....z$ have to be chosen for module h. We also assume that if two alternatives are compatible, then their versions are also compatible.

$$x_{gsq} - x_{hu_t c} \leq M y_t$$

$$q = 2,.....,V_{gs}, \; c = 2,.....,V_{hu_t}, s = 1,.....,m_g \qquad (8)$$

$$\sum y_t = z\left(V_{hu_t} - 2\right) \qquad (9)$$

Constraint (9) ensures that only one alternative is compatible.

Constraint (3) to (7) is equivalent to problem (P1). Constraint (8) and (9) make use of binary variable y_t to choose one pair of alternatives from among different alternative pairs of modules. If more than one alternative compatible component is to be chosen for redundancy, constraint (9) can be relaxed as follows.

$$\sum y_t \leq z\left(V_{hu_t} - 2\right) \qquad (10)$$

Constraint (10) ensure more than one alternative is compatible.

3.2 Multi-Objective Optimization Model II

Problem (P1) can be transformed to another optimization problem using compatibility constraint as follows.

$$\text{Maximize} \qquad R = \sum_{l=1}^{L} f_l \prod_{i \in s_l} R_i$$

$$\text{Minimize} \qquad C = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \sum_{k=1}^{V_{ij}} c_{ijk} x_{ijk}$$

Subject to

$$X \in S$$

$$x_{gsq} - x_{hu_t c} \leq M y_t$$

$$q = 2,.....,V_{gs}, \; c = 2,.....,V_{hu_t}, s = 1,.....,m_g$$

$$\sum y_t = z\left(V_{hu_t} - 2\right)$$

$$\sum y_t \leq z\left(V_{hu_t} - 2\right)$$

Similar constraints can be written for all pairs of compatible modules.

3.3 Selection Model For Cots Software Products Based On Fuzzy Decision Theory

The model formulation for the above said problem requires an estimate of reliability and cost for various alternative COTS in the modules. Due to the changing environment, these estimates cannot be determined definitely because cost and reliability are affected by ambiguous and uncertain factors which cannot be measured precisely. Also the decision maker's assessment about these estimates may be based on incomplete knowledge about the COTS product itself and other aspects (e.g. vendor's credentials).Under such conditions; making a decision based upon crisp model is not the best decision. Since software development cost is ever changing and it becomes difficult to estimate the definite cost and reliability of the software. Therefore the issue of selecting COTS software products becomes the one of a choice from a fuzzy set of subjective/intuitive interpretations, the term fuzzy being suggestive of the diversity of both the decision maker's objective functions as well as that of the constraints.

Therefore, we formulate fuzzy multi-objective optimization model for COTS software products selection based on vague aspiration levels, the decision maker may decide his aspiration levels on the basis of past experience and knowledge possessed by him. To express vague aspiration levels of the decision, various membership functions have been proposed [13, 14]. A fuzzy linear programming problem with non linear membership function results in a non linear programming problem. Usually, a linear membership function is employed to avoid nonlinearity. Also, if membership function is interpreted as the fuzzy utility of the decision maker, which describes the behavior of indifference, preference or aversion towards uncertainty, a non linear membership function is a better representation than a linear membership function.

In this paper, we use a logistic function [12], i.e. a non linear S-shape membership function to express vague aspiration levels of the decision maker. The S-shape membership function is given by

$$f(x) = \frac{1}{1+\exp(-\alpha x)}$$

where α, $0 < \alpha < \infty$ is a fuzzy parameter which measures the degree of vagueness. The reason why we use this function is that, it is easily handled. Also, the logistic membership function preserves linearity even when the operator "product" is used instead of the operator "min" to aggregate the overall satisfaction to arrive at the fuzzy set decision.

In the MOP model proposed in Section 3.1 and 3.2, the two objectives i.e. the reliability and the cost are considered to be ambiguous and uncertain. We use the following nonlinear S-shape membership functions to express the vague aspiration levels.

- The membership function of the goal for the reliability is given by

$$\mu_R(x) = \frac{1}{1+\exp\left(-\alpha_R\left(\sum_{l=1}^{L} f_l \prod_{i\in s_l} R_i \text{-R}_m\right)\right)}$$

where R_m is the mid-point (middle aspiration level for the reliability) at which the membership function value is 0.5 and α_R can be given by decision maker based on his own degree of satisfaction.

- The membership function of the goal for the cost is given by

$$\mu_C(x) = \frac{1}{1+\exp\left(\alpha_C\left(\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{k=1}^{V_{ij}} c_{ijk}x_{ijk} - C_m\right)\right)}$$

where C_m is the mid-point (middle aspiration level for the cost) at which the membership function value is 0.5 and α_C can be given by decision maker based on his own degree of satisfaction.

Following Bellman-Zadeh's Maximization principle [2] and using the above defined fuzzy membership functions, the fuzzy multi-objective optimization model for selecting the COTS software products is formulated as follows:

Problem P

$$\max \ \lambda$$

$$s.t \ \lambda \le \mu_R(x),$$

$$\lambda \le \mu_C(x),$$

$$0 \le \lambda \le 1,$$

and the constraints (3) to (7).

Fuzzy multi-objective optimization model (P) is solved for maximized degree of membership for the fuzzy decision. In this approach all the fuzzy objectives are treated equivalently. However, approaches have been discussed in literature with situations in which the objectives are not equally important [7, 11].

4.0 ILLUSTRATIVE EXAMPLES

Consider a software system having two modules with more than one alternative for each module. The cost reliability data set is given in Table-1. Note that the cost of first version i.e. the virtual versions for all alternatives is zero and reliability is 0.001. This is done for the following reason: If in the optimal solution, for some module $x_{ij1} = 1$, that implies corresponding alternative is not to be attached in the module.

Let $L = 3,\ s_1 = \{1,2\},\ s_2 = \{1\},\ s_3 = \{2\},\ f_1 = 0.5,\ f_2 = 0.3$ and $f_3 = 0.2$.

