Effect of Enhancing MAC layer Security and Power Saving Mode on Mobile Ad Hoc Network

Sneha Kanchan*
Research Scholar
Computer Engineering Department,
YMCAUST, Faridabad -121006, India
sneha.kanchan159@gmail.com

Poonam Mittal
Assistant Professor
Computer Engineering Department,
YMCAUST, Faridabad -121006, India
poonamgarg1984@gmail.com

Dr. C.K. Nagpal
Professor
Computer Engineering Department,
YMCAUST, Faridabad 121006, India
nagpalckumar1@rediffmail.com

Abstract— Mobile Ad Hoc Network is the wireless network with no centralized monitoring system. The nodes are free to move anywhere in the network. These mobile nodes also act as routers and make the routes for any data transmission on their own. They take the responsibility of route discovery and packet transmission of other. This cooperative approach of packet transmission has made these ad hoc networks much popular. Due to lack of infrastructure and centralized monitoring system, these networks are vulnerable to the security threat. If there is an intruder among the mobile nodes, the whole system can be damaged to the large extent. Since there is no central framework to monitor the security issues, mobile nodes have to implement their own security feature. The security feature, that is to be implemented on the network, must pass through simulation so that the actual effect of it on the performance of network may be analyzed prior to its implementation. This paper focuses on the effects of adding MAC layer security feature to the mobile ad hoc networks. Also the effect of adding power saving mode, which dominates the co-operative behavior of mobile nodes, has been discussed. This analysis gives a better picture for the implementation of routing protocols.

Keywords: Ad hoc networks; MAC layer; Pause time; Power saving; QualNet; Random Waypoint mobility; Routing protocols; Security; Simulation.

I. INTRODUCTION

Security is the major concern in the Mobile Ad Hoc Networks due to wireless channel access and multi-hop routing. Any node can enter into the network and participate in the transmission because there is no centralized system to monitor. Thus, MANET network can be hacked very easily and it may leak very important information. Various security attacks can be done on the ad hoc networks and if not implemented with a good security profile, the whole network can be infected or destroyed. In the current era, even the most critical processes of the organizations are done online. If the network is hacked, the company will loose the confidential data which can hamper their whole business. So, a MANET should provide the security services such as authentication, confidentiality, integrity, anonymity, and availability to the mobile users [1]. Although there are various security attacks present in the network like Trojan horse, Packet sniffing, Wormhole attack, Email virus and Denial of services, we can protect our network by using Firewalls, Antivirus software, Anti-spyware applications, Encryption etc. In this paper, we are focusing on the Wormhole attack and effect on the performance of MANET when implemented with the required security feature. Also, we are simulating the network with power saving mode and the resulting behavior is compared with non- power saving mode. The simulation is performed over Random Waypoint mobility model with a pause time of 30 seconds and proactive, reactive and hybrid routing protocols are thoroughly examined.

II. PROTOCOL SPECIFICATION

The routing protocol decides how the routes will be discovered in the network. The change in MANET topology may be very fast and unpredictable. Also, MANET nodes are considered vulnerable to failure [2]. A routing protocol must be able to cop up with these mobile nodes. Nowadays, building or even choosing a perfect protocol for the network is a big challenge. So, simulation is performed to check the characteristics of a particular protocol while changing the load and other features of the network. If the protocol is performing well under certain conditions, we can choose those protocols to implement in our network.

The protocols evaluated in this paper can be described as follows:

A. Proactive Protocols

In proactive approach, tables for each node are maintained. These tables specify the neighbor of the nodes, routes and distances between them. Here nodes have to maintain all entries in the tables. It does not matter that the routes are demanded or not. It is also possible that those routes are never being demanded. Then there is no use of making such unused routes. However, table is maintained to speed up the response time. But proactive protocols are not suitable for the large network as they have to maintain each and every nodes position which may result in very large sized tables.

