A Study On Routing for Secure Adhoc Wireless Network

S C Dutta[1] , Sudha Singh[2] and D K Singh[3]
[1]Assistant Professor, Department of Computer Science and Engineering,
BIT Sindri, Dhanbad-828123, India.
dutta_subhash@yahoo.com
[3]Professor, Department of Electrocics and communication Engineering,
National Institute of Technology, Patna-800005, India.
dksingh@nitp.ac.in, dksingh_bit@yahoo.com
[2]Professor, Department of Computer Engineering, MGM college of Engg. and Technology,
Kamothe, Navi Mumbai-410209, India.
sudha_2k6@yahoo.com.

Abstract : An ad hoc mobile network is a collection of dynamic nodes and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The network topology in such a network may keep changing randomly. To provide secure communication within such network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption. In this paper we are examining issues with implementations and giving a way to solutions. Through proposed work we have eliminated the weaknesses of Ad Hoc wireless network mentioned in Dutta et. al. [5]. Also through proposed work, there is a highest level of secure communication.

Keywords : MANET , Security , Time to Travel , Time to Live , Issues in Routing for Ad Hoc Wireless Protocol.

I. INTRODUCTION

An ad hoc wireless network consists of a set of nodes that are connected by wireless links. The network topology in such a network may keep changing randomly. Routing protocols that find a path to be followed by data packets from a source node to destination node used in traditional wired networks cannot be directly applied in adhoc wireless networks due to their highly dynamic topology, absence of established infrastructure for centralized administration, bandwidth constraint wireless links and resource constrained nodes [14].

Due to these inherent complexities of such network intrusion detection is an especially complicated process and make it difficult to transfer existing wired intrusion detection approaches to the such environment. Issues in designing a routing protocol for Ad Hoc Wireless networks are given below[14]:

(1) Mobility Management: In the ad-hoc network environment, mobile hosts can move unrestricted from place to place. Mobility management handles the storage, maintenance and retrieval of the mobile node position information.

(2) Bandwidth Management: In wireless network, the radio band is limited and hence the data rates it can offer are much less than what a wired network can offer. This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

(3) Resource constraints: Two essential and limited resources that form the major constraints for the nodes in an Ad hoc wireless network are battery life and processing power. Devices used in ad hoc wireless networks in most cases require portability and hence they also have size and weight constraints along with the restrictions on power source.

(4) Security: The mobile nodes in MANETs are highly susceptible to malicious damage. Security issues are important in MANETs to prevent potential attacks, threats and system vulnerabilities.

(5) Error-prone shared broadcast radio channel: The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless network. The wireless links have time varying characteristics in terms of link capacity and link error probability. This requires that the ad hoc wireless network routing protocol interacts with the MAC layer to find alternate routes through battery quality links.

(6) Hidden and exposed terminal problems: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the receiver. Collision occurs when both nodes transmit packets at the same time without knowing

about the transmission of each other. The exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node to another node.

II. Literature review and features of proposed system

The security protocol designed for ad hoc wireless network faces various challenges like mobility of nodes, resource constraints, error prone channel state and hidden and exposed terminal problems [14]. Solutions for hidden and exposed terminal problem [7] include medium access collision avoidance [12], medium access collision avoidance for wireless [1], floor acquisition multiple access and dual busy tone multiple access [3]. The destination sequenced distance vector routing protocol [17] is a table driven algorithm based on a classical Bellman-ford routing mechanism. Wireless routing protocol[15], Cluster-Head Gateway switch routing protocol which uses hierarchical network topology[2] and source tree adaptive routing protocol[8] are table driven routing protocol. On demand routing protocol execute the path finding process and exchange routing information only when a path is required by a node to communicate with the destination. Dynamic source routing protocol[11], ad hoc on demand distance vector[18] routing protocol, temporary ordered routing algorithm[16], location added routing[13], associatively based routing[21], signal stability based adaptive routing protocol[4] and flow oriented routing protocol[20] are on demand routing protocols. In hybrid routing protocols, each node maintains the network topology information upto m hops. Core extraction distributed ad hoc routing protocol [19], zone routing protocol [9], zone based hierarchical link state routing protocol [10] are hybrid protocols. Characteristics of an ideal routing protocol for ad hoc wireless networks are given in section 7.2.6 of book [14] Proposed work is the extension of Dutta et. al. [5,6] to provide power aware ad hoc on demand distance vector routing protocol for secure communication.

