ISSN : 2231-0711

Dr.Mahmood K. Ibrahem et al | International Journal of Computer Science Engineering and Technology(IJCSET) | July 2014 | Vol 4, Issue 7,223-230

A Secure Routing Protocol for MANET

Assist.Prof.Dr.Mahmood K. Ibrahem , Ameer M. Aboud

Internet Engineering Department - Network Engineering Department,

College of Information Engineering, Al-Nahrain University

Baghdad, Iraq

***Abstract*— Mobile ad hoc networks (MANETs) have become a remarkable technology for wireless communication in recent years because of its critical and emergency situations that may cover. Routing protocols for ad hoc network are vulnerable to various types of attack. Security is an essential issue in MANET due to open medium and absence of clear line of defence. Security services are prerequisite for using mobile ad hoc networks in sensitive or inimical environments. This research is dedicated for providing a secure routing protocol for MANET with large number of security services in the network layer. The proposed work integrates IPsec protocol with three routing protocol for MANET; Ad hoc On demand distance vector (AODV), Optimized Link State Routing (OLSR), and Geographical Routing Protocol (GRP) to provide confidentiality, authentication, integrity, and access control for routing information and data messages. The designed secure and unsecure networks are simulated under the effect of two types of attack, Intelligence Pulse Jamming Attack (IPJA) which makes Denial of Services (DoS) and Misbehaviour Attack (MA) which performs malicious action of some nodes with respect to others. Simulation results using Optimized Network Engineering Tool (OPNET) Modulator demonstrates that the throughput is degraded and the end to end delay rises in secure network. Best throughput among these three routing protocol with IPsec integration is IPsec-GRP and the worst is IPsec-AODV, while the best end to end delay of the network in case of IPsec-OLSR and the worst is IPsec-AODV. Network with security services under the effect of MA gives better throughput than the network under IPJA influence but the end to end delay in case of MA is more than as compared with IPJA.**

***Keywords*— MANET, IPsec, OPNET, AODV, OLSR, GRP, IPJA, MA.**

I. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Key features of MANETs summarized as; No Fixed Infrastructure, Dynamic Topology, Power and Processing Constraints, Intermittent Connectivity, Varying Security Requirements, Scarce Bandwidth and High-Loss, Unreliable Links. Multihop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. The design goal for ad hoc network routing protocols are Minimal control overhead, Minimal processing overhead, Multihop routing capability, Dynamic topology maintenance, Loop prevention, Centralized vs. distributed approaches, Optimal route, Scalability, and Efficiency [1][2][3][4]. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. The network layer security designed for MANETs are concerned with protecting the network functionality to deliver packets between mobile nodes through multihop ad hoc forwarding. Therefore, they seek to ensure that the routing message exchanged between nodes is consistent with the protocol specification, and the packet forwarding behaviour of each node is consistent with its routing states [5].

II. PROBLEM STATEMENT

Routing Protocols for mobile ad hoc networks suffer from the malicious action of the nodes in network when sending the packet from source through intermediate nodes to destination, so the security in the network layer is the most important issues to countermeasure various types of attacks in MANETs. Many researchers investigate secure routing protocol to protect data communication and provide more reliable route between nodes in the whole network. These secure routing protocols are designed either as an extension to the existing routing protocol for MANET or a standalone to be applicable to some types of routing protocols. The main goal of security in ad hoc network is to provide more security services, as possible, to prevent large number of attacks that may launch to the network. This part of research investigate the adding of security services by using IPsec protocol to the existing unsecure protocol for MANET and analyze the efficiency of both secure and unsecure protocols on the overall performance of the ad hoc network.

III. SECURITY IN MANET

The basic security needs of wireless ad hoc networks are more or less the same as those of wired networks. To some extent, several security schemes of the wire-line networks have been developed and implemented in wireless cellular networks. To make ad hoc networks secure, we need to find ways to incorporate some of these schemes of wireless and wire-line networks. While communicating over a wireless medium, the transmitted and received signals travel over the air. Hence, any node that resides in the transmission range of the