1) Source Tree Adaptive Routing: STAR broadcasts its source tree information in the network. Each node sends an update message to its neighbor during its initialization and also about new destinations, chances of routing loops, cost of paths etc. The nodes in this network develop the partial topology graph based on its adjacent links with neighbor and source tree broadcasted by neighbor. STAR protocol has two variations. These can either use optimum route approach (ORA) or the least overhead routing approach (LORA). ORA tries to find out the shortest path available but LORA finds the path in which least overhead is required. STAR is basically known for its LORA approach unlike other routing protocol. Hence the path returned may or may not be optimal.

2) Optimized Link State Routing: OLSR is the optimization of classical link state routing protocol, LSR. Here, each node selects a set of neighbour nodes as 'multipoint relays' (MPR). Only the nodes which have been selected as MPR are responsible for forwarding the broadcasted messages during the flooding process. Number of nodes and packets, which involve in routing, are reduced in OLSR. Also the node has to report only to its MPR selectors. So, partial link state information is distributed in the network. This protocol always provides optimal routes in terms of number of nodes in the route. It is best suited for the large and dense networks.

3) Intrazone Routing Protocol: IARP is the proactive approach of ZRP. IARP's routing zones can be efficiently used to guide route queries outwards rather than blindly relaying queries from neighbour to neighbour. IARP's proactive tracking of local network connectivity provide support for route acquisition and route maintenance. Routes to local destinations are immediately available as table is already maintained. Once routes are discovered, IARP's routing zone offers enhanced, real time route maintenance. If link fails, traffic can be re-routed to the suboptimal routes. It makes them more robust to changes in the network topology and hence improves the quality of the network.

B. Reactive Protocol

Reactive protocols try to find out and set up routes once demanded. No table is maintained here. So, they save lots of overhead of maintaining tables and routes. But it increases the time period for searching the routes and hence data packets transmission. The delay is more before data transmission because it has to wait until any route is found. As the request/reply packets are flooded in the network in finding the route, they are not optimal at bandwidth utilization. But these are more scalable to the topology change, hence more suitable for highly mobile networks. Also for large networks, we don't need to maintain information for every table and this increases the scalability of the network.

1) Dynamic Source Routing: In DSR, a route is established by flooding the route request messages. A route cache is maintained in which the recent routes are being cached. Whenever there is a need of a route, and if the route is in cache, it is returned immediately without the need of moving up to the destination. This mechanism of "Route Discovery" and "Route Maintenance" are the major components of DSR. It eliminates the periodic update feature of DSDV and other Proactive routing protocols. DSR allows the senders to select and control the route. It avoids the "counting to infinity" problem avoiding the loop.

2) Ad- Hoc On-Demand Distance Vector: AODV combines the route discovery and route maintenance features of DSR and hop by hop routing sequencing number and periodic updating of packets feature of DSDV. When a route is demanded and if it is not available, a route request (RREQ) message is generated and flooded in a limited way to its neighbor. When this RREQ reaches to its destination or to the node which is having the route cached to the destination, we can say that the route is found. Then, a connection is setup between the source and destination using this route. After this, the packet can be transferred to the destination. AODV is

highly adaptive to the dynamic networks and also enjoys loop free routing like DSR. It detects the latest route. But if the source sequence number is old, it can lead to inconsistent routes.

3) Dynamic MANET on-Demand: DYMO routing protocol is defined in IETF Internet-Draft. It has the "Path accumulation" property of DSR and simplifies AODV by removing the unnecessray Route Reply packets, RREP, beconing property and precursor lists [3]. RREQ packets are flooded in the network. Target, after receiving the RREQ, replies by sending the reply packets. The transmission of packets is in hop-by-hop fashion. When the source receives the target's reply, then the connection is established between them. While maintaining a route, a Route ERROR packet, RERR, containing the list of unreachable nodes is broadcasted. After receiving this, nodes check in their cache that if they have the lost node route or not. If yes, the entry is invalidated saying that the route is found else the RERR is broadcasted again. DYMO also use sequence numbers and so enjoys the loop free routing.

4) Interzone Routing Protocol: IERP is the reactive approach of the zone based routing technique of hybrid protocol. In hybrid routing, nodes have predefined path up to some level but after crossing that level, routes are found once demanded. IERP is the protocol responsible for finding the paths which are not within the routing zone. It broadcasts using unicast routing to send the packet to the boundary and then to the peripherals of the current zone. If a route is found by any node, then it replies. Otherwise the request is transmitted to the further peripheral zones. It is used with the Intra-zone Routing Protocol (IARP) in zone based routing.