Its features are given below:

(1) It is adaptive to frequent topology changes caused by the mobility of nodes.

(2) It provides minimum connection setup time.

(3) It is localized.

(4) It is loop free and free from stale routes.

(5) The number of packet collision is minimum because the communication between nodes is very much limited and communication takes place only when it is required.

(6) It always takes optimal routes with respect to time. The convergence is quick if signal is strong. The convergence is slow if signal is weak or when there is no signal.

(7) It optimally uses the system resources.

(8) It provides quality of service with secure communication.

III. Proposed system for complete solution and its limitations

To proceed ahead, we suppose that the transmission range of a node is k feet (It is normally 30 feet for getting strong signal with mobile nodes in ad hoc wireless network, but variations are there). It means k is the diameter of the circle with node as a center. We are taking this circle as a zone.

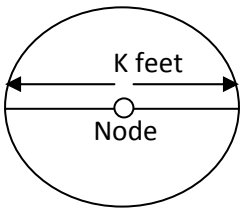

Fig. 1. Zone

Since nodes are dynamic, sometimes signal is strong and sometimes it is weak. It also happens that any nodes may lose connections for few milliseconds. Practically we found that signals are strong in more than 98% of chances if distance between two nodes is less than k/2. Signals are strong or weak if distance between two nodes is more than k/2 and less than (k-k/4). There will be weak signal or no signal if node will be in the range of (k-k/4) and (k+k/4).

In one zone, there may be more than one number of nodes with its own zone. Within zone, signal strength will be high. On the boundary, it will be poor.

In one particular network, suppose there are m numbers of zones available. And in a zone there are n numbers of nodes. We have Network=$\bigcup_{i=1}^{m}\{Z_i = \bigcup_{j=1}^{n} N_j\}$.

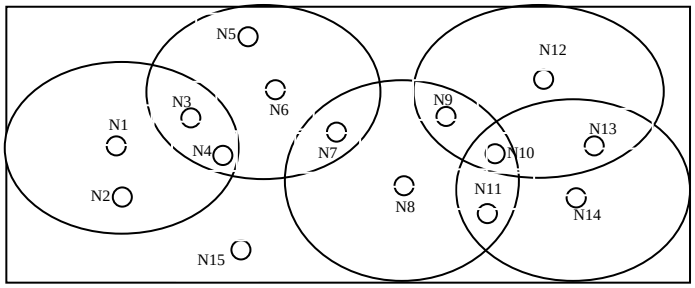

Fig. 2: Network with zones and nodes

A network with n number of nodes can have at most {n*(n-1)/2} number of links. For secure connection nodes have to connect through service set identifier (SSID) and password. Password should be different for each and every node. SSID should have the combination of digits (0-9), alphabets (A-Z; a-z) and special characters. We are distinguishing every wireless network with SSID (known as network group). An ad hoc wireless network can have any number of nodes and any number of network groups. It means one node may have on more than one network group. We avoided such situation because it causes excessive energy drain and consequent reduction of lifetime in battery operated devices.

We study the two cases of Ad Hoc Wireless network. These cases provide higher level programming language.

CASE (A) : Nodes are connected but some or all are unknown to each other.

Nodes are unknown to each other. They are secretly connected in a network group through secret netID and password. If N_i is sending message to N_j, it means Ni and Nj are on the same network group. They may be on different zones but within strong transmission range. Each node will make friend from the neighboring nodes. If they wish to increase the friend list, they can. Note that node will select friendship request only if both are connected by strong signals. There may be some nodes which are in strong transmission range of one or more zones but are not interested in network group. For example, in fig. 2 , N1, N3, N6, N7, N8, N9, N10, N12, N13 and N14 are on the same network group while N2,N4,N5,N11 and N15 are not in this group. Since friends have shared the secret key, rule is that, you will not disclose it to more than f persons. Limitations are there on the number of zones and total number of friends due to limited energy resources, scalability and quality of services. Maximum number of friends and zones will be f and z respectively for a network group. Now they can have the secure communication in their network group.

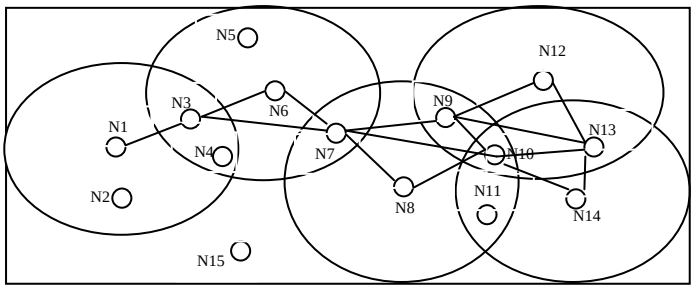

Fig. 3: Network with zones, nodes and link.

