www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9 September 2014 Page No. 7979-7985

Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks (MANETS)

Dimple Saharan

CSE deptt. MVV College of Engineering,
Jagadhri, Haryana,India
email:RSsaharan.4@gmail.com

Abstract: In the past few years mobile ad hoc networks (MANETs) have been emerged as the networks for next generation wireless networks. MANETs networks does not require an underlying infrastructure and have dynamically changing network topology. Due to high dynamism and mobility these networks are more vulnerable to attacks. The network performance might be improved if the network is clustered by grouping together nodes that are in close proximity. The primary goal is to enhance the performance of the network and to improve the durability of the nodes and hence the network life time. In this paper the effect of Wormhole attack is analyzed on AODV routing protocol in MANET and a prevention mechanism is presented to secure the network.

Keywords: MANETS, AODV, Wormhole Attack**.**

1. Introduction

Mobile ad hoc networks are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure. Unlike cellular networks, MANETs establishes multi-hop wireless links among mobile nodes. The routing, path maintenance and resource management are done in distributed manner in which all the mobile nodes coordinate to enable communication among them.

A Mobile Adhoc Networks (MANET) is an autonomous collection of mobile nodes and there is no fixed infrastructure, so it is more vulnerable to attack and the problems related to the routing and security. Security is a primary concern in almost all the application scenarios and in order to provide the secure communication between the mobile nodes. The ad-hoc networks are more vulnerable to security attacks due to the lack of limited physical protection of broadcast medium. In such scenarios **Authentication** is one of the most remarkable security aspects in any system because all the remaining attributes (i.e. integrity, confidentiality, availability etc) depends completely on it. Secondly, efficient resource usage and utilization of the available limited amount of energy in deploying the network in the most efficient way is one of the greatest challenges faced by ad-hoc networks. The network performance might be improved if the network is clustered more proficiently by grouping together nodes that are in close proximity via efficient **Clustering** scheme. Thirdly, the radio links in MANETs are opportunistic because of the restricted bandwidth between the nodes thus **Load balancing** is of vital importance in such networks. Due to inherent properties of MANETs, providing a robust solution these issues is a challenging task. [1]

The research problem is how to provide security protection to the network. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control. The attacker doesn't allow the packet to arrive at real destination. In addition, the attacker produces some packets and sends them in the network to consume the bandwidth and create the bottleneck in the network. One of these attacks is Wormhole Attack that has an important and dangerous effect on Mobile Adhoc networks and cause problems in the network. This attack effect is analyzed on AODV routing protocol in MANET and a prevention mechanism is presented to secure the network.

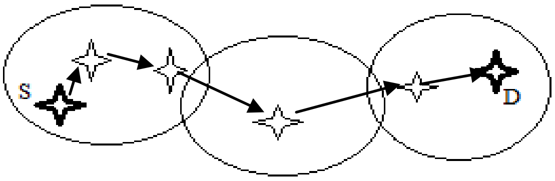

Figure 1 Multi hoping mechanism

MANET nodes behave as a router and as well as perform the computations. Source to destination packet forwarding is attempted using multi-hoping mechanism. The packet or the task takes various hops so as to reach the destination as shown in Figure 1. In CH(Cluster Head) formation, CH participates in all communication via and within the cluster boundaries. In that case, CH may face the bottleneck problem because the CH becomes the head of the system which may be responsible for most of the tasks and as nodes in MANETs are equipped with low battery, low computation, low bandwidth, self configuring features. In this scenario, load balancing is the critical issue for CH in terms of its performance and quality of services. Here a new algorithm is introduced which is recursive and efficient to select the neighbor potential nodes, which assist the CH and agree to share the load if CH is overloaded/ overburdened. The main objective of this work is to enhance the pursuit of the network and to increase the lifetime of the network nodes and proportionally the network's lifetime.

ALBOANs: Adaptive Load Balancer Optimized Adhoc Networks Algorithm is proposed to balance the load in MANETs, this algorithm is designed for packet forwarding so as to balance the load and also it enhances the quality and performance of network. The proposed algorithm selects the best node for load balancing with respect to battery life and processing power of node. It also tries to improve the durability of network.