5) Location Aided Routing: LAR1 uses the location information of the mobile nodes. In this, locations can be categorized into two parts, expected zone and request zone. According to the previous position of the node, some zones are defined as the expected zone of the node. The RREQ is only sent to that expected zone. The zone which includes the expected zone and the surrounding is known as request zone. Hence the RREQ is only flooded in the request zone and so, it reduces very large traffic overhead. Once the destination node receives the RREQ, it replies with its position, speed and the current time. If no RREP is received within the specified timeout period, the source have to broadcast the RREQ to the whole network. Then the smallest rectangular area can be chosen which covers the expected area and the source as well. This rectangular zone is known as request zone. This zone based reactive approach reduces the routing packets produced in comparison to blind broadcasting.

C. Hybrid protocol

Hybrid routing combines the best features of both proactive and hybrid protocols. It is almost a zone based routing. It means the nodes are categorized into different zones. Based upon their zonal regions, routes are decided. There may have been some predefined routes up to a level and beyond that level, a route is found out once demanded. If not handled correctly, it will pose the overhead of both routing approaches. The main examples of this type of protocol are ZRP and LANMAR. While comparing with proactive protocol, fast route establishment is there but overhead is much less in hybrid protocols. On the other hand, in comparison to reactive protocols it requires high storage because of maintaining the table up to some extent. But processing time is faster than reactive approach. It is used in the network which in large in size but needs quick response.

1) Landmark Routing Protocol: LANMAR utilizes the concept of landmark for scalable routing in large networks. After being introduced in wired network as landmark, it borrowed the concept of landmark into wireless ad hoc network. If the members are moving in groups, LANMAR keeps track of that. These groups have a landmark that they can update their table within this scope only. This can be also useful in case of link failure. This reduces the routing table size up to a large extent. This helps in improving scalability. The protocol uses proactive protocol as a base but mobile nodes should also support the sub-networking concept [4]. LANMAR is a very efficient hybrid protocol, which may not give the very quick start but its overall performance is better than ZRP.

2) Zonal Routing Protocol: ZRP combines the IARP and IERP routing protocols. As a IARP protocol, it maintains an up-to-date routes in a table of a zone centered on each node. The routes are immediately searched within this zone because of the already maintained table. But if the destination is in some other zone, a route discovery procedure is needed, which can take the advantage from the local routing information of other zones as well. Here IERP is used to find out the route when demanded and the router finds the route using reactive approach.

III. MOBILITY MODEL

Mobility model describes the movement pattern, speed and location variation of the mobile users. It simply tells about the movement behavior of the users. In order to evaluate the performance of mobile wireless systems, the realistic mobility model is very crucial and difficult aspect of simulation. But mobility model can create a scenario similar to the realistic environment. To evaluate the performance of a protocol for an ad hoc network, the protocol should be tested under realistic conditions. For this an accurate mobility model must be chosen. Random waypoint mobility model allows the nodes to move randomly and independent of each other. In this model, nodes can also pause for few seconds. The mobile hosts pauses in one location for a certain period of time. That time is

known as pause time. It is the important feature of this mobility model because if the nodes are always moving, their neighbors will change too frequently to make a session for transmitting the packets. The routes can be broken in the middle of transmission if the node moves out of the range too frequently. Then the source node has to reinitiate the whole routing process again. Hence, it's a better practice to take the benefits of pause time and give the nodes sufficient time for the packet propagation. In this paper, we are taking the pause time as 30 seconds. It means that the nodes will pause for 30 seconds in the network and then it moves to the next location.