It is also assumed that $t_1 = .01, t_2 = .05$ and $t_3 = .01$

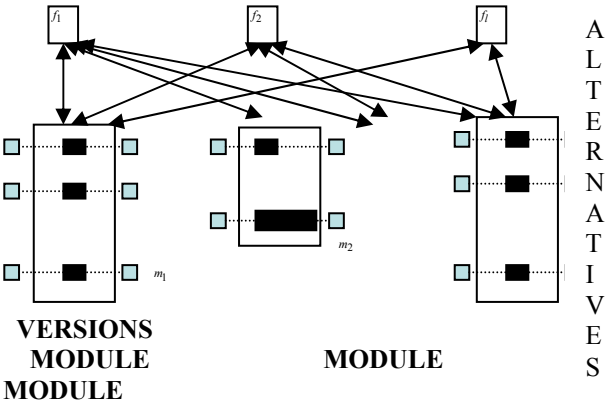


Figure 1: Structure of the software

Cost and Reliability Dataset

Modules	Alternatives	Versions 1		2		3	
		Cost	Reliability	Cost	Reliability	Cost	Reliability
1	1	0	0.001	8.2	.90	9.0	.88
	2	0	0.001	7.5	.86	9.0	.92
	3	0	0.001	8.5	.90	9.5	.88
2	1	0	0.001	3.2	.87	4.0	.86
	2	0	0.001	3.4	.91	4.3	.89
	3	0	0.001	5.0	.89	6.8	.86
	4	0	0.001	4.8	.86	6.8	.88

By taking $\alpha_R = 0.60$ and $\alpha_c = 16$

4.1 Optimization Model I

The problem is solved using software package LINGO [8]. Following solution is obtained.

$$x_{111} = x_{122} = x_{132} = 1$$

$$x_{211} = x_{222} = x_{232} = x_{242} = 1$$

It is observed that two or more alternatives are chosen for each module. Redundancy is allowed for both the modules. The system reliability for the above solution is 0.79 and cost is 30.5 units and the achievement level of membership function is $\lambda = 0.58$.

4.2 Optimization Model- II

To illustrate optimization model for compatibility, we use previous results. We assume second alternative of second module is compatible with second and third alternatives of first module. Following solution was obtained using LINGO.

$$x_{111} = x_{123} = x_{132} = 1$$

$$x_{211} = x_{222} = x_{223} = x_{243} = 1$$

It is observed that due to the compatibility condition, second alternative of first module is chosen as it is compatible with second alternative of second module. The system reliability for the above solution is 0.79 and cost is 32 units and the achievement level of membership function is $\lambda = 0.58$.

5.0 CONCLUSION

In this paper, fuzzy multi-objective optimization model approach for selecting the optimal COTS software product among alternatives for each module in the development of modular software system is discussed. The problem is formulated for consensus recovery block fault tolerant scheme. In today's ever changing environment, it is arduous to estimate the precise cost and reliability of software. For such situation where the software is developed by assembling COTS software products, then it is not possible to get the crisp estimates of cost and reliability of these COTS products. Therefore, we have drawn on fuzzy methodology for the estimation of reliability and cost. This developed approach can effectively deal with the vagueness and subjectivity of expert information.

REFERENCES

[1]. Belli F, Jadrzejowich P. "An approach to reliability optimization of software with redundancy" IEEE transactions on Software Engineering 1991; 17(3): 310-312

[2]. Bellman, R., Zadeh, L.A.:"Decision making in a fuzzy enviornment", Management Science 17, 1970; 141-164

[3]. Berman O, Dinesh Kumar U. "Optimization models for recovery block schemes" European Journal of Operational Research 1999; 115: 368-379

[4]. Dinesh Kumar U, "Reliability Analysis of fault tolerant recovery block", OPSEARCH, 1998; 35(2), 281-294

[5]. Jha P.C. , Shivani Vaid and Kapur P.K. " Optimal Component Selection For Fault Tolerance COTS Based Software Under Consensus Recovery Block Scheme", INDIACoM-2009,387-390

[6]. Meyers, B.C., Oberndorf, P., "Managing Software Acquisition Open systems and COTS products." Addison-Wesley, Reading (2002)

[7]. Narasimhan, R.: "On fuzzy goal programming – some comments",Decision Sciences 12;1981; 532-538

[8]. Gupta P., Mehlawat M.K., Mittal G., Verma S,"A Hybrid Approach for selecting Optimal COTS Products ", Computional Science and its Application-ICCSA 2009;Springer publication; 5592; 949-962.

[9]. Roger, S.P.: "Software Engineering: A Practitoner's Approach", McGraw Hill Companies, 5th Edition, New York 2001
[10]. Scott RK, Gautt JW and Mc Alliter DF "Fault tolerant software reliability modelling" IEEE transactions on Software Engineering 1987; 582-592
[11]. Tiwari, R.N., Dharmar, S., Rao, J.R.: "Fuzzy goal programming – an additive model", Fuzzy Sets and systems24, 1987;27-34
[12]. Watada, J.:" Fuzzy portfolio selection and its applications to decision making",Tatra Mountains Mathematical Publications 13, 1997; 219-248.
[13]. Zimmermann, H.-J.:"Description and optimization of fuzzy systems". International Journal of General Systems 2; 1976;209-215
[14]. Zimmermann, H.-J.:"Fuzzy programming and linear programming with several objective functions." Fuzzy Sets and Systems 1; 1978; 45-55

Continued from page no. 317

[18]. Routray S., Sherry A. M., Reddy B. V. R.(2005), "A Genetic Algorithm Approach for Dynamic Routing of ATM Networks", *Paradigm* Vol. IX, No. 1, January-June 2005, pp 86-92.
[19]. Routray S., Sherry A. M., Reddy B. V. R.(2006), "Bandwidth Optimization through Dynamic Routing in ATM Networks: Genetic Algorithm &Tabu Search Approach" IJCS *International Journal of Computer Science*, Vol. 1., No. 3, pp 188-194.
[20]. Routray S., Sherry A. M., Reddy B. V. R.(2006), "Handoff Scheme for Wireless ATM Network: A Genetic Algorithm Approach" *The 4th International Conference on Computing, Communications and Control Technologies*: CCCT '06, 2006.
[21]. S. Routray, A. M. Sherry, B. V. R. Reddy, "ATM network planning: A genetic Algorithm Approach", Journal of Applied & Theoretical Information Technology (JATIT), available through EBSCO Publishing USA, Volume 3 No.4, December 2007 pp 72-79.
[22]. Srinivas M., Patnaik Lalit M.(1994), "Genetic Algorithms: A survey", *IEEE*, 1994, 17-26.
[23]. Srinivas M., Patnaik Lalit M. (1994), "Adaptive probabilities of crossover and Mutation in Genetic Algorithms", *IEEE Trans. System*,1994, 656-667.
[24]. Thompson D. R., Bilbro G. L.(2000), "Comparison of a genetic algorithm with a simulated annealing algorithm for the design of an ATM network", *Communications Letters, IEEE* Volume 4, Issue 8, Page(s):267 – 269.
[25]. Wong P. and Britland D.(1993), " Mobile Data Communication ", Artech House, 1993.
[26]. Wu T., Kolar D. J., and Cardwell R. H.(1998), "Survivable Network Architectures for Broadband Fiber Optic Networks: Models and Performance Comparisons", *IEEE Journal of Lightwave Technology*, vol. 6, no. 11, pp. 1698-1709.