At each node, routing information table or path matrix is initialized. For example see table 1. Any node will have routing information up to zone q only (because of limited power resources of a node). If number of nodes are high then it will have routing information up to neighbors only. This table will get updated after every 2 minutes. If a node wants to send message, then it will update the path matrix through beacons before sending message.

Connection between nodes is represented by the time (in milliseconds) spent in traveling from Ni to Nj. It may change time to time and get updated for any node when it receives any message from other nodes. Also, entries in the table can be of three different colors- green, orange and red. Conditions are applied on distance because some or all the nodes are mobile.

Green:	if signal is strong AND for each pair of nodes (Ni, Nj) of path from source to destination, distance(Ni, Nj)<=k/2
Orange	if for any pair of nodes (Ni, Nj), (distance(Ni,Nj)>k/2 and distance(Ni,Nj)<k) and (signal is there).
Red	if there is no signal.

Table 1: Path matrix

	N1	N3	N6	N7	N8	N9	N10	N12	N13	N14
N1	-	3	6	5	7	9	8	11	13	14
N3	3	-	4	3	4	7	10	15	14	15
N6	6	4	-	4	7	6	9	14	12	15
N7	5	3	4	-	4	3	3	12	15	11
N8	7	4	7	4	-	3	7	11	13	13
N9	9	7	6	3	3	-	5	5	4	5
N10	8	10	9	3	7	5	-	4	3	3
N12	11	15	14	12	11	5	4	-	4	7
N13	13	14	12	15	13	4	3	4	-	3
N14	14	15	15	11	13	5	3	7	3	-

First of all users can see that how many nodes are on the network group. Ni can communicate neighboring nodes without any delay. Suppose N1 want to communicate with N8 directly, it will send message containing destination ID, time to live. All the nodes will ignore and pass the message except destination. The node N8 may receive duplicate packets, which it will ignore.

With the help of this table, user can find the shortest path (with respect to time) from one node to another and can send data through that path. Data will automatically get deleted after time to live period.

If all the fields are green in the path from source to destination, then time to live will be the shortest time (t) to reach from source to destination. If some or all the fields are orange in the path from source to destination, then time to live will be the (shortest time (t)+t/2) to reach from source to destination. If any of the fields are red in the path from source to destination, then time to live will be the (2*shortest time (t)+t/2) to reach from source to destination

If a node receives three or more independent packets from a node Nr within t1 milliseconds, then this act will considered as malicious behavior. That node will stop entertaining node Nr and consider this node as malicious node.

This method gives no guarantee that packet will be indeed received by destination or not. If packet will get lost due to any reason then destination will not receive this packet and it will be lost permanently. Destination will get to know in next message that something is missing, then it can request for previous message.

The drawback of this type of network group is the new group member. We cannot pass important or secret information over here.

CASE (B) : Nodes are connected but known to each other

All nodes are known to each other. They have to work on an adhoc wireless network. For security, each node will have unique secret code(SCD).All the nodes have the information about themselves only, even if they are known to each other. If they try to disclose SCD to other, then that node will be attacked by malicious node. Rest nodes get unaffected. They are secretly connected in a network group through secret netID and unique password. This network group has fixed number of nodes. Initial setting of network can be done by flooding a message on the network with time to live(TTL),previous node, time to travel(TTT). Information will get appended in this message in each pass and each node will initialize and update its path matrix with TTT between nodes using above message till TTL expires. Entries in this matrix can be done as

(i). Null(-), if source and destination is same;

(ii). 0, if there is no strong path between Ni and Nj;

(iii). x, if time required to travel from source to destination is x milliseconds; where is x is any real number.

Since we are considering only strong signals and making their entries in the table. This table will get updated after every 2 minutes. If a node wants to send message, then it will update the path matrix/table through beacons before sending message.

The entries in the table will be done as follows:

(i). Entries of strongly connected will be in green while entries of weakly connected will be in orange and entries of not connected will be in red color.

(ii). Initialization of path matrix is explained in case 1. An example of table after initialization in case 2 will be a table like table1 with orange entries will be zero. We try to update the table at regular time interval and before sending a message.