IV. MAC LAYER IEEE 802.11

Mac Layer is an important layer of the network. Wormhole is the security attack which can leak information to the other network and can significantly disrupt the communication across the network. It is hard to detect the wormhole in the network as they can behave like a normal node. However one can easily implement it [5]. Wormholes can easily participate in the routing and transmission of packets without the knowledge of the legitimate nodes in the network. So, MAC layer provides a facility to secure the network by adding security feature and the parameter under this security feature is the wormhole victim turnaround time which has two values 0 seconds and 10 seconds. The network can also be protected from the timing attack of the wormhole using the hop count facility [6]. The hop count can not be least at all the time. So, if the node is offering minimum hop count every time, it can be taken as the misbehavior. The misbehavior of the nodes is countered. If exceeding from a limit, nodes can be considered as the wormhole [7]. MAC layer also provides the power saving facility which denotes the selfish behavior of the node. The power saving mode provided by the IEEE 802.11 is the most well known power saving strategy [8]. Nodes can move to sleep state when they want and at that time they don't take part in routing or packet transmission. This is used to conserve the battery power. Without battery power, nodes become useless [9]. Since battery power is limited, we need to conserve it, so power saving is an important feature of the nodes. But if the node is using this feature much time, this also can be considered as the misbehaving activity of the node. If this behavior exceeds from a threshold, the node is flagged as misbehaving and rest of the nodes are informed about this misbehavior [10]. So, the rest of the node can change their route.

V. PROPOSED WORK AND SIMULATION

In this paper, MANET network is simulated over the wormhole attack protection and power saving features of the MAC layer. The protocols are compared on the basis of various parameters form application layer and transport layer. The simulation is performed by varying the number of nodes in between 10-80 nodes. It is smoothly noted that how the protocol behavior changes when the load increases on the network. The proactive protocols used are STAR, OLSR and IARP. Reactive protocols include DSR, AODV, LAR1, IERP and DYMO. ZRP and LANMAR are included from hybrid protocols. These are compared on the basis of various application layer and transport layer parameters. Application layer parameters include Average Jitter, First Packet Received, Total Bytes/Packets Received, Last Packet Received, Average End to End Delay and Throughput. Transport layer has only two parameters namely Packet from application and Packet to application. All protocols are compared on the outcome of all these parameters.

The packets are sent from node 1 to 3 at the constant bit rate. The parameter table of the whole scenario better describes the picture:

TABLE I. SIMULATION PARAMETERS

Parameter Name	Parameter Value
Size of Region	1500*1500
Shape of Region	Square
No. of nodes deployed	10,20,30,40,50,60,70,80
Mobility Model used	Random Waypoint
Battery Model	Linear Model
Energy Model	Mica Motes
Total bytes sent	12288
Total packets sent	24
Throughput (bits/sec)	4274
Routing protocol	AODV,DSR,DYMO,LAR1,IERP, STAR, OLSR, IARP, ZRP, LANMAR
MAC Layer Feature	Security, Power saving
Traffic model of sources	Constant Bit Rate

The protocols are tested by varying the MAC layer's security feature and power saving mode. Under security feature, it is enabled as 'yes' and wormhole victim turnaround time is varying from 0 to 10 seconds. The power saving mode is also enabled and disabled to simulate the network. All these simulation is done under all combinations possible.

So we can categorize our research in following scenarios:

- Security feature is enabled and wormhole victim turnaround time is 0 second.
- Security feature is enabled and wormhole victim turnaround time is 10 seconds.
- Security feature is enabled and wormhole victim turnaround time is 0 second. Power saving mode is enabled.
- Security feature is enabled and wormhole victim turnaround time is 10 seconds. Power saving mode is enabled.
- Security feature is disabled and power saving is enabled.
- Both Security feature and Power saving mode are disabled.

At first, we have evaluated the protocol is behaving best under which category. Then that is taken as the most eligible feature of the protocol. For further evaluations, we proceed with that feature of the protocol. After that the best protocol of proactive, reactive and hybrid is compared. And for each parameter, best protocol is selected. We can get different protocol for different parameters. We just need to select the protocol according to the need of our network.

VI. RESULTS AND DISCUSSIONS

The results of above scenarios are being discussed in this section. The protocol which shows the best as well as constant behavior among all is chosen as best.