Iterative Self Organized Data Algorithm for Fault Classification of Mechanical System

Jayamala K. Patil[1], P. B. Ghewari[2] and **S. S. Nagtilak[3]**

Submitted in February 2010; Accepted in August 2010

Abstract - ***The challenging issue for mechanical industry is to develop fast & reliable fault diagnosis systems before total breakdown of machine. Fault diagnosis & classification of faults of mechanical systems is a difficult task. It improves productivity & reduces cost of production. This paper presents an approach for classification of commonly observed faults in gears of mechanical system. These faults include weared gear, gear with one tooth broken & gear with crack on one tooth. The Power Spectral Density (PSD) of the vibration signals of faulty gears is used to construct feature vectors. Principle component analysis (PCA) is used to reduce the dimensions of feature vector. The Routine checkup of the machine generates Known fault vectors. The ISODATA (Iterative Self Organizing Data Analysis Technique) [1] classifies fault vectors along with newly collected fault vector. If the fault is different from the previously identified fault a new fault cluster is created else new fault belongs to one of previously identified fault clusters.***

1.0 INTRODUCTION

The complexity of engineering systems increases the danger of failure of system/machine. This affects productivity, & environment. With complex machines the maintenance cost increases. Hence fast & precise identification of faults is essential.

Fault can be defined as an abnormal state of a machine or system such as malfunction or dysfunctions of part or an assembly .[3]

The critical element in any machine is Gear. The study carried out in Germany, on samples of gears shows that 19-24% failure of mechanical system is usually because of mishandling or inadequate maintenance. This study also shows that damage or failure caused by gears & bearings is in the ratio of 3:1.about 60% failures are because of faults in gear; 19% failures are because of faults in bearings & 10% failures are because of faults in shafts. [4]

The process of fault diagnosis consist of fault detection & classification of fault. The faults in gears can be detected by using vibrations generated from it.

The vibration analyst of a machine requires detailed knowledge of a mechanical system, dynamic properties of machine along with history of it's maintenance .

This paper provides the approach of identifying the type of fault occurred in gear system. This provides novel approach of using pattern recognition algorithm named as ISODATA for classification of faults in gear system. The computing efficiency of the classifier is improved by reducing feature vector dimension using Principal component analysis. The method suggested above helps inexperienced machine user to detect various fault in machine under observation.

The present methods of fault classification includes use of Learning Machine,. Hoelder Exponents, PCA, ANN, Support Vector Machine, Generalized Discriminant Analysis, WT-ANN, Case Based Reasoning etc.

[1,2,3] *Department of Electronics and Telecommunication, Bharati Vidyapeeth College of Engineering, Kolhapur, Maharashtra, INDIA*
E-Mail: [1]jayamala.p@rediffmail.com,
[2]p_ghewari@rediffmail.com and
[3]sameer_nagtilak@rediffmail.com

2.0 THE ISODATA ALGORITHM [1]

ISODATA stands for *Iterative Self-Organizing Data Analysis Techniques*. This is a more sophisticated algorithm which allows the number of clusters to be automatically adjusted during the iteration by merging similar clusters and splitting clusters with large standard deviations.

We first define the following parameters:

1. K = number of clusters desired;
2. I = maximum number of iterations allowed;
3. P = maximum number of pairs of cluster which can be merged;
4. Θ_N= a threshold value for minimum number of samples in each cluster can have (used for discarding clusters);
5. θs = a threshold value for standard deviation (used for split operation);
6. θc= a threshold value for pairwise distances (used for merge operation).

The algorithm:

Step1: Arbitrarily choose k (not necessarily equal to K) initial cluster centers:

M_1, M_2, ……., M_k from the data set { Xi , i=1, 2…….,N}

Step2: Assign each of the N samples to the closest cluster center:

$$X \sim \omega_j \quad if \quad D_L(X, M_j) = max \left\{ D_L(X, M_i), \quad i = 1, \cdots, k \right\}$$

Step3: Discard clusters with fewer than θN members, i.e., if for any j , $N_J < \theta_N$ then discard Wj and k. k-1

Step4: Update each cluster center:

$$M_j = \frac{1}{N_j} \sum_{X \sim \omega_j} X \quad (j = 1, \cdots, k)$$

Step5: Compute the average distance Dj of samples in cluster Wj from their corresponding cluster center:

$$D_j = \frac{1}{N_j} \sum_{X \in w_j} D_L(X, M_j) \quad (j = 1, \cdots, k)$$

Step6: Compute the overall average distance of the samples from their respective cluster centers:

$$D = \frac{1}{N} \sum_{j=1}^{k} N_j D_j$$

Step7:If k ≤ k/2 (too few clusters), go to Step 8; else if k>2k (too many clusters), go to Step 11; else go to Step 14.
(Steps 8 through 10 are for split operation, Steps 11 through 13 are for merge operation.)

Step8: First step to split. Find the standard deviation vector ∑ j = [σ1(j) ,….., σ n(j)]T for each cluster:

$$\sigma_i^{(j)} = \sqrt{\frac{1}{N_j} \sum_{X \in w_j} (x_i - m_i^{(j)})^2}, \quad (i = 1, \cdots, n, \ j = 1, \cdots, k)$$

where ,
$m_i^{(j)}$ is the i^{th} component of M_J and σ_i is the standard deviation of the samples in Wj along the i^{th} coordinate axis. Nj is the number of samples in Wj.

Step9: Find the maximum component of each∑ j and denote it by σ_{max} (j) ; Do this for all

$$j = 1, \cdots, k$$

.

Step10: If for any σmax(j) , (j =1,…..,k) , all of the following are true

$$\sigma_{max}^{(j)} > \Theta_S$$

,

$$D_j > D$$

,

$$N_j > 2\Theta_N$$

Then *split* Mj into two new cluster centers Mj(+) and Mj(-) by adding ±δ to the component of Mj corresponding to σmax(j) , where δ can be α σmax(j) , for some α >0. Then delete Mj and let k. k -1. Go to Step 2 else Go to Step 14.

Step11: First step to merge. Compute the pairwise distances Dij between every two cluster centers:

$$D_{ij} = D_L(M_i, M_j), \quad (for \ all \ i \neq j)$$

and arrange these k(k-1)/2distances in ascending order.

