ISSN No: - 2456- 2165

Improve Security For Mobile Adhoc Networks Using Genetic Zonal Routing Protocol

Gajanand Sharma
Associate Professor
Department of CEIT
Suresh Gyan Vihar University,Jaipur
Gajanan.sharma@gmail.com

Ashutosh Sharma
Suresh Gyan Vihar University
Jaipur
Sharmaashu121212@gmail.com

Dr. Dinesh Goyal
Professor
Department of CEIT
Suresh Gyan Vihar University,Jaipur
dinesh8dg@gmail.com

Abstract :- In Wireless Network , Mobile Adhoc Network is a special kind of Network. It is a group of many mobile nodes in which we does not require any big infrastructure. In a wireless Network, any attack can be apply easily as compare to the wire based communication because in wireless sensor network we have limited security. In this paper , our main aim is to increase Packet Delivery Ratio for the system along with low Delay. The simulation results is carried out by the 1000 mobile nodes by using network simulator. In the Base Paper , they are working for the ZONE Routing protocol for show the Packet Delivery ratio and End to End delay . In this Research , we improving the network performance by improve the Packet Delivery Ratio and by decrease the end to end delay from Genetic Zone Routing Protocol .

Keywords: *MANET, ZRP, security, mobility, route.*

I. INTRODUCTION

In the present time, Mobile Adhoc Network (MANET Mobile Network) is taking the big attention because it is self design , self maintenance and cooperated environment. In mobile Adhoc Network all the nodes are mobile nodes and the topology of the network are changing instantly. The MANET structure is showing in figure 1. In the Network PDAS and Laptop are using to Route the Data Packets. In MANET (Mobile Adhoc Network) all the mobile nodes will active and message will transmit for the destination by the multiple Hop[1]. Normally routers and end point are different in MANET[2]. It uses the wireless channel and asynchronous data transmission through the multiple-hop. The vital characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes. The QOS is enabled by end-nodes like E2E (End-to-End) delay, secure transmission of data throughput and packet-loss [2]-[3]. The potential MANET deployment is available in number of scenarios e.g. that in the situations where an infrastructure isn't the feasible one like the cyclone and disaster relief and so on. The MANETs is having potential of understanding Omni directional, ubiquitous, and free communication [3].

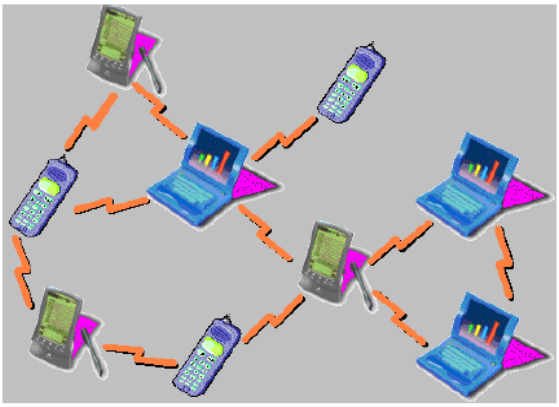


Fig 1. Structure of MANET.

All wireless (remote) channels may be accessible by both malicious as well as legitimate users. In particular environment, there's not any guarantee in which a route in between all two nodes can be free for a malicious users, that willn't fulfill with protocol employed. All malicious users try to harm a network operation.

The MANET is the self-configuring network of the mobile routers associated by wireless (remote) links that having no access point. Each mobile device in the network is independent. All mobile devices are having nature to move freely haphazardly and then organize them arbitrarily. The MANET nodes share the wireless (remote) medium as well as the network topology modifies dynamically and erratically. In the MANET, communication link breaking is extremely frequent, as the nodes are independent to move to everywhere. The nodes densities as well as the number of nodes are depending on entire applications in that we are utilizing MANET. The MANET raised number of applications such as Device Networks, Data Networks, WSN (Wireless Sensor Network and Tactical networks, and so on. With the number of applications, there're still some issues of design and then

ISSN No: - 2456- 2165

challenges to overcome. The essential objectives of mobile Ad Hoc Networking required expanding the mobility into realm autonomous, wireless domains and mobile, wherever the nodes set that may be gathered hosts and routers. They form infrastructure of network routing in Ad Hoc fashion. So many security vulnerabilities in the remote (wireless) environment, like MANET, it has been identified and then counter measures set were suggested as well. Whereas only some of them have given the guaranty, that is usually orthogonal to the challenge of critical security. By taking certain parameters into the concern, the main vision of mobile ad hoc networking is to support efficient and robust operation in the portable wireless networks by including the functionality of routing into the mobile nodes. These networks are having envisioned for dynamic, occasionally changing rapidly, random, multi hop topologies that are suitably collected of the relative wireless links bandwidth- constrained. The MANET is extremely vulnerable than the wired network because of all mobile nodes, threats are from network compromised nodes, restricted physical security, scalability, dynamic topology and deficiency of the centralized management. Only because of certain vulnerabilities, the MANET is largely prone to the malicious attacks.