A. Average Jitter Comparison

The average jitter of the packet transmission should be as less as possible. Among AODV protocols' categories, it minimizes the average jitter when its security feature is enabled and wormhole victim turnaround time is 0 seconds. IERP is not making any server in any case of our simulation. So, it is not considered useful for this analysis. DSR when implemented without any security minimizes the average jitter produced between the packets. DYMO with 0 or 10 seconds turnaround time minimizes the average jitter produced by DYMO protocol. LAR1 with no security minimizes the average jitter produced by LAR1 protocol. IARP with 10 seconds turnaround time minimizes the average jitter produced by IARP protocol. OLSR with no security minimizes the average jitter produced by OLSR protocol. STAR with 0 seconds turnaround time or STAR without any security minimize the average jitter produced by the STAR protocol. LANMAR without any security minimize the average jitter produced by LANMAR protocol. ZRP with 0 seconds victim turnaround time minimize the average jitter produced by ZRP protocol.

B. Average Delay Comparison

The best protocol comprises of the minimum average delay. Almost all protocols give optimized delay when implemented without any security. DSR and ZRP with 0 seconds turnaround time can also give the optimal result.

C. Throughput Comparison

Almost all protocols give best throughput when implemented with security of wormhole victim turnaround time as 10 seconds. Only ZRP and STAR are the protocols which gives their best throughput when implemented without any security.

D. Best in each protocol category

Among all proactive protocols, for average jitter, STAR is the best. And within various sub categories of STAR, it is best when implemented without any security. Also, STAR receives 'First' and 'Last' packet in the least time. It poses minimum average delay in message transmission. OLSR without any security receives the maximum number of bytes/packets and it gives maximum throughput. Also it sends very huge number of packets from an application and receives even more number of packets from other application. No other protocol can compete with OLSR on this parameter.

In case of reactive routing protocol, AODV poses the minimum jitter and minimum overall delay. DSR has the minimum delay for receiving the first packet. Also, it receives the maximum number of bytes and packets. DYMO has the best throughput. All protocols are sending same number of packets from application but DSR is receiving the most packets from any application.

In hybrid protocol, LANMAR is best in all parameters except the first packet received parameter. ZRP is the quickest to respond; hence it is receiving the first packet in minimum time.

E. Best protocol for each parameter

In this section we are comparing the best protocol of proactive, reactive and hybrid protocol. It means the protocol selected here will be the overall best protocol for that parameter.

1) Average Jitter: LANMAR is producing the minimum jitter.

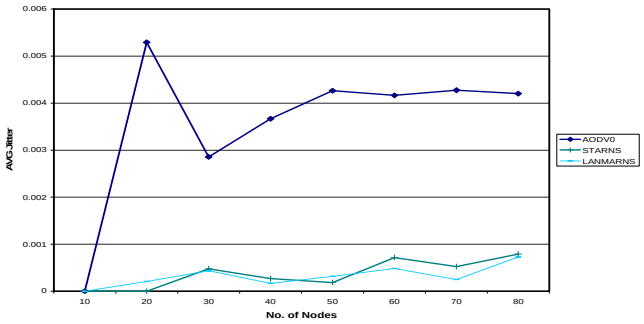

Figure 1. Average Jitter Comparison

2) First Packet Received: ZRP is the quickest to respond. So, it's receiving the first packet in minimum time.

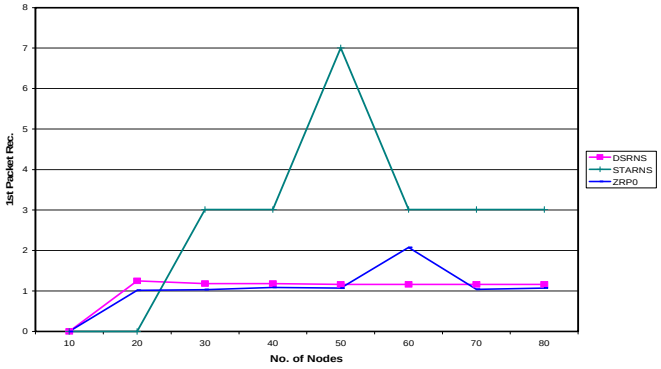

Figure 2. First Packet Comparison

3) Total Bytes/Packets Received: DSR is receiving the maximum number of bytes/packets.