In order to work with ***ALBOANs,*** some parameters or some pre-arrangements we need to follow is cluster formation. Second come Alboan_PHAROS_CALL which includes beapharos_request message that is used to send request to start the communication as shown in Figure 2 and beapharos_reply message that is used for acknowledgement that means that a particular node is ready to communicate as shown in Figure 3. The next parameter is CHmain_tab as shown in Figure 4 that is maintained by a commencer of the network and a CH maintenance table (CHmain_tab) is made on the basis of information received from pharos_reply packets and manage the CH nodes information in the table in the descending order on the basis of qualifying parameters. For every communication, the nodes may have battery life left (BLL) more than TTL (time to live assumed to be 50%) will be only considered else will be rejected or the communication will continue for next node in the CHmain_tab. To balance the load, check the processing power of the clusterhead, if the power consumption (PPC) is more than β (tolerance level, assumed to be 80%), then the CH will make a call to the nodes in the CHmain_tab so as to forward the packet. If this power consumption doesn't exceed the tolerance level then the CH itself will manage the work load.

Source IPaddress (4 bytes)	**Destination IP address** (port id) (4 bytes)	**IR1 + IR2** (4 bytes)

Figure 2 beapharos_request packet

Source IP address (port id) / (4 bytes)	**Destination IP address** (4 bytes)	**Processing power** (2 bytes)	**Battery life** (2 bytes)

Figure 3 beapharos_reply packet

Cluster Ids	**Nodes with port id**	**CH selected**

Figure 4 Format of CHmain_tab

The proposed work is about to prevent the mobile Adhoc network from the wormhole attack. In this research we are presenting the complete work with AODV protocol. The proposed work is about to prevent the mobile Adhoc network from the wormhole attack. This paper proposes a way to detect the wormhole node and to prevent the wormhole attack by encrypting the packet at each levels by sharing the Secret Key with the neighboring nodes and ensuring secured delivery via decrypting the packet at the neighbor node and matching the distributed Secret Key in MANET in AODV protocol environment.

2. Ad Hoc OnDemand Distance Vector Routing (AODV)

The AODV routing protocol is designed for adhoc mobile networks and it can handle unicast routing and as well as multicast routing [2, 3, 4]. This protocol has the advantageous features of both DSR and DSDV algorithms and this protocol is an example of On-demand routing protocol which means the routes will be created only when there is a demand and also it maintains the routes only as long as they are needed. Creating and maintaining the routes in the network only when they are needed/demand makes this AODV protocol very useful and also a good algorithm for mobile ad hoc networks (MANET) [5]. All the nodes in the network have routing tables of their own and they also maintain sequence numbers in order to avoid looping problems [5]. If a source node wants to send some data to a destination node and if it doesn't have a route to the destination at that time then the source node broadcasts a route request (RREQ) packet throughout the network [2, 6]. The nodes will reply with a RREP if either the destination node or the intermediate node which is on the way to find the destination node. A node which receives the PREQ will send a reply (RREP) only if it is either the destination or if it is a path/route to the destination with a corresponding sequence number and only when that number is greater than or equal to the number which contains the RREQ [2]. In cases like this the nodes will unicasts a RREP to the source, otherwise; the nodes will rebroadcast the RREQ. The nodes will discard the RREQ and do not forward them if they have been processed those already. And the RREP will set up forward pointers to the destination by propagating back to the source nodes [2, 7, 8] When the source node receives the RREP, it records the latest sequence number to the requested destination and this process is called as Forward Path setup [9]. The intermediate nodes that receives another RREP after they had propagated the previous RREP towards the source, it then checks and compares the new destination sequence number of the new RREP with the previous RREP. These intermediate nodes updates their routing information and propagates a new RREP only when,

1. The destination sequence number is greater or
2. The new sequence number is same but the hop count is small or

It will just skip the new RREP. This process ensures that this algorithm is not making any loops and only the most effective is chosen [5]. If the data packets keep travelling from one node to another node along a certain path only then the route remains active otherwise the links will timeout and then be deleted from the routing tables of the intermediate nodes. In situations like where the links break while the route is being active then the node upstream of the link break generates a route error (RERR) to the source node to inform that it is not reachable to the destination(s).

After the source node receives this (RERR) message, then even if the source node still needs the route then it will reinitiate the route discovery to that destination [4, 10].