Step12: Find no more than P smallest Di j 's which are also smaller than θC and keep them in ascending order:

$$D_{i_1 j_1} \leq D_{i_2 j_2} \leq \cdots \leq D_{i_P j_P}$$

Step13: Perform *pairwise merge*: for l = 1,……P, do the following:
If neither of M_i and M_j l has been used in this iteration,
Then merge them to form a new center:

$$M = \frac{1}{N_{i_l} + N_{j_l}} [N_{i_l} M_{i_l} + N_{j_l} M_{j_l}]$$

Delete M_{il} and $M_{j\,l}$, and let k. ← k -1. Go to Step 2.

Step14: Terminate if maximum number of iterations I is reached. Otherwise go to Step 2.

The ISODATA algorithm is more flexible than the K-mean method. But the user has to choose empirically many more parameters listed previously.

3.0 EXPERIMENTAL SET UP

It consists of an half HP induction motor mounted on rigid steel structure. Driven gear is mounted on motor shaft. The load is coupled to driver gear by driven gear. The machine runs at constant speed of 1470 RPM at constant load (80 % of rated capacity). Both gears are identical having 62 teeth. Different Fault conditions were created on driven gear typically weared gear, cracked tooth, broken tooth. Figure 1 shows photograph of the model of experimental set up kept on rubber pad. These pads are used to reduce weak foundation fault effects on feature vector sets.

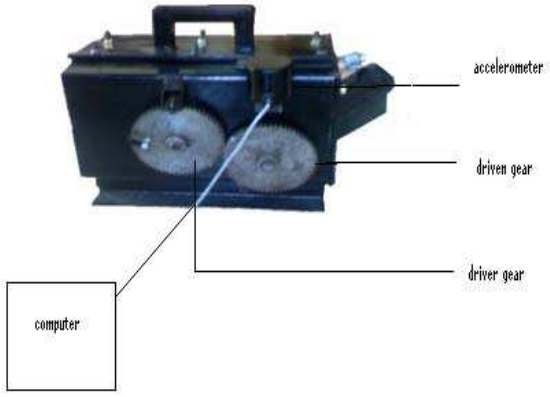


Figure 1: Model of experimental set up

Using this set up the faulty vibration signatures are collected by accelerometer & stored in memory of computer.

3.1 Artificially Creation of Faults on Gear Tooth.[5]

The common faults observed in Spur gear are:

3.1.1 Weared gear : This fault was created by filing the gear teeth in both direction of rotation to remove the material from teeth up to 500 micron.

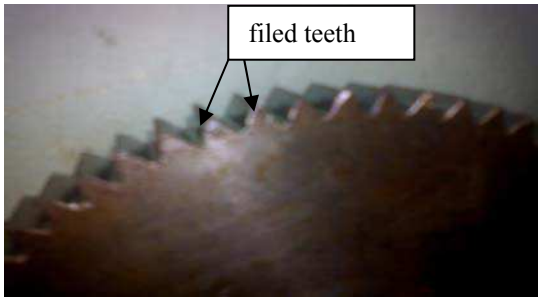


Figure 2: Weared Gear

3.1.2 One Tooth Broken Or Missed: To get signal of this condition ,the gear tooth was removed by hack-saw blade.

Figure 3: Gear with One Tooth Broken or Missed

3.1.3 Crack On One Tooth: The signal of this condition is obtained by cutting the tooth with hack-saw blade at the root of the tooth in the direction of rotation.

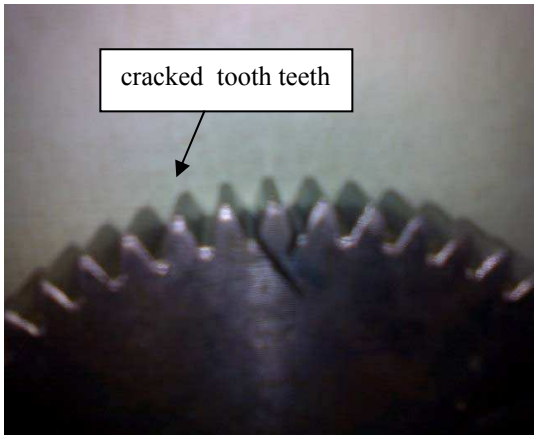


Figure 4: gear with crack on one tooth

3.2 Construction of Accelerometer

The accelerometer used in this set up uses ring type crystal as a sensor which has a mass attached to one of its surfaces. When the mass is subjected to a vibration signal, the mass converts the vibration (acceleration) to a force, this then being converted to an electrical signal representative of the incoming vibration signal as shown in following figure. This is the basis of the Accelerometer. The accelerometer output may then be processed to provide the instantaneous velocity and displacement signals.

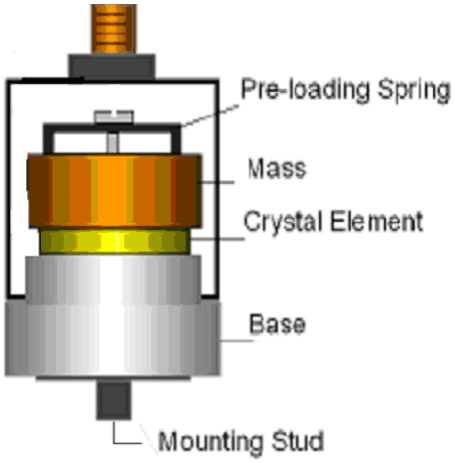


Figure 5: Accelerometer

3.3 PROCEDURE FOR RECORDING SIGNAL

3.3.1 The motor is run at the rated speed of 1470 rpm. Load is applied by providing sufficient tension to break & pulley system.

3.3.2 The accelerometer is mounted near the driven gear & its output is connected to microphone input of sound card of computer.

3.3.3 First the readings for non–defective, good lubricated gear condition are recorded using 'Gold wave' software for a period of one minute. It is stored for further analysis and comparison with other signals derived from faulty gears mentioned above.

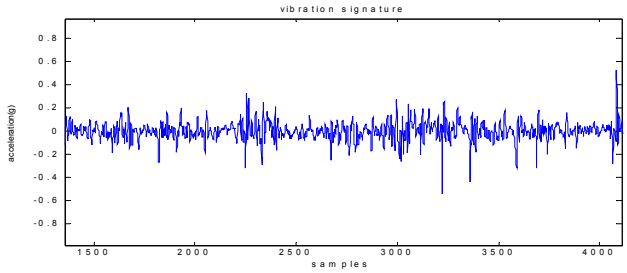
3.3.4 The non-defective gear is then removed using gear puller and replaced by faulty gears. For each faulty gear signal derived from accelerometer is recorded & stored in memory of computer in wave file format for further analysis.