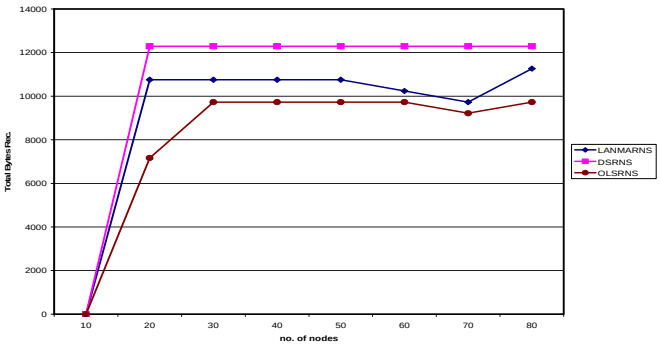

Figure 3. Total Byte Received Comparison

4) *Last Packet Received:* It is also receiving the last packet in minimum time.

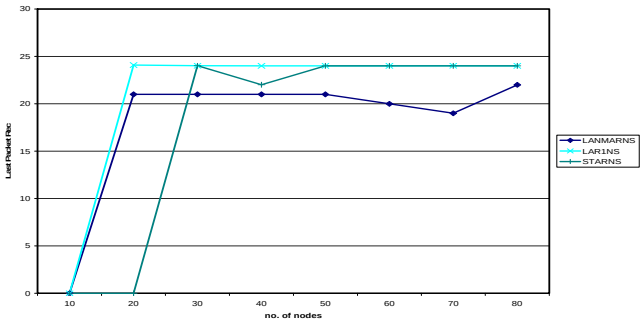

Figure 4. Last Packet Received Comparison

5) *Average end to end delay:* STAR has the minimum overall delay.

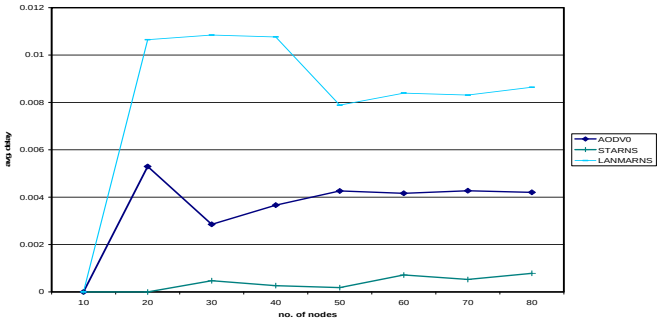

Figure 5. Average Delay Comparison

6) *Throughput:* DYMO is giving the best throughput among all.

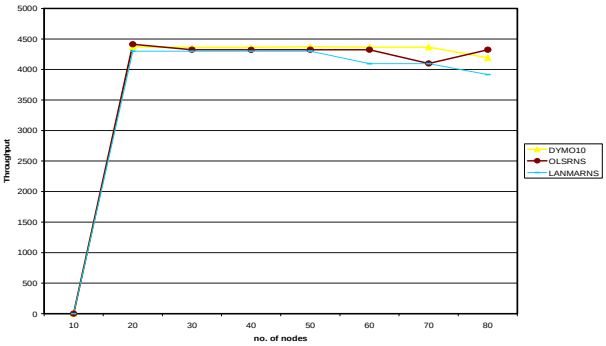

Figure 6. Throughput Comparison

7) *Packets from Application:* OLSR is best in sending maximum number of packets from an application.

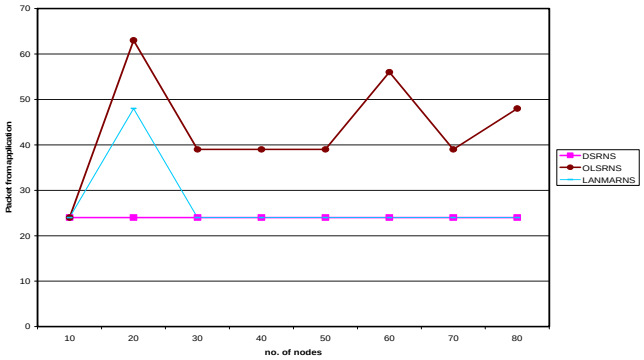

Figure 7. Packet from Application Comparison

8) Packets to Application: OLSR is also receiving maximum number of packets from an application. So, maximum number of packet recevied by the application is in OLSR protocol.