Route Discovery Mechanism in AODV: If the source node “A” wants to initiate communication with destination node “E” as shown in the Figure 4.1 ,then it will make a connection between itself and the destination and will generate a route request message (RREQ). This message is then forwarded to the neighboring nodes, and the neighboring nodes will forward this control message to their neighboring nodes. This process of finding destination node continues until the destination node is located itself or the node that has the fresh route to the destination. Once an intermediate node with enough fresh routes is located or destination node is located, they generate the route reply message (RREP) and send it back to the source node. When RREP reaches back to the source node, a route or the path is established between the source node “A” and destination node “E”. Once the route is established between “A” and “E”, node “A” and “E” can communicate with each other. Figure 5 depicts the exchange of control messages between source node and destination node.

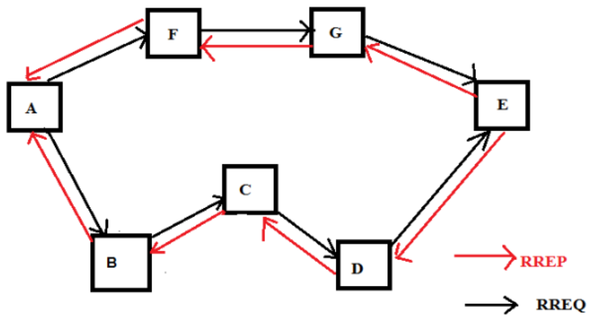

Figure 5 Route Discovery Mechanisms

Route Maintenance Mechanism: When there is a link down or a link breakage between destinations that causes one or more than one links unreachable from the source node or neighbor’s nodes, then the RERR message is generated by the node and sent to the source node. If there is a route from “A” to “E” via “D”, and if there is a link breakage “D” and “E”, then the node “E” will generate and send the RERR message to the source node “A” informing the source node that there is a route error. The scheme is as shown in the Figure 6.

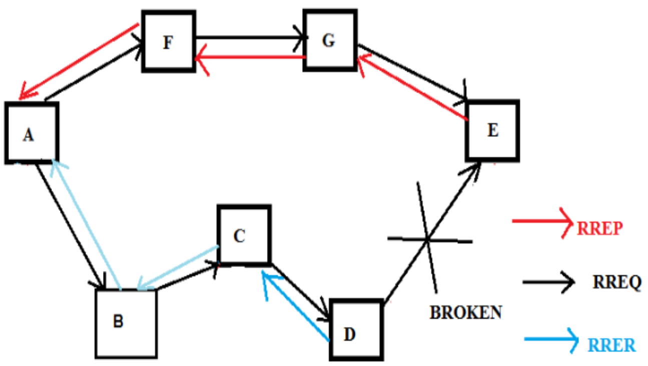

Figure 6 Route Error Message

3. WORMHOLE ATTACK

In this type of attacks, the attacker interrupts the usual flow of routing packets. This attack can be done with one node or two or more nodes. But generally, two or more attackers are connected via a link called “wormhole link”. The two malicious nodes in the network are located in the way that one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing. They intercepts the packets at one end and replay them at the other end using private high speed network. The attacker tunnels the request packet RREQ directly to the destination node, without increasing the hop count value and thereby, prevents any other path from being discovered. Or it makes the tunneled packet arrives faster and with better metric value.

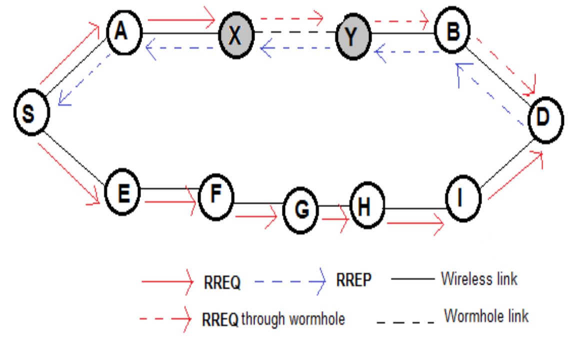

Figure 7 Wormhole Attack

Wormhole attack associates two remote malicious nodes shown as X and Y in Figure 7 which are attached via a wormhole link and target to attack the source node S. S broadcasts RREQ to find the route between source S and destination node D. Now, the neighbors of S, A, and E will also broadcast the RREQ to their neighbors. Now, when the malicious node X receives RREQ forwarded by A, it tunnels the RREQ by the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to the destination D via B. Thus, RREQ is forwarded via S-A-X-Y-B-D. And the other RREQ packet is also forwarded through the path S-E-F-G-H-I-D. However, RREQ via X and Y reaches fast to D, as X and Y are connected via a high speed bus. Therefore, destination D discards all the RREQ packets that reach later and choose the path D-B-A-S to send an RREP packet to the source node S. As a result, S chooses the route via X and Y to send data that to destination D.