(iii). We will send message secretly with the method used by Dutta and singh [5,6]. We can easily understand above example (in CASE 1) in view of case 2. All the examples and simulation work, given in Dutta et. al. [5], will be applicable over here with little modification in simulation parameters given in later section of this paper . We are taking another example in which node is requested for updation of path matrix and shortest way to reach to destination N15.

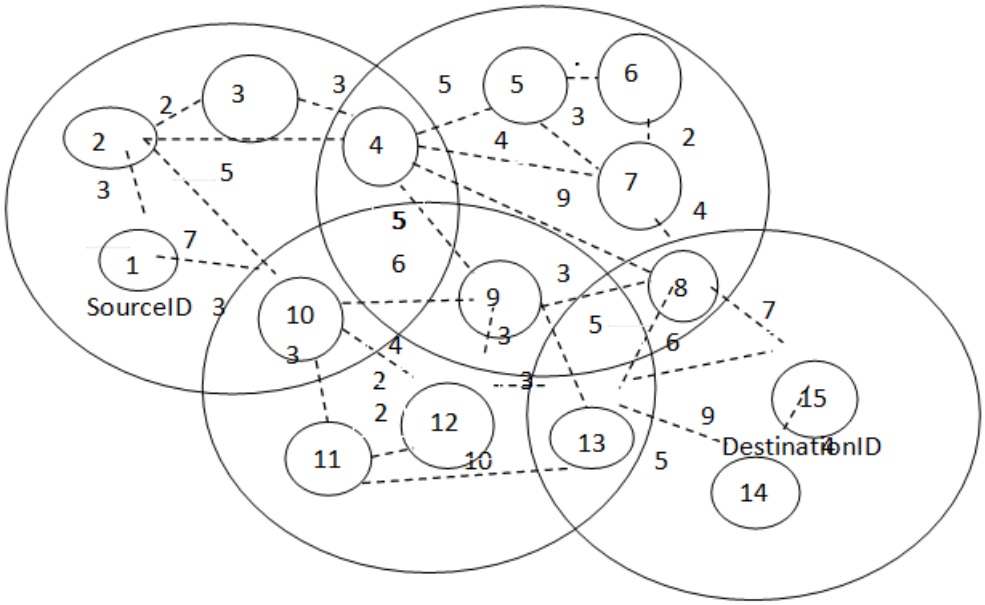

Fig. 4: An example of network group with zones, nodes and strong link.

Route establishment in this network group is explained through the following table:

Table 2: To calculate shortest path.

Node number	Predecessor node	Path with time	Flag	Shortest time
15	15	15(0)	15	0
14	15	15-14(4)	15-4	4
13	14	15-14-13(9), 15-13(9)	15-13	9
12	13	15-14-13-12(12), 15-13-12(12)	15-13-12	12
11	12	15-13-12-11(14), 15-13-11(19)	15-13-12-11	14
10	12	15-13-12-11-10(17), 15-13-12-10(16)	15-13-12-10	16
9	10	15-13-12-10-9(22), 15-13-9(14), 15-13-12-9(15)	15-13-9	14
8	9	15-8(7), 15-13-9-8(17)	15-8	7
7	8	15-8-7(11)	15-8-7	11
6	7	15-8-7-6(13)	15-8-7-6	13
5	6	15-8-7-6-5(14), 15-8-7-5(14)	15-8-7-5	14
4	5	15-8-7-5-4(19), 15-8-7-4(15), 15-8-4(16), 15-8-9-4(15)	15-8-7-4	15
3	4	15-8-7-4-3(18)	15-8-7-4-3	18
2	3	15-8-7-4-2(20), 15-8-7-4-3-2(20) 15-8-9-4-2(20), 15-8-9-10-2(23) 15-13-12-10-2(23)	15-8-7-4-2	20
1	2	15-13-12-10-1(19), 15-13-12-11-10-1(20) 15-13-9-10-1(23), 15-8-9-10-1(19)	15-8-9-10-1	19

(iv). If there are more than three messages within k milliseconds from outside group or any big interference, then be silent for t milliseconds and check the network. if messages are still coming then wait for 2*t ms and again check. This checking will continue iteratively till we get clearer surroundings. Using this method, we can able to minimize the effect of jamming/flooding attack and denial of service type of attack.