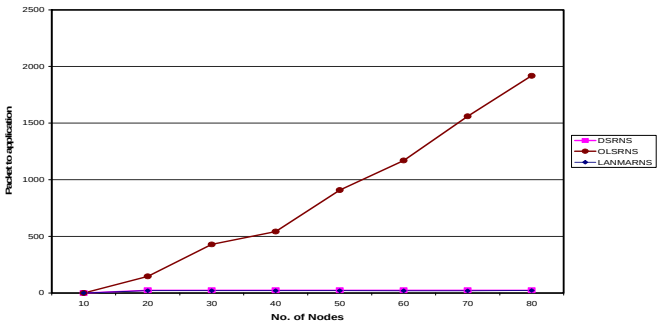

Figure 8. Packet from Application Comparison

VII. CONCLUSION AND FUTURE WORK

In this paper, proactive, reactive and hybrid protocols are compared by adding the MAC layer's security feature and Power saving mode. Power saving mode makes the nodes sleep in idle time. In most of the cases, it is not making any server and so transmission is not possible there, thus, allowing the protocols to loose many packets. On the other hand, adding the security feature in MAC layer increases the delay in transmission. However the throughput is best when we have added the security and wormhole victim turnaround time is 10 seconds. So, when we implement the network with this security feature, maximum throughput can be obtained. If anyone wants to implement the network with the minimum jitter or overall quickest response, then LANMAR with no security can be used. ZRP is the quickest among all protocols when it is implemented with 0 second wormhole victim turnaround time. These both are the hybrid protocols, so use the best feature of proactive to give quickest response. OLSR is implemented with optimized link state route, so it can send and transmit the maximum packet in an application. The network can be implemented according to our need and best for each criterion can be referenced from here. In future, we can extend this work by adding more security features like protection from virus and other intruders.

REFERENCES

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang's, "Security in Mobila Ad Hoc Networks: challenges and solutions", IEEE Wireless Communications • February 2004

[2] Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K. Tripathi, "A framework for reliable routing in Mobile Ad Hoc Networks", Proceedings of the IEEE INFOCOM, 2003.

[3] Archie Budhiraja and Roopali Garg's, "Performance comparison of dynamic Mobile ad-hoc network on-demand multipath routing protocol with AODV", International Journal of Scientific & Engineering Research, Volume 2, Issue 11, November-2011.

[4] Kap-Dong Kim*, Kwangil Lee**, Jun-Hee Park**, and Sang-Ha Kim*** "A scalable multicasting with group mobility support in Mobile Ad Hoc Networks", International Journal of Information Processing Systems, Vol.3, No.1, June 2007.

[5] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, "Wormhole attack in wireless Ad Hoc Networks: analysis and countermeasure", Department of Electrical and Computer Engineering University of British Columbia, 2006.

[6] Jonny Karlsson,Laurence S. Dooley and Göran Pulkkis, "Identifying time measurement tampering in the Traversal Time and Hop Count Analysis (TTHCA) wormhole detection algorithm", ISSN 1424-8220, 2007.

[7] Usha Sakthivel and S. Radha "Misbehaving node detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science 7 (5): 723-730, 2011 ISSN 1549-3636 © 2011 Science Publications.

[8] Chiung-Ying Wang, *Chi-Jen Wu, Guan Nan Chen, 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)0-7695-2316-1/05 $20.00 © 2005 IEEE.

[9] Yu-Chee Tseng, Chih-Shun Hsu, Ten-Yueng Hsieh, "Power-Saving Protocols for IEEE 802.11-Based Multi-Hop Ad Hoc Networks", 0-7803-7476-2/02/$17.00 (c) 2002 IEEE

[10] S. Usha, Member, IACSIT and S. Radha, "Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks", International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011.