4. METHODOLOGY

The proposed work is about the prevention of the network from the wormhole attack. In this work, a mechanism is presented to secure the communication between source and destination. As the node has to start the communication, it first starts with the neighbor discovery from the neighbor list. It first generates the "Hello" message and encrypts it using the secret key. The encryption technique is used to prevent the network from the wormhole attack. As the neighboring node receives this message, the node will decrypt it using the same secret key and send the acknowledgement back to the sender. If the node is not authentic, it will remove its entry from the neighbor list. After the neighbor discovery if sends the RREQ to its immediate neighbors from the neighbors list to have the route to the destination. As the RREQ reaches the destination, it will generate a RREP message and unicast it to the source node.

The packet format of the HELLO packet, RREQ and RREP message is:

HELLO (Source , Destination , Source Hash , Dest Sequence , Secret Key)

RREQ (Source, Destination, Source Hash, Encrypt [Secret Key], Secret Key of Src)

RREP (Source , Destination, Source Hash, Encrypt [Secret Key], Secret Key of Src)

To check the authentication of the node, it will also check the response time of the node. If the response time is greater than the threshold then also it excludes the node from the list. The complete process is repeated node by node till the destination node is achieved.

5. SIMULATION ENVIORNMENT

The basic parameters of the proposed approach are presented in Table 1 respective to the simulation environment. The approach is implemented with NS2 simulator and the xgraph is used as the tool for the analysis.

Table 1: Simulation Parameters

PARAMETER	VALUE
Traffic Type	TCP , UDP
Number of Nodes	36
Area Covered	800 X 800
Speed of the Node's	1,2 m/s
Simulation Time	25 sec
Routing Approaches	AODV
Nodes Initial Energy	0.5 watts
Mobility Type	Critical Mobility
Threshold Energy of Node's	1.4231E-12

The mobile Adhoc network of 36 nodes is constructed in the NS2 with the boundary area of 800m X 800m with the use of Tcl script. The nodes are mobile with the initial energy, speed and threshold energy as shown in the table. AODV routing protocol is used here as the protocol for the analysis.

SIMULATION ANALYSIS

Simulation scenario when there is no wormhole attack:

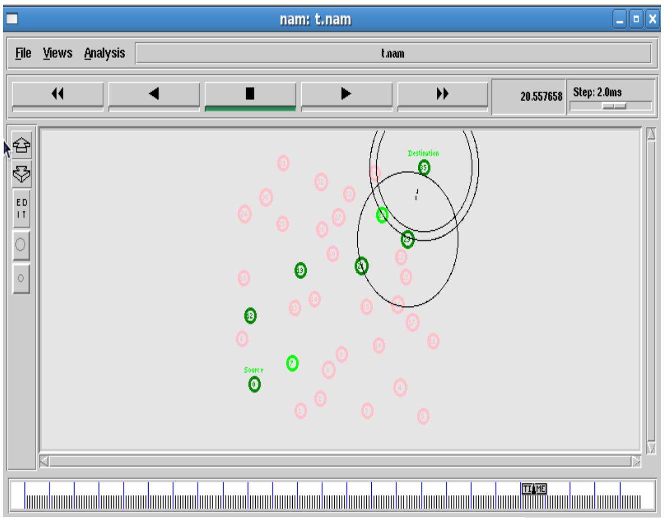

Figure 8 Data Transfer without Wormhole attack

The nodes transferring data without wormhole nodes make the smooth passage of the data in the adhoc network environment. The data drop in this process is very negligible as in figure 8. The source can easily send data without any late delivery and packet loss. This scenario is very reliable to send the data from the source to the destination nodes.