(v). Using this method, battery power of node will not get exhaust and will be saved. Also due to the rest time period of the battery and recovery capacity effect, longer lifetimes of the battery can be achieved. The recovery capacity effect is concerned with the recovery of charges under idle conditions. By increasing the idle time, one may be able to completely utilize the theoretical capacity of the cell.

IV. Simulation and Result

Proposed routing protocol is already successfully tested in real scenarios with following parameters: Number of nodes : 20 (different types of nodes),

Area : 50m x 50m, Node speed: 0-5m/s,

Transmission range: 50m, we are getting strong signal up to 25-35m.

To evaluate the effectiveness, stability, security and robustness of proposed protocol for higher number of nodes, higher distance and more node speed, simulation (ns-2) is used.

The critical simulation parameters used in simulation are given below:

Simulation area: 2000m x 2000m, 2000m x 1000m, 2000m x 500m

Total nodes: 200, 150, 100

Source nodes: 30, 50

Node speed: 0-1 m/s, 5m/s, 10m/s, 20m/s

Pause time: 0 sec, 30sec, 50 sec, 70sec, 120 sec.

Transmission range: 100m, 150m

Packet size: 512 bits, 1024 bits,

Packet generation rate:4 packets per seconds

Mobility model: random

Different number of nodes, area sizes, node speed, pause time and transmission range are taken to verify and analyze the performance of network group. The final results are the average of the results obtained with variation of the parameters. Final results are given below:

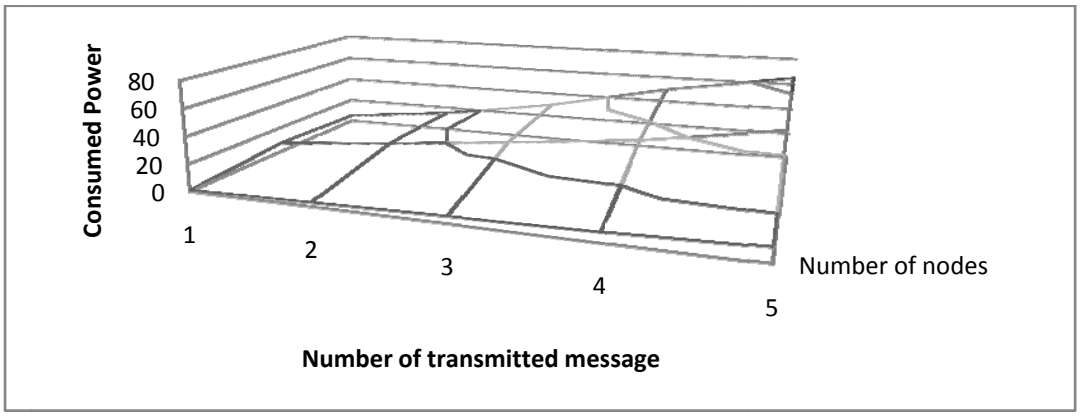

Fig. 4: Power Consumption

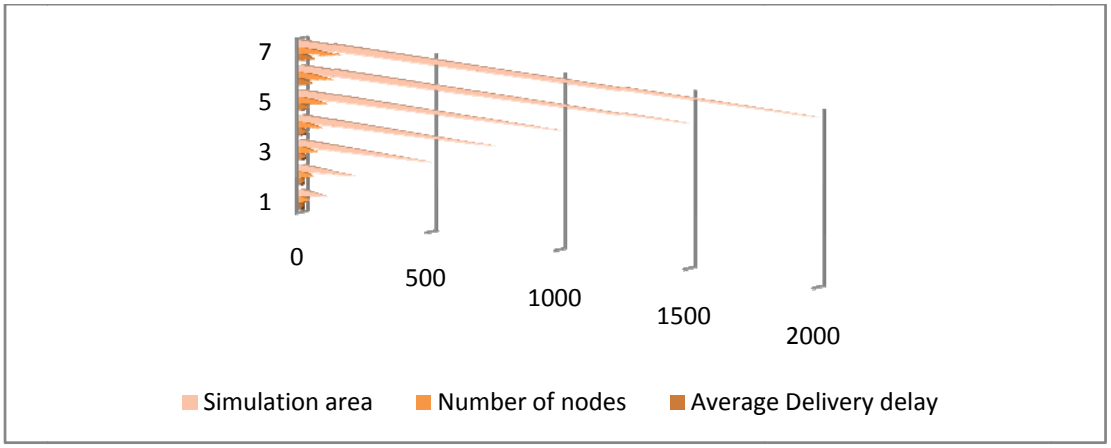

Fig. 5: Packet delivery delay

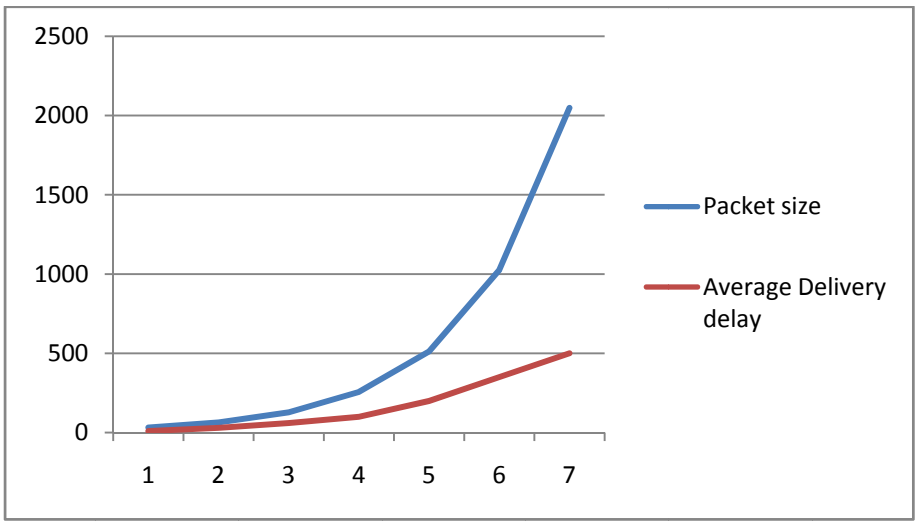

Fig. 6: Packet delivery delay with respect to packet size (it is observed that more the packet size, more secure will be the message)