II. RELATED WORK

The algorithm of secure routing in the wireless communication are concentrated on as well as suggested for the increment in the levels of security [4]. Where, certain algorithms cannot protect network from the attackers, who obtained the key data [5]. Reseracher *J.Li* [6] suggested the mechanism of general encryption key for the MANETs by using the DSR (Dynamic Source Routing). The drawback of particular model is which has dropped maximum packets even though the network had only some malicious users [7]. The AODV (Adhoc On-Demand Distance Vector) is utilized to give the reliable and secure data transmission on MANETs [8]. So many strategies had employed in order to detect non-cooperative nodes during data packets forwarding to destination [9]. In the [10], the authors trusted and discussed the established approach for communication in between mobile users. Communication happens depending on a watch dog. As well, trusted values are usually represented from '-1' to '+1'.

The attack of black hole is a typical service denial where the malicious node may attract entire packets by claiming falsely a fresh destination route and then absorb all of them without forwarding to destination [11]. The researcher Smith [12] tested the distance vector protocols routing security in the developed and general counter measures for the vulnerabilities by defending both routing updates and routing messages. They suggest the digital signature and sequence numbers for routing updates and messages and consisting the predecessor data in the routing updates.

III. ZONE ROUTING PROTOCOL

Particular model represents the safe communication in between mobile nodes. The data scenario of transmission is in between all two mobile-nodes are considered. Where the source desires to transmit entire data packets towards the destination, the source ensures that whether the source is communicating via cluster head with the real node. The service authentication uses the key management in order to recover a public key that is trusted by 3rd party destination identification. As well the similar method is used by the destination for source authentication. And after key management module execution, the session key is invoked; it's used by the both destination and source for the suitable communication confidentially. In particular way, entire crucial messages get transmitted to a destination.

The paths get maintained with the requirement of source. We utilize the sequence numbers in order to continue with up-to-date data. The information of routing has been updated by using RREQ (Route Request) packet. If source desires to communicate with the desired destination, for that it doesn't have route, then RREQ packet is broadcasted by it to a network. And after receiving, the RRE (Route Reply) packet is broadcasted by intermediate node. If RREQ packet has processed already, then it gets discarded. The module utilizes the ZRP (Zonal Routing Protocol). Every node actively restrains the possible set of routes with the region. Every knowledge area is studied by ZRP to enhance efficiency of network performance. DSDV also studied regarding nodes within area. In order to search routes for the that are out of area, the DSR is used there.

The ZRP (Zone Routing Protocol) was a 1st Protocol of Hybrid Routing [9] [11]. It is suggested to minimize the overhead control of the proactive routing protocol as well as to minimize the Reactive routing protocol latency. It's appropriate for entire networks with the diverse mobility patterns and large span. For every node the zone of routing gets defined independently. And within the zone of routing, the routes get available right away; but for outside of zone, the ZRP uses to route the discovery procedure. For every node, the separate zone of routing is defined. The zone of routing with the neighboring nodes; usually overlap with every different zone. Every zone of routing has the radius 'ρ' that expressed in the hops [9]. The zone comprises the nodes, those the source node distance is mostly the 'ρ' hops.

The Routing Zone comprises entire nodes excepting the node 'L', as it lies exterior of routing zone node 'A'. The Routing Zone is not considered as the physical distance, it gets defined in the hops. There're considerably the two distinct types of nodes for the ZRP routing zone [9]:

- Peripheral Nodes: In these nodes minimum distance to central node is equal to 'ρ' (zone radius). Here, the peripheral nodes are E, F,G,K,M.
- Interior Nodes : In these nodes minimum distance to central node is less than 'ρ' (zone radius). Here

ISSN No: - 2456- 2165

interior nodes are B, C, D, H, I, J.The node 'L' is outside the routing zone of the node 'A'.