3.3.5 For each reading load & speed conditions are kept constant.

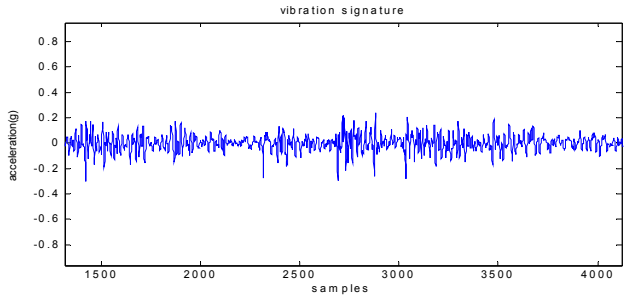
3.3.6 The accelerometer signal is sampled at the sampling rate of 44100 samples per seconds. Each sample is of 16 bit, MSB reserved for sign. Gear mesh frequency of machine under observation is 24.5 RPS x 62 teeth = 1519 Hz. The second and third harmonics shoes significant amplitude and sidebands along the gear mesh frequency harmonic. Hence sampling rate of 44100 samples per second proved sufficient throughout experimentation.

4.0 RESULTS

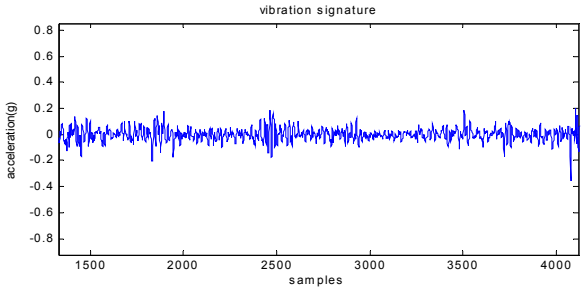
Figure 6 shows the vibration signal for each type of gear.



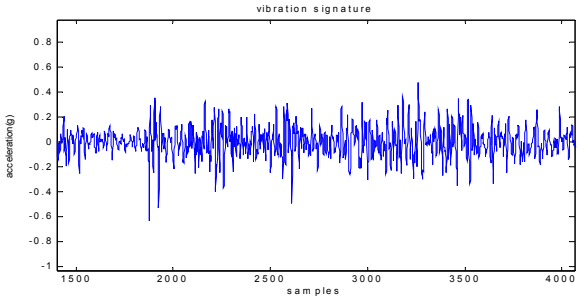
Good Gear



Gear With Broken Tooth



Gear With Cracked Tooth



Weared Gear

Figure 6: Vibration Signature

By observing above signatures/signals its difficult to recognize type of fault**.**

4.1 Kurtosis

The kurtosis can be used to check the distribution of signal.. Kurtosis is a measure of how outlier-prone a distribution is. The kurtosis of the normal distribution is 3. Distributions that are more outlier-prone than the normal distribution have kurtosis greater than 3; distributions that are less outlier-prone have kurtosis less than 3.

The kurtosis of a distribution is defined as

$k=E(x-\mu)4 \ /\sigma 4$

where,

μ is the mean of x,

σ is the standard deviation of x,

E(t) represents the expected value of the quantity

The kurtosis of good lubricated gear is low indicating normal signal distribution while other signals shows higher kurtosis indicating outlier –prone distribution. Table1 shows kurtosis of all gear signals is given in table1

Type of signal	Kurtosis
Lubricated good gear	4.8383
Gear with one tooth broken	7.4362
Gear with crack on one tooth	9.4898
Warned gear	6.8536

Table1: Kurtosis

The observations in table show different kurtosis value for each type of gear signal; but from this value we cannot predict type of fault in the gear. Hence some type of intelligent system should be used to identify the fault. This paper used ISODATA to identify the fault.

4.2 Feature Vector Generation and PCA

The feature vectors are generated by determining 256 point Power Spectral Density (PSD) of fault signal . This produces set of dimensional feature vectors from each type of class/fault signal. Figure 7 shows Power spectral density of each type of fault:

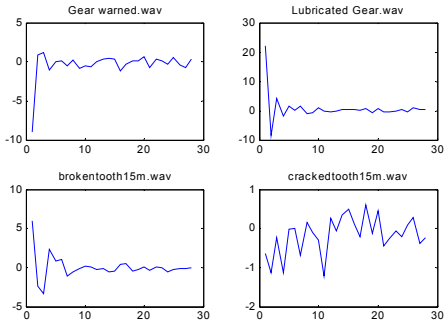


Figure 7: PSD of All Types Of Signals Of Gear Vibration.

The dimensionality of this feature vector is large & may result in to large classification or training period. Hence it is needed to reduce the dimensionality of input vector .For this Principle Component Analysis (PCA) [2] is used.

PCA removes redundant information. PCA has three effects:

4.2.1 It orthogonalise the components of input vectors ; so that they are uncorrelated with each other.

4.2.2 It orders the resultants orthogonal components (Principle Components), so that those with largest variation come first.