Simulation scenario of Wormhole attack:

The wormhole node becomes the one hop neighbors to most of its neighboring nodes. The source node transfers data through the wormhole node to the destination. The wormhole node makes use of the tunnel to transfer the data. The tunnel created by the pair of wormhole nodes is called wormhole tunnels which causes late delivery of the data and overall incurs the energy losses in the network.

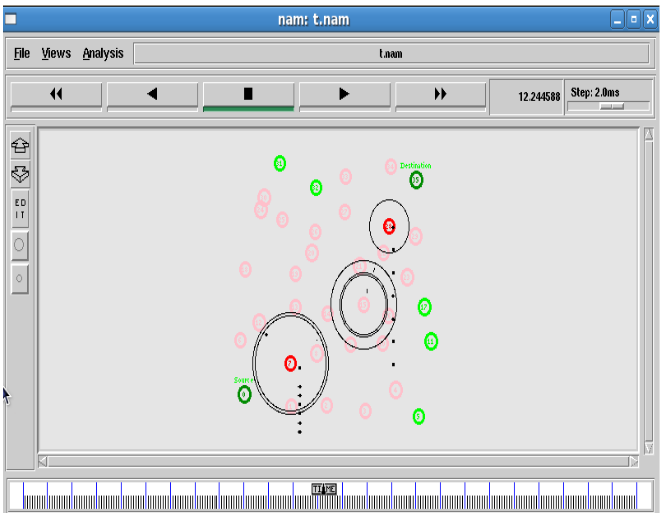

Figure 9 Packets dropping due to wormhole attack

The wormhole node transfers the data through the tunnel thus, in this process it put large number of the data packet in its queue to process the large number data and while processing all the data it drops the data packet beyond its queue size shown in Figure 9. Thus, the wormhole node drops data constantly while they are effective in the network.

PERFORMANCE EVALUATION

Network throughput with and without wormhole attack:

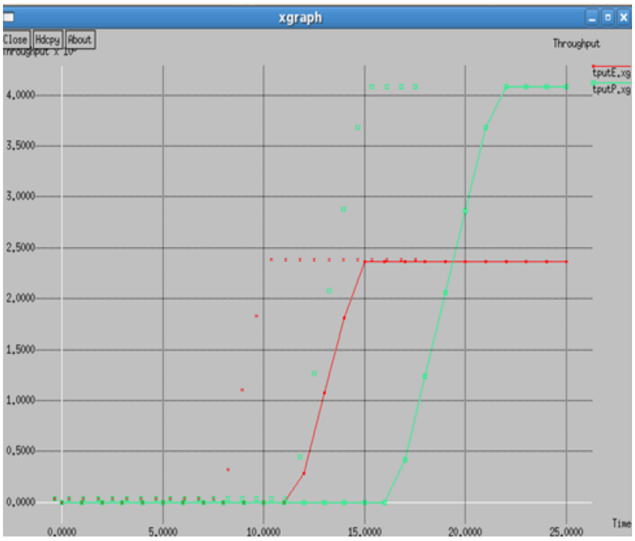

Figure 10 Comparison of network throughput with and without wormhole attack

The above compared throughput are of the scenario's when there is no wormhole node present in the network which is represented in green while the red curve represents the throughput after the intrusion in the network i.e the packet losses during the wormhole attack decreases the throughput of the network which is caused by the packet losses incurred on the wormhole nodes

The comparison of the packet drop:

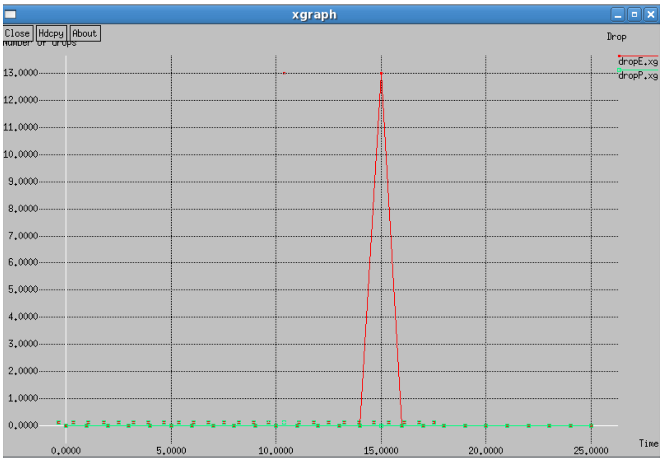

Figure 11 Packets loss during wormhole attack vs without wormhole attack

The above graph in figure 11 shows the number of packets dropped during the wormhole attack which is represented in red. The other losses in the network are very less and negligible as compared to the wormhole packet losses thus they are represented in green.