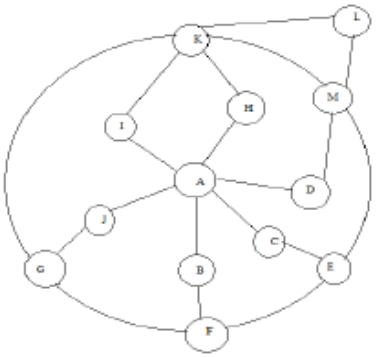


Fig 2. Routing Zone of Node A with Radius ρ=2 hop

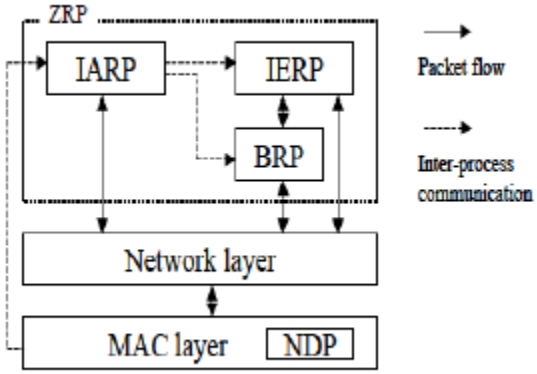


Fig 3. Architecture of ZRP

A source node sends the 'route request' to other peripheral nodes of the zone. The route request includes the address of source, the unique sequence number and the destination address. Every peripheral node verifies its destination local zone. If a destination isn't the local zone member, the RRP (Route Request Packet) get added with the peripheral node with an own address of it and further forwards entire packet to the peripheral nodes. If a destination with its local zone member, it transmits the route reply with the reverse path reverse to the source. A source node utilizes the path reserved in RRP (Route Reply Packet) in order to send the data packets to a destination. And by adjusting nodes transmission power, the nodes numbers in a routing zone may be regulated. The lowering of power minimizes the nodes number within the direct reach as well as vice-versa [10].

The ZRP utilizes all strategies that is Reactive and Proactive routing. The proactive strategy is utilized within the routing zone and the reactive strategy is utilized within the routing zones. The ZRP is referring to the local proactive routing element as the IARP (Intr A-zone Routing Protocol). The global element of reactive routing is considered as IARP (IntEr-zone Routing Protocol) [9].

The IARP keeps up routing data of nodes that are inside the zone of routing node. The route maintenance and route discovery is offered by the IERP. At the point when worldwide disclosure is required, if the topology of nearby zone is known, it can be utilized to minimize the traffic. Rather than the packet broadcasting, the ZRP utilizes the Border casting concept [10]. The packet service of border casting is given by the BRP (Border casting Resolution Protocol). The BRP [11] utilizes the extended routing zone map, given by the neighborhood IARP, to build Border cast trees beside that the query packets are co-ordinate. The BRP utilizes the extreme mechanism of query control components to guide route request far from network territories which have effectively covered by query [11].

IV. PROPOSED METHODOLOGY

The GZRP (Genetic Zone Routing Protocol) is the augmentation of ZRP (Zone Routing Protocol) is embracing the idea of GA (Genetic Algorithm). The GZRP is contemplated for its execution contrasted with ZRP in number of folds such as versatility of packet delivery and demonstrated with the enhanced results. The GZRP functions like the ZRP when the destination node is inside the zone of routing (or the routing table) of source node. The destination route is accessible in the table of routing of a source node that is created because of IARP. Notwithstanding, if a node destination isn't found in the source node routing table, it starts the process of route discovery by sending the RREQ (Route Request) packets with the assistance of the IERP. These packets of RREQ are casted border by the BRP. Each border node finds the destination node within the table of routing. At the point when the destination route is found, the RREP (Route Reply) packet is sent back to a source node.