4.2.3 It eliminates those components which contribute least to the variations in the data set.

4.3 CLASSIFICATION OF FAULTS (USING ISODATA)

4.3.1 Classified fault database

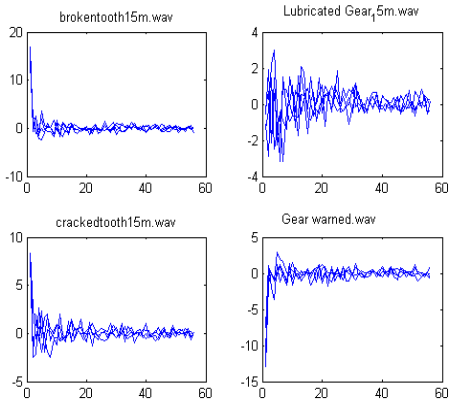


Figure 8: Classified fault database

4.3.2 Locating unknown fault

4.3.2.1 Weared Gear:

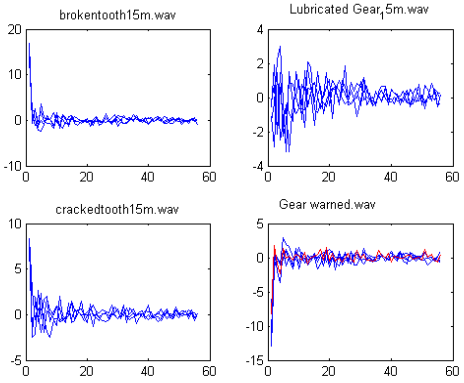


Figure 9: Classified Weared Gear Fault

4.3.2.2 Crack On One Tooth

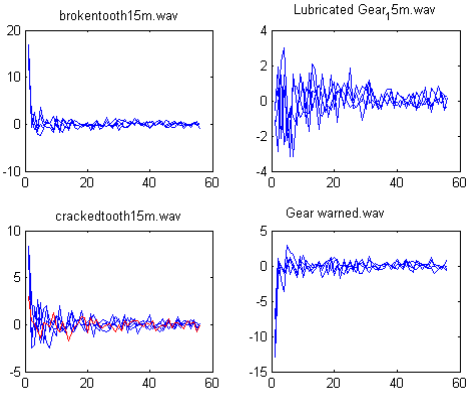


Figure 10: Classified Cracked tooth Gear Fault

4.3.2.3 One Tooth Broken Or Missed

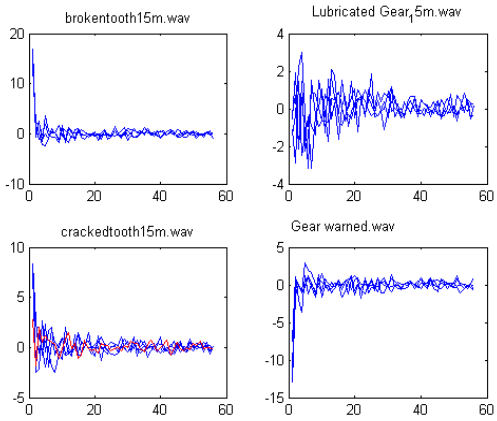


Figure 11: Classified Broken or missed tooth Gear Fault

Following table shows the success of ISO DATA Algorithm in classifying various signatures of gear fault.

Type of signal	% of success
Good , Lubricated gear	100
Warned gear	100
Gear with crack one tooth cracked	100
Gear with on e tooth broken	Failed

Table2: Success Of ISODATA

5.0 CONCLUSION

The ISODATA algorithm classifies all types of faults. On some occasions it fails to distinguish between the faults. This happens if the fault feature vectors are in close vicinity. e.g. it fails to distinguish between the signal of broken tooth & cracked tooth as depicted in fig 11 above. This is the limitation of this algorithm & it could be overcame by searching better vibration signal processing method that keep feature vectors apart .

REFERENCES

[1]. J.T. Tou, P. C. Gonzalez, 1974, *Pattern Recognition Principles*, Wesly Publication Company

[2]. Neural Network toolbox, Matlab version 6.5

[3]. Erik Olsson, Peter Funk, Ning Xiong, Fault Diagnosis in Industry Using Sensor Readings & Case Based Resoning,Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, Volume 15 , Issue 1 (January 2004) Pages: 41 - 46 ,2004

[4]. Martin, Detection of Gear Damage by Statistical Vibration Analysis, IMechE,Journal of Mechanical Engineering, Pages 395-401, 1992,

[5]. Patil Atul & Gawade S, Acoustic Intensity Analysis Of Gearbox & Fault Diagnosis of Gear Teeth By CBM; Proceedings of International Conference On Advances in Machine Design & Industry Automation, January 10-12,2007.

BIJIT - BVICAM's International Journal of Information Technology

Paper Structure and Formatting Guidelines for Authors

BIJIT is a peer reviewed refereed bi-annual research journal having **ISSN 0973-5658**, being published since 2009, in both, Hard Copy as well as Soft copy. Two issues; **January – June** and **July – December**, are published every year. The journal intends to disseminate original scientific research and knowledge in the field of, primarily, Computer Science and Information Technology and, generally, all interdisciplinary streams of Engineering Sciences. **Original** and **unpublished** research papers, based on theoretical or experimental works, are published in BIJIT. We publish two types of issues; **Regular Issues** and **Theme Based Special Issues.** Announcement regarding special issues is made from time to time, and once an issue is announced to be a Theme Based Special Issue, Regular Issue for that period will not be published.

Papers for Regular Issues of BIJIT can be submitted, round the year. After the detailed review process, when a paper is finally accepted, the decision regarding the issue in which the paper will be published, will be taken by the Editorial Board; and the author will be intimated accordingly. However, for Theme Based Special Issues, **time bound Special Call for Papers** will be announced and the same will be applicable for that specific issue only.

Submission of a paper implies that the work described has not been published previously (except in the form of an abstract or academic thesis) and is not under consideration for publication elsewhere. The submission should be approved by all the authors of the paper. If a paper is finally accepted, the authorities, where the work had been carried out, shall be responsible for not publishing the work elsewhere in the same form. *Paper, once submitted for consideration in BIJIT, cannot be withdrawn unless the same is finally rejected*.

1. Paper Submission

Authors will be required to submit, MS-Word compatible (.doc, .docx), papers electronically *after logging in at our portal and accessing the submit paper link*, available at http://www.bvicam.ac.in/bijit/SubmitPaper.asp. Once the paper is uploaded successfully, our automated Paper Submission System assigns a Unique Paper ID, acknowledges it on the screen and also sends an acknowledgement email to the author at her / his registered email ID. Consequent upon this, the authors can check the status of their papers at the portal itself, in the Member Area, after login, and can also submit revised paper, based on the review remarks, from member area itself. The authors must quote / refer the paper ID in all future correspondences. Kindly note that we do not accept E-Mailic submission. To understand the detailed step by step procedure for submitting a paper, click at http://www.bvicam.ac.in/BIJIT/guidelines.asp.

2. Paper Structure and Format

While preparing and formatting papers, authors must confirm to the under-mentioned MS-Word (.doc, .docx) format:-

- The total length of the paper, including references and appendices, must not exceed **six (06) Letter Size pages**. It should be typed on one-side with double column, single-line spacing, 10 font size, Times New Roman, in MS Word.
- The Top Margin should be 1", Bottom 1", Left 0.6", and Right 0.6". Page layout should be portrait with 0.5 Header and Footer margins. Select the option for different Headers and Footers for Odd and Even pages and different for First page in Layout (under Page Setup menu option of MS Word). Authors are not supposed to write anything in the footer.
- The title should appear in single column on the first page in 14 Font size, below which the name of the author(s), in bold, should be provided centrally aligned in 12 font size. The affiliations of all the authors and their E-mail IDs should be provided in the footer section of the first column, as shown in the template.
- To avoid unnecessary errors, the authors are strongly advised to use the "spell-check" and "grammar-check" functions of the word processor.
- The complete template has been prepared, which can be used for paper structuring and formatting, and is available at http://www.bvicam.ac.in/BIJIT/Downloads/Template_For_Full_Paper_BIJIT.pdf.
- The structure of the paper should be based on the following details:-

Essential Title Page Information

- **Title:** Title should be Concise and informative. Avoid abbreviations and formulae to the extent possible.
- **Authors' Names** and **Affiliations:** Present the authors' affiliation addresses (where the actual work was done) in the footer section of the first column. Indicate all affiliations with a lower-case superscript letter immediately after the author's name

and in front of the appropriate address. Provide the full postal address of each affiliation, including the country name and e-mail address of each author.