The comparison of the packet delivery ratio:

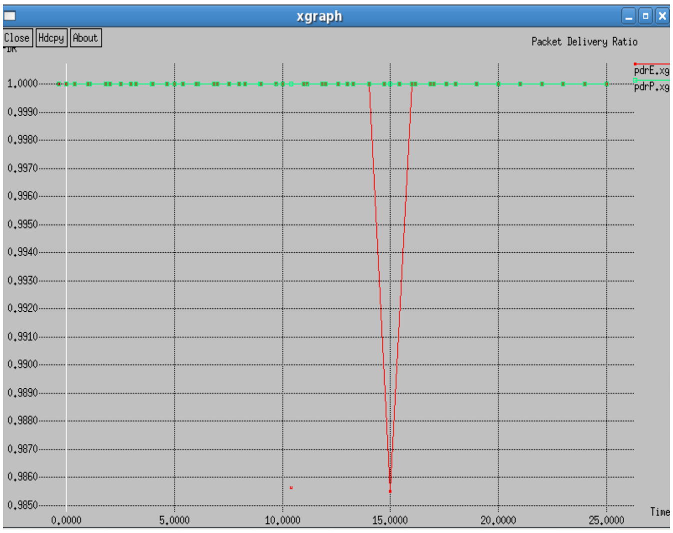

Figure 12 Packet delivery comparison of network that has wormhole attack vs network without attack

The packet delivery ratio touches a new low when the wormhole nodes are effective in the network thus, the delivery of the packets are affected when the wormhole nodes put the packets in the queue and also when it drops the packets.

6. CONCLUSION

In this paper a solution is proposed to prevent the network against wormhole attack. A secret key is used for encryption and decryption of hello packets. Because of this only authentic nodes will remain in the network, non-authentic nodes (wormhole node) will be discarded. As a result communication can take place only between the trusted nodes. So malicious node cannot enter into system and communication is secured. In this work we choose AODV as routing protocol for MANET, a pair of wormhole nodes is selected for performing wormhole activity. And simulation is done on NS 2.34 with 36 nodes. Simulation clearly shows that our method is well effective in preventing the network against wormhole attack.

7. Related Work

Alexandros et. al. in 2005 evaluated multicasting algorithms for MANETs. Multicasting is used for one to many and many to many node communications. Performance of MAODV (multicast ad hoc on demand distance vector routing protocol) and ODMRP (on demand multicast routing protocol) are evaluated on the basis of packet delivery ratio and latency. From MAODV, it has been observed that it performs well in large areas while ODMRP performs much better in high speed. [11]

Priyanka et. al. in 2010 introduced a nod selection algorithm named FRENSA (farthest reliable efficient node selection algorithm), works on multi-hopping mechanism. FRENSA is designed for next node selection and to enhance the quality of network. It selects the next node with respect to distance from sender node, its power backup and reliability for packet forwarding. This criterion reduced the overall communication head and improves the reliability of the network. [12]

Ajay Jangra et. al. in 2011 proposed EPSAR (efficient power saving Adaptive routing protocol) which is a novel approach for the selection of farthest and efficient node within the clusters. EPSAR used AODV & DSDV. In order to get reliable and efficient path in multi-hopping EPSAR is followed. It tried to find out the actual working with different parameters like unreliable battery, malicious node. FRENSA is the basic concept of EPSAR. [13]

Kimaya sanzgiri et. al. in 2002 proposed a certificate based protocol named ARAN to reduce security threats to AODV & DSR and tries to avoid all identified attacks. It discussed about different activities which are possible against routing protocol in ad hoc network and identify various security environments with their varying requirements and security threats. They had explored in detail about security requirements of ad hoc networks and finally proposed a secure routing protocol for managed open environment that does put any extra work load on nodes of the network but still prevent the network from many security threats; simulation study proves efficiency of the proposed protocol. [14]