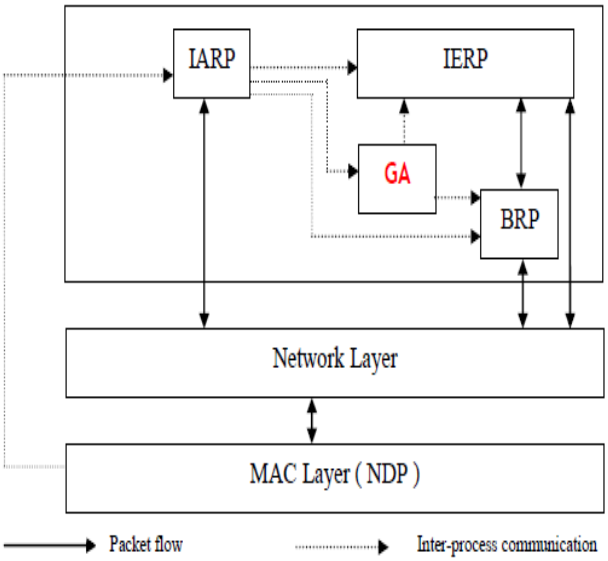
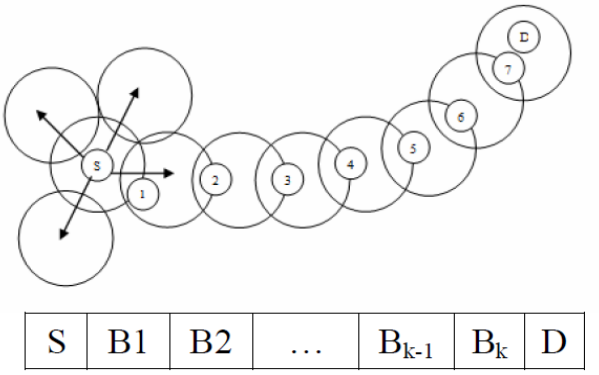


Fig. 4. Architecture of Genetic Zone Routing Protocol

ISSN No: - 2456- 2165

The GZRP utilizes the GA at every border node and creates the conceivable path that might be problematic (sub-optimal) or ideal (optimal). These alternative ways get stored in border nodes for the two essential reasons: (a) They may use certain routes as the existing node fails or routes fails (fault tolerance) (b) They may dispense the packets on various alternative routes to minimize the congestion and too to adjust the system (load balancing). At every border node, rather than RREQ packets border casting on the necessary primary path, they may be the border casted on number of routes. Despite the fact that, GA develops numerous conceivable alternative ways, we make the utilization of pre-determined number of option that are either ideal (optimal) or close ideal (near optimal).



S	B1	B2	…	B_{k-1}	B_k	D

Fig. 5. Encoding method of border nodes

While by utilizing the GA for figuring the shortest ever paths, it incorporates the procedure such as mutation and crossover to create new routes. The GA utilized with the GZRP is clarified briefly below:

The initial phase in the GA is to encrypt the chromosomes components. The GA chromosome comprises of positive integer sequence which speak to the nodes IDs through that passes a route path. Every chromosome locus presents the node order (demonstrated by locus gene) in the path of routing. The first locus gene is constantly saved for a source node. It never requires more than the nodes of N number in the network system to form the path of routing. Subsequently, the greatest size of the length of chromosome may be 'N'. The chromosome (routing path) predetermines the issue by posting up node IDs from the source node to the destination node depended on topological data (that given by IARP) of system.

The population is generated with the individual group (chromosomes) generated randomly. Certain chromosomes in a population get estimated. In the research paper, a routing is concerned with the border nodes. Therefore, the length of the route gets minimized in size as compared to the normal on demand networks. In this way, it lessen the size of population of network too. The work measured with the size of population twice the nodes number in the network. After that, the literature recommended which the random method of initialization may be adopted to produce the greatest population.

The GA fitness function is generally having the function objective which needs to be optimized. In SP-routing issue the fitness function is noticeable due to the amounts of SP computation for searching the minimal cost path. The selection operator is considered to enhance the average population quality by providing chromosomes of high-quality, the better chance to copy into next generation. The suggested technique of GA utilizes the selection of roulette wheel that is widely used.

The crossover tests this solution to conclude that present one is better or not. Physically the problem of crossover SP routing performs the exchanging role at every partial route of the two selected chromosomes in which the off-spring created by a crossover representation at only single route. It dictates the single-point crossover selection as the scheme of good candidate for suggested GA. One general route joins a source node with the intermediate node, as well as the another partial route joins an intermediate to destination node.

In this proposed scheme, the two chromosomes selected for the crossover that should have the minimum one common gene or node except the destination and source nodes, but there's no need in which they located the similar locus. The crossover doesn't base on the node position in the routing paths. It's suitable which loops get formed that during the crossover. The simple counter measure should be taken in particular ground. The penalty and repair operations are the ggeneral counter measures.