- **Corresponding Author:** Clearly indicate who will handle correspondence at all stages of refereeing and publication. Ensure that phone numbers (with country and area code) are provided, in addition to the e-mail address and the complete postal address.

Abstract

A concise abstract not exceeding 200 words is required. The abstract should state briefly the purpose of the research, the principal results and major conclusions. References and non-standard or uncommon abbreviations should be avoided. As a last paragraph of the abstract, 05 to 10 Index Terms, in alphabetic order, under the heading Index Terms ***(Index Terms - …….)*** must be provided.

NOMENCLATURE

Define all the abbreviations that are used in the paper and present a list of abbreviations with their definition in Nomenclature section. Ensure consistency of abbreviations throughout the article. Do not use any abbreviation in the paper, which has not been defined and listed in Nomenclature section.

Subdivision - numbered sections

Divide paper into numbered Sections as 1, 2, 3, ….. and its heading should be written in CAPITAL LETTERS, bold faced. The subsections should be numbered as 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. and its heading should be written in Title Case, bold faced and should appear in separate line. The Abstract, Nomenclature, Appendix, Acknowledgement and References will not be included in section numbering. In fact, section numbering will start from Introduction and will continue till Conclusion. All headings of sections and subsections should be left aligned.

INTRODUCTION

State the objectives of the work and provide an adequate background, with a detailed literature survey or a summary of the results.

Theory/Calculation

A Theory Section should extend, not repeat the information discussed in Introduction. In contrast, a Calculation Section represents a practical development from a theoretical basis.

RESULT

Results should be clear and concise.

DISCUSSION

This section should explore the importance of the results of the work, not repeat them. A combined Results and Discussion section is often appropriate.

CONCLUSION AND FUTURE SCOPE

The main conclusions of the study may be presented in a short Conclusion Section. In this section, the author(s) should also briefly discuss the limitations of the research and Future Scope for improvement.

APPENDIX

If there are multiple appendices, they should be identified as A, B, etc. Formulae and equations in appendices should be given separate numbering: Eq. (A.1), Eq. (A.2), etc.; in a subsequent appendix, Eq. (B.1) and so on. Similar nomenclature should be followed for tables and figures: Table A.1; Fig. A.1, etc.

ACKNOWLEDGEMENT

If desired, authors may provide acknowledgements at the end of the article, before the references. The organizations / individuals who provided help during the research (e.g. providing language help, writing assistance, proof reading the article, sponsoring the research, etc.) may be acknowledged here.

REFERENCES

Citation in text

Please ensure that every reference cited in the text is also present in the reference list (and vice versa). The references in the reference list should follow the standard IEEE reference style of the journal and citation of a reference.

Web references

As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list, as well.

Reference style

Text: Indicate references by number(s) in square brackets in line with the text. The actual authors can be referred to, but the reference number(s) must always be given. Example: '..... as demonstrated [3,6]. Barnaby and Jones [8] obtained a different result ....'

List: Number the references (numbers in square brackets) in the list, according to the order in which they appear in the text.

Two sample examples, for writing reference list, are given hereunder:-

Reference to a journal publication:

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread-spectrum watermarking for multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 64 – 69, December 1997.

Reference to a book:

[2] J. G. Proakis and D. G. Manolakis – Digital Signal Processing – Principles, Algorithms and Applications; Third Edition; Prentice Hall of India, 2003.

Mathematical Formulae

Present formulae using Equation editor in the line of normal text. Number consecutively any equations that have to be referred in the text

Captions and Numbering for Figure and Tables

Ensure that each figure / table has been numbered and captioned. Supply captions separately, *not attached to the figure*. A caption should comprise a brief title and a description of the illustration. Figures and tables should be numbered separately, but consecutively in accordance with their appearance in the text.

3. Style for Illustrations

All line drawings, images, photos, figures, etc. will be published in black and white, in Hard Copy of BIJIT. Authors will need to ensure that the letters, lines, etc. will remain legible, even after reducing the line drawings, images, photos, figures, etc. to a two-column width, as much as 4:1 from the original. However, in Soft Copy of the journal, line drawings, images, photos, figures, etc. may be published in colour, if requested. For this, authors will need to submit two types of Camera Ready Copy (CRC), after final acceptance of their paper, one for Hard Copy (compatible to black and white printing) and another for Soft Copy (compatible to colour printing).

4. **Referees**

Please submit, with the paper, the names, addresses, contact numbers and e-mail addresses of three potential referees. Note that the editor has sole right to decide whether or not the suggested reviewers are to be used.

5. Copy Right

Copyright of all accepted papers will belong to BIJIT and the author(s) must affirm that accepted Papers for publication in **BIJIT** must not be re-published elsewhere without the written consent of the editor. To comply with this policy, authors will be required to submit a signed copy of Copyright Transfer Form, available at http://bvicam.ac.in/bijit/Downloads/BIJIT-Copyright-Agreement.pdf, after acceptance of their paper, before the same is published.

6. Final Proof of the Paper

One set of page proofs (as PDF files) will be sent by e-mail to the corresponding author or a link will be provided in the e-mail so that the authors can download the files themselves. These PDF proofs can be annotated; for this you need to download Adobe Reader version 7 (or higher) available free from http://get.adobe.com/reader. If authors do not wish to use the PDF annotations function, they may list the corrections and return them to BIJIT in an e-mail. Please list corrections quoting line number. If, for any reason, this is not possible, then mark the corrections and any other comments on a printout of the proof and then scan the pages having corrections and e-mail them back, within 05 days. Please use this proof only for checking the typesetting, editing, completeness and correctness of the text, tables and figures. Significant changes to the paper that has been accepted for publication will not be considered at this stage without prior permission. It is important to ensure that all corrections are sent back to us in one communication: please check carefully before replying, as inclusion of any subsequent corrections cannot be guaranteed. Proofreading is solely authors' responsibility. Note that BIJIT will proceed with the publication of paper, if no response is received within 05 days.