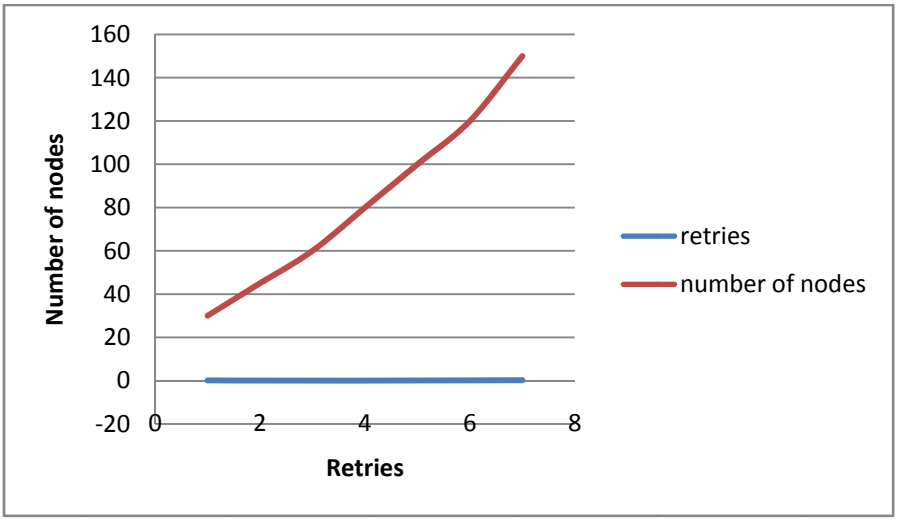

Fig. 7: Latency if path signal is strong

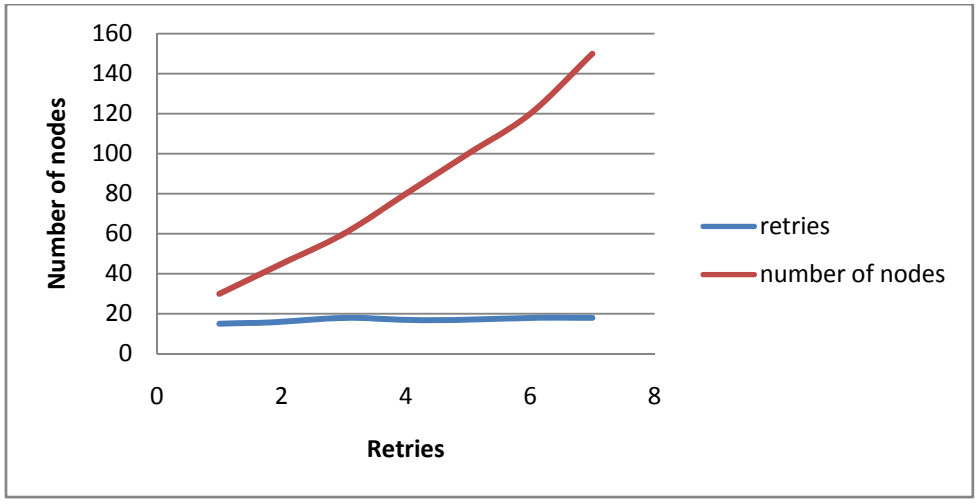

Fig. 8: Latency if path signal is combination of strong and weak

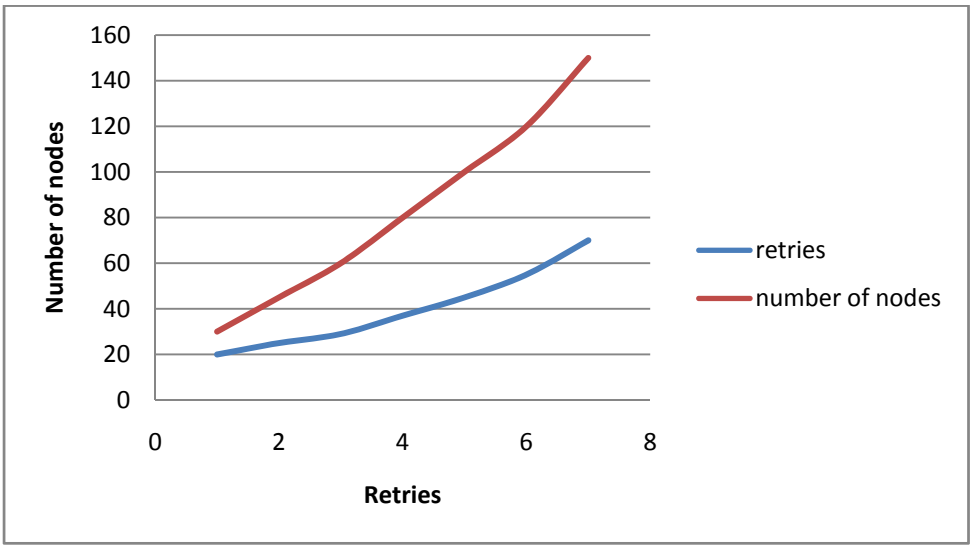

Fig. 9: Latency if path signal is weak or no signal

V. CONCLUSION AND FUTURE PROSPECTS

In this paper we have examined issues with implementations and given a way to solutions. Through proposed routing protocol we have eliminated the weaknesses of Ad Hoc wireless network like limited energy resources and information disclosure, Jamming etc mentioned in dutta et al [5]. Major threats have minimum or no effect in this system. All security services are applied over here. So there is a highest level of secure communication. Future prospects of this work is to increase the simulation parameters like area, nodes etc and examine individual effect of various factors of with respect to these parameters.

REFERENCES

[1] Bharghavan, V.,Demers A,Shenker S. and Zhang L.,"MACAW: A media access protocol for Wireless LANs", Proceedings of ACM SIGCOMM 1994,pp 212-225,1994.
[2] Chiang C. C., Wu H.K., Liu W. and Gerla M.,"Routing in clustered multihop mobile wireless networks with fading channel", Proceedings of IEEE SICON 1997, pp197-211,1997.
[3] Deng J. and Haas Z "Dual busy tone multiple access(DBTMA): A new medium access control for packet radio networks", Proceedings of ICUPC 1998, vol.1, pp 973-977,1998.
[4] Dube R, Rais C D, Wang, K. Y and Tripathi S. K., " Signal Stability based adaptive routing for adhoc mobile networks", IEEE personal communication magazine, pp36-45, 1997.
[5] Dutta S. C., Singh Sudha and Singh D. K. "Fully secured ad hoc wireless network by using on demand half full weighing matrix", under publication, 2014.
[6] Dutta S. C., Singh Sudha and Singh D. K. "Enhancement of Mobile Adhoc Network security using Improved RSA algorithm", proceedings of Springer 2015 , vol 1, pp 1027 – 1036., 2015.
[7] Fullmer C. L and Garcia-Luna-Aceves, "Solutions to hidden terminal problems in wireless network", Proceedings of ACM SIGCOMM 1997,pp 39-49,1997.
[8] Garcia-Luna-Aceves and Spohn, M.," Source tree routing in wireless networks", Proceedings of IEEE ICNP 1999, pp.273-282,1999.
[9] Haas Z. J. " The routing algorithm for the reconfigurable wireless networks", Proceedings of ICUPC 1997, vol.2, pp. 562-566, 1997.
[10] Joa-Ng M. and Lu I. T. " A peer to peer zone based two level link state routing for mobile adhoc networks", IEEE journal on Selected areas in communications, vol.17, no.8, pp. 1415-1425., 1999.