The populace experiences the transformation by a genuine change or flipping of certain node of candidate chromosomes, by keeping the local optima away. Generally, it creates an option of partial route from mutation node to the destination node in suggested GA. One of nodes, associated specifically to the node at alternative partial route, is picked randomly as the primary node of an alternative partial route. As said before, the crossover may create the infeasible chromosomes which damage the requirements of producing loops in the routing paths. It must be noticed that none of the chromosomes of the underlying population or after the transformation is infeasible on the grounds that when once a node is picked, it is rejected from the hopeful nodes shaping rest of path or route.

V. RESULTS

In the Results session , we are showing the results for Packet Delivery Ratio and End to End Delay for the Video Transmission by MANET network. Figure 5 is showing the video frame . We will divide the video into frames before transmit it .

Figure 6 is showing the Packet Delivery Ratio for the Zone Routing Protocol . As we can see from the figure the Packet delivery ratio is not in constant , increasing or decreasing form

ISSN No: - 2456- 2165

and in the last packet Delivery ratio are getting at 0. So we have to improve the packet delivery ratio.

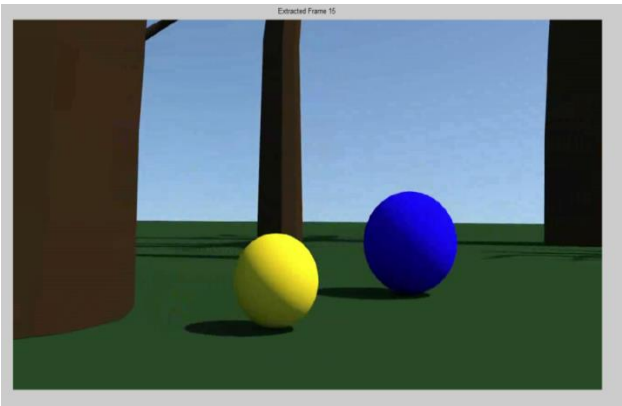


Fig 5. Video Frames

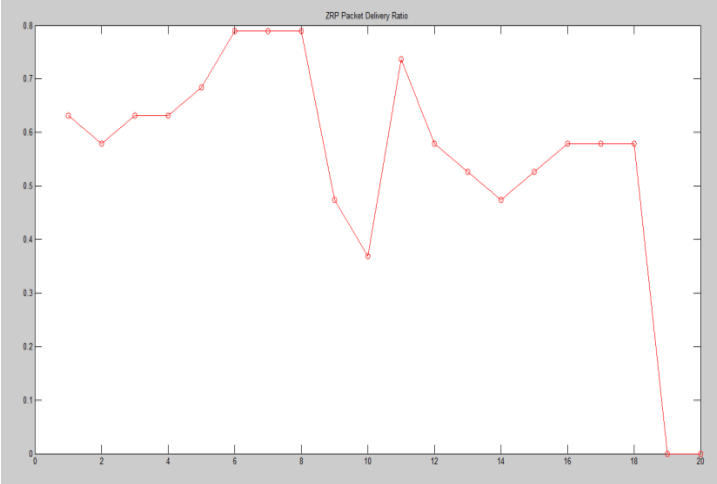


Fig 6. Packet Delivery Ratio for ZONE Routing Protocol

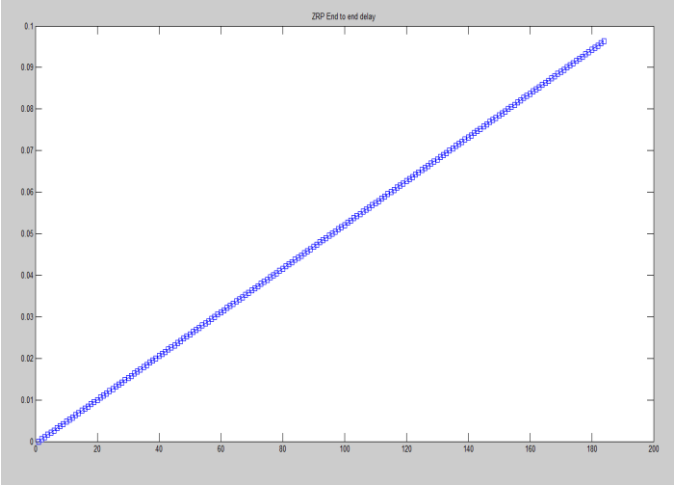


Fig 7. End to End Delay for the Zone Routing Protocol

Figure 7 is showing the End to End Delay for the Zone Routing Protocol. End to End delay is showing for the delay in transmission of the packets. As the number of packets get increase at the network the end to end delay get introduce and it get increase as we can see from the figure 7.