BVICAM'S International Journal of Information Technology (BIJIT)

(A Biannual Publication; ISSN 0973 - 5658)

Subscription Rates

Category	I Year		3 Years	
	India	**Abroad**	**India**	**Abroad**
Companies	Rs. 400	US $ 45	Rs. 1000	US $ 120
Institution	Rs. 300	US $ 40	Rs. 750	US $ 100
Individuals	Rs. 250	US $ 30	Rs. 600	US $ 075
Students	Rs. 150	US $ 25	Rs. 375	US $ 050
Single Copy	Rs. 250	US $ 25	-	-

Subscription Order Form

Please find attached herewith Demand Draft No._____ dated _____

For Rs._____ drawn on _____Bank in favor of **Director, "Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi"** for a period of 01 Year / 03 Years

Subscription Details

Name and Designation _____

Organization _____

Mailing Address _____

_____ PIN/ZIP _____

Phone (with STD/ISD Code)_____FAX_____

E-Mail (in Capital Letters)_____

Date: **Signature**

Place: (with official seal)

Filled in Subscription Order Form along with the required Demand Draft should be sent to the following address:-

Prof. M. N. Hoda
Chief Editor – BIJIT,
Director, Bharati Vidyapeeth's
Institute of Computer Applications & Management
A-4, Paschim Vihar, Rohtak Road, New Delhi-110063 (INDIA).
Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at: www.bvicam.ac.in

Bharati Vidyapeeth's
Institute of Computer
Applications & Management
A-4, Paschim Vihar, Rohtak Road, New Delhi-63

Jointly with

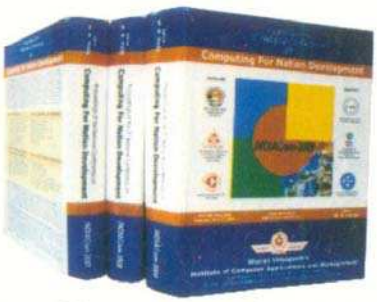
GURU GOBIND SINGH
INDRAPRASTHA UNIVERSITY

IEEE COMPUTER SOCIETY
Delhi Section

The Institution of
Electronics and Telecommunication
Engineers (IETE), Delhi Centre

ISTE, Delhi Section

BVP CSI Students'
Branch, New Delhi



(Copies of the proceedings of past *INDIACom*s)

Correspondence
All correspondences related to the conference may be sent to the address:

Prof. M. N. Hoda
Chief Convener, *INDIACom* - **2011**
Director, Bharati Vidyapeeth's
Institute of Computer Applications and Management
A-4, Paschim Vihar, Metro Station Paschim Vihar (E),
Rohtak Road, New Delhi-63
Tel.: 011-25275055, TeleFax: 011-25255056, 09212022066 (Mobile)
E-Mails: conference@bvicam.ac.in, indiacom2011@gmail.com
For further details, visit us at: http://www.bvicam.ac.in

INDIACom-2011

5th National Conference on

Computing For Nation Development

(10th-11th March, 2011)

Information and communication technologies play a dramatic impact on effectiveness, efficiency, growth and development in various areas such as education, health-care & modernization. Foreseeing the importance and impact of the above and encouraged by the resounding success met with the previous Four editions of the INDIACom(s); INDIACom-2010, INDIACom-2009, INDIACom–2008 and INDIACom– 2007; we hereby announce **INDIACom – 2011**, which aims to develop a strategic plan for balanced growth of our economy through IT in critical areas like E-Governance, E-Commerce, Disaster Management, GIS, Nano-Technology, Intellectual Property Rights, AI and Expert Systems, Networking, Software Engineering and other Emerging Technologies.

The **INDIACom - 2011** intends to bring eminent academicians, scientists, researchers, industrialists, technocrats, government representatives, social visionaries and experts from all strata of society, under one roof, to explore the new horizons of innovative technology to identify opportunities using IT and defining the path forward. This new path will envision to eliminate isolation, discourage redundant efforts and promote scientific progress aimed to accelerate India's overall growth to prominence on the International front. The INDIACom - 2011 will feature regular paper presentation sessions, invited talks, key note addresses, panel discussions and poster exhibitions. More than 700 papers have been received from over 950 authors from all over country. Eminent speakers from Academia, Industry and Government have already confirmed to participate in INDIACom -2011. Our previous editions of Pre-Conference Proceedings have widely been appreciated from all academic circles. As earlier, this year also, we will publish both soft and hard copies of the Pre-Conference Proceedings with ISSN and ISBN serials. Maximum benefits from this event can be derived by participating in huge number and together making it a grand success. Further details are available at our website **www.bvicam.ac.in/indiacom**.

Registration Fee :

	Early Bird on or before 18th December, 2010 (in Rs.)		After 18th December, 2010 (in Rs.)		Spot Registration (only in Cash)	
Category of Delegates/ Authors	***CSI/IETE IEEE/ISTE Members**	**General**	***CSI/IETE IEEE/ISTE Members**	**General**	***CSI/IETE IEEE/ISTE Members**	**General**
Students# (Delegates only)	600.00	800.00	800.00	1000.00	1000.00	1200.00
Teachers/Research Scholars	2200.00	2500.00	2700.00	3000.00	3000.00	3500.00
Industry	3000.00	3500.00	3500.00	4000.00	4000.00	4500.00

10% discount will be given on three or more registrations from one organization in General Category only.

* Members must mention their membership number of CSI / IETE /IEEE/ISTE.

#***Authors can not register under Students Category.*** Bonafide students as on 31st January, 2011, must submit the Bonafide certificate from their Institute / College /Department. Students will not be given the hard copy of the Conference Proceeding. Soft copy will only be given.

The registration fee includes tea, lunch, conference kit and the Soft and hard copies of Conference Proceedings along with other printed materials related to the conference. The payment can be made in Cash in the office of the Institute or by Demand Draft in favour of **Director, Bharati Vidyapeeth's Institute of Computer Applications and Management,** payable at **New Delhi.**

NSC-2011

4th National Students' Convention on

Computing For Nation Development

(12th March, 2011)

Bharati Vidyapeeth's CSI Students' Branch is also organizing 4th National Students' Convention (NSC-2011) on the same theme of **"Computing For Nation Development"** on 12th March, 2011. Further details are available in the attached brochure and also on the website **www.bvicam.ac.in/nsc**