[11] Johnson D.B. and Maltz, D.A., " Dynamic source routing in Ad Hoc Wireless networks", Mobile computing, kluwer Academic publisher, vol.353, pp.153-181, 1996.
[12] Karn, P, "MACA-A new channel access method for packet radio",Proceedings of APRL/CRRL Amateur radio computer networking conference 1990, pp134-140,1990.
[13] Ko Y. and Vaidya N.H., "Location aided routing in mobile ad hoc networks", Proceedings of ACM MOBICOM 1998, pp. 66-75, 1998.
[14] Murthy C S Ram and Manoj B S," Adhoc wireless network architecture and protocols", Pearson Education Inc, 20th edition, 2014.
[15] Murthy S and Garcia-Luna-Aceves, "A efficient routing protocol for wireless networks", ACM mobile networks and Application journal, Special issue on routing in mobile communication networks, Vol.1, No. 2, pp183-197, 1996.
[16] Park V.D. and Corson M.S., " A highly adaptive Distributed routing algorithm for mobile wireless networks", Proceedings of IEEE INFOCOM 1997, pp.1405-1413, 1997.
[17] Perkins C.E. and Bhagwat, "Highly dynamic destination-sequenced Distance vector routing for mobile computers", Proceedings of ACM SIGCOMM 1994, pp 234-244, August 1994.
[18] Perkins C.E. and Royer E.M., " Ad hoc on demand distance vector routing", Proceedings of IEEE Workshop on Mobile computing systems applications, pp. 90-100, 1000
[19] Sinha P., Sivakumar R and Bharghavan V., "CEDAR: A core extraction Didtributed Ad hoc routing algorithm", IEEE journal on selected areas in communications, Vol.17, no.8, pp.1454-1466,1999.
[20] Su W and Gerla M, "IPv6 Flow Handoff in ad hoc wireless networks using mobility prediction", Proceedings of IEEE GLOBECOM 1999, pp271-275,1999.
[21] Toh C. K." Associativity based routing for Ad hoc mobile networks", Wireless personal communications, Vol.4, No. 2 pp.1-36, 1997

AUTHOR PROFILE

S C Dutta received his B. E Degree from Bangalore University (MS R IT) in the year 1993 and M. Tech Degree in Control Systems in 2009.He is working as Research Scholar in the area Mobile Ad Hoc Network, its applications, securities and Routing since 2011. He is presently working as Assistant Professor, in the department of Computer Science & Engg. In B I T Sindri since 2006. He is also heading the department of IT, in BI T Sindri since 2011. He has more than 10 research papers published in International / National Journals / International / National conferences of repute. His area of research area is MANET and its Security.

Sudha singh received her Ph. D degree from VBU, Hazaribag in the faculty of Engg. (Computer Science & Engg.) in 2009. Her current research intereset include Computer Networks, its Security and their applications, Application of Hadamard Matrices, MANET , Routing , Coding Theory, Cryptography. She has already published more than 29 research papers in International / National Journals / International / National conferences of repute. She has more than 10 years of teaching experience in her specialized area at different levels(B. Tech , M.Tech). She is presently supervising a number of M. Tech and Ph. D Research Scholars. She is presently working as professor and Head , Department of Computer Engineering, MGM college of Engg. and Technology, Kamothe, Navi Mumbai-410209.

D K Singh is presently working as Professor in the department of ECE in NIT Patna since September 2011. He is also working as DEAN (Academic) in NIT Patna . Previous to this (More than 20 years), he was working as Professor and heading the department of CSE, ECE and IT in BIT Sindri . He has published more than 45 papers in International / National Journals / International / National conferences of repute (TAYLOR and FRANSIS, ….). He is presently supervising a number of M. Tech and Ph. D Research Scholars. His current research intereset include Mobile Ad Hoc Networks, Routing , Swarm Intelligence based optimization, Routing, Coding Theory, Photonic Crystal Fibres.