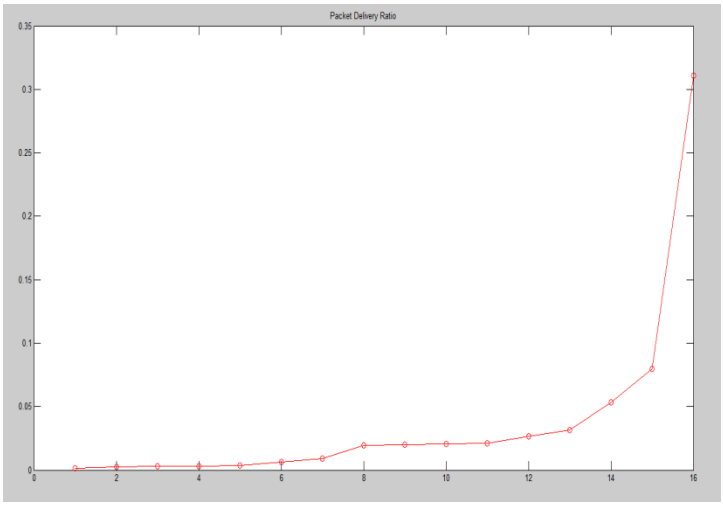


Fig 8. Packet Delivery Ratio for the Genetic Zone Routing Protocol

As we can see from the Figure 8 the Packet Delivery ratio is getting increase continues as the number of nodes get increase for Genetic Zone Routing Protocol. In Figure 9 , we show the comparison for the End to End delay as we can see form the figure , end to end is low as compare to Zone routing protocol end to end delay.

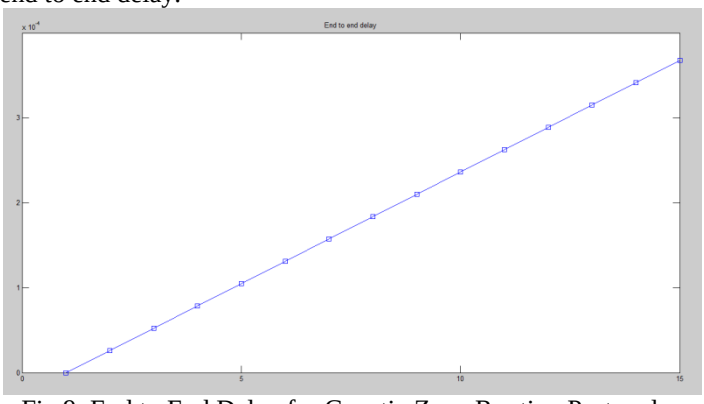


Fig 9. End to End Delay for Genetic Zone Routing Protocol

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

There are various MANET protocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes. It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks. In this model, we have discussed the security issues for MANETs. It focuses on the security architecture. Since, every attack has own characteristics. One of the limitations of this model is that it works based on the assumption of malicious nodes, which do not work as a group. It may be happened in a real situation.

ISSN No: - 2456- 2165

In ZRP, the packets are forwarded with full power without considering the node's position inside the zone. According to Inverse Square Law, the received power is inversely proportional to square of the distance between the nodes. The node could waste power if the distance between the sender and the receiver node is less. As the distance between the sender and border nodes increases, the zone area will also increase that means the radio coverage of the sender node will not be able to reach the border nodes in the zone. Due to this reason, the sender node will increase the no. of broadcasts to find the border nodes in the zone, that will enhances bandwidth utilization.

In this Research ,we apply Genetic Zone Routing Protocol for increase the packet delivery ratio and decrease the end to end delay. As we can see from the results session the packet delivery ratio is getting increasing for Genetic Zone Routing Protocol as compare to the Zone routing protocol and end to end delay is decreasing for the Genetic Zone Routing Protocol as compare to Zone routing protocol end to end delay.

B. Future Scope

The proposed protocol presented in this thesis considers that, the Genetic Zone Routing Protocol are safe within the network and are free from any kind of attacks caused either by external advisory or internal compromised nodes. A possible extension of the work may include employing additional feature to SZRP so that it can handle a scenario where the trusted certification authorities are compromised or attacked. Additionally we have assumed that, the Neighborhood Discovery Protocol (NDP) is implemented as a MAC layer protocol. But in some special cases the MAC layer does not include an implementation of NDP. In such situations the proposed protocol may be modified to provide the functionality of NDP at IP layer.