Yi et. al. introduced a new protocol named MOCA (mobile certificate authority) based on PKI (public key infrastructure) and CA (certificate authority) proposed for efficient communication. [15]

Madhavi et. al. in 2008 proposed an intrusion detection system named MIDS (mobile intrusion detection system) for multi-hop network. This system very efficiently detects the misbehavior of nodes, packet drop in network and delay by appointing a monitor in the network. [16]

Chiung-Ying Wang et. al. in 2005 proposed a p-MANET which is an efficient power saving protocol. This work tried to reduce the power consumption and transmission latency by offering new foundation (MAC) layer power saving protocol. [17]

A.K.Sharma and Amit Goel et. al. in 2005 proposed a novel algorithm for selecting best neighbor node in multicast MANETs named BNNSA (best neighbor node selection algorithm). [18]

A.K.Sharma and Amit Goel et. al. in 2005 proposed an excellent, multicast efficient routing protocol named MOMENTAP (moment to moment node transition awareness protocol). [19]

References

[1] P. Siva Kumar, Dr. K. Duraiswamy, “A QoS Routing Protocol for Mobile Ad hoc Networks based on the Load Distribution”, 2010 IEEE.

[2] Ade, S.A. and P.A. Tijare, Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks. International journal of information technology and knowledge management, 2010. 2(2): p. 545-548.

[3] Das, S.R., et al., Performance comparision of two on-demand routing protocols for ad hoc networks, in IEEE Personal Communications Magazine2001.

[4] Perkins, C., et al. AODV. Available from: http://moment.cs.ucsb.edu/AODV/.

[5] Perkins, C.E. and E.M. Royer, Ad-hoc on demand distance vector routing.

[6] Perkins, C.E., et al. AODV. Available from: http://moment.cs.ucsb.edu/AODV/.

[7] Royer, E.M. and C.E. Perkins. An implementation study of the AODV routing protocol. in Proceedings of the IEEE wireless communications and Networking Conference. 2000. Chicago, IL: IEEE.

[8] Zapata, M.G. and N. Asokan, Securing ad hoc routing protocols. ACM, 2002: p. 10.

[9] Gorantla, K., Routing protocols in mobile ad-hoc networks, in Computing Science2006, Umea University: Umea. p. 36.

[10] Chakeres, I.D. and E.M. Belding-Royer, AODV Routing Protocol Implementation Design, in Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW'04) - Volume 72004, IEEE Computer Society. p. 48-53.

[11] Vasiliou, A., Economides, A.A.: Evaluation of multicasting algorithm in MANETs. In: Proceedings of World Acadmy of Science, Engineering and Technology, vol. 5 (April 2005); ISSN 1307-384

[12] Priyanka, Komal Kumar Bhatia, Ajay Jangra “FRENSA: Farthest, Reliable and Efficient Node Selection Algorithm for Mobile Ad-hoc Networks (MANETs)" in IJCST International Journal of computer Science and Technology **Vol. 1 Issue 2 December 2010**

[13] Ajay Jangra, Nitin Goel & Priyanka "Efficient Power Saving Adaptive Routing Protocol (EPSAR) for MANETs using AODV and DSDV: Simulation and Feasibility Analysis" in IEEE, IPTC 2011.

[14] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields and Elizbeth M.Belding-Royer "A secure routing protocol for Ad Hoc Networks" Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.

[15] Seung Yi, Robin Kravets "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks" University of IIIinois at Urbana-Champaign Urbana, IL61801, {seungyi, rhk}@cs.uiuc.edu.

[16] S. Madhavi, Tai Hoon Kim, "An Intrusion Detection System in Mobile Ad hoc Networks", international journal of security and its applications, vol. 2 no. 3, july 2008.

[17] Chiung-Ying Wang, Chi-Jen Wu, Guan Nan Chen and Ren Hung Hwang, "p-MANET: Efficient power saving protocol for multi-hop mobile ad hoc networks", proceedings of the third international conference on information technology and applications (ICITA'05) 2005.

[18] A.K.Sharma and Amit Goel, "Best Neighbor Node Selection Algorithm for MANET", journals of institution of engineers, Jan 2005.

[19] A.K.Sharma and Amit Goel, "Moment to moment node transition awareness protocol (MOMENTAP)", international journal of computer application (IJCA) special issue, IASTED, vol. 27/1 jan2005.