REFERENCES

[1]. H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, "Security in Mobile Adhoc Networks: Challenges and Solutions", *IEEE Wireless Communications*, Vol. 11, pp. 38-47(2004).
[2]. A. Perrig et al., "The TESLA Broadcast Authentication Protocol", *RSA Crypto Bytes*, Vol. 5, No. 2, p. 2-3(2002).
[3]. C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Adhoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 2, No. 3, pp. 257-269(2003).
[4]. Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester " An Overview of Mobile
ad hoc Netwroks: Applications & Challenges" .
[5]. K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02,2002.
[6]. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.
[7]. Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.
[8]. B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBECOM '06.
[9]. Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Workshop on Real-World Wireless Sensor Networks, June 20–21, 2005.
[10]. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, Vol. 24, No. 2, Feb. 2006.
[11]. HaoYang, Haiyun & Fan Ye — Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.
[12]. Buttyan, L., and Hubaux, J. P. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*: Special Issue on Mobile Ad Hoc Networks, **8**(5), 2003.
[13]. S. Corson and J. Macker, "RFC 2501 - Mobile Ad Hoc Networking (MANET): Routing Protocol Pe", Network Working Group, Request for Comments: 2501, University of Maryland, Naval Research Laboratory, JAN 1999.
[14]. Ad hoc Networking, C.E. Perkins, Addison Wesley, Jan. 2001.
[15]. C-K Toh, "Future Application Scenarios for MANET-Based Intelligent Transportation Systems", Proc. of Future Gen. Comms and Networking (FGCN 2007) - Vol. 2, p. 414-417.
[16]. Shiv Rama Murthi and Prasad " Adhoc Wireless network" page no. 249-252, First edition, PHI, 2004
[17]. R. Ramanathan and J. Redi, "A Brief Overview of ad hoc networks: challenges and Directions," IEEE Commun. Mag., vol. 40, no. 5, May. 2002.
[18]. Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, **1**(1), 2003, pp. 13–64.
[19]. M. Grossglauser and D. Tse,"Mobility increases the capacity of ad hoc wireless networks", IEEE/ACM Transactions on Networking, Vol. 10, No. 4, August 2002.
[20]. Gajanand Sharma, Amit Gupta, Dinesh Goyal, "Analysis & Design of Visual Cryptography using Moving Image" in International Journal of Information and communication Technology Research (ISSN: 2223 – 4985) Volume 03– Issue no 12, Nov.-Dec. 2013.
[21]. Manish Kumar Jha, Mr. Gajanand Sharma & Mr. Ravi Shankar Sharma,"Performance Evaluation of Quality of Service in Proposed Routing Protocol DS-AODV" in "International Journal of Digital Application & Contemporary research (ISSN: 2319-4863) Volume 02– Issue no 11, June 2014.
[22]. Nikhil Gupta , Gajanand Sharma , Ravi Shanker Sharma,"A Comparative Study of ANFIS Membership Function to Predict ERP User Satisfaction using ANN and MLRA" in International Journal of Computer Applications (ISSN: 0975 – 8887) Volume 105– Issue no 05, Nov. 2014.

[23]. Sunil Yadav & Gajanand Sharma ,"Improvisation Of Data Mining Techniques In Cancer Site Among Various Patients Using Market Basket Analysis Algorithm" in BEST: International Journal of Management, Information Technology and Engineering (ISSN: 2348-0513) Volume 3 Issue no 10, Oct. 2015.
[24]. Rinki Kumari , Gajanand Sharma, Akhilesh Pandey, "An Intellectual System For Human Personality Identification Using Soft Computing" in BEST: International Journal of Advanced Technology in Engineering and Science (ISSN: 2348-7550) Volume 3 Issue no 10, Oct. 2015.
[25]. Bertil Jeppsson "Ai-Controlled Life In Role-Playing Games" in International Journal of Computer Informatics & Technological Engineering (ISSN: 2348-8557) Volume 2 Issue no 11, Nov. 2015.
[26]. Manish Poonia, Gajanand Sharma, "Danger Theory Based Model to Prevent Sleep Deprivation Attacks in MANET's" in International Journal of Emerging Research in Management &Technology (ISSN: 2278-9359) Volume 4 Issue no 12, Dec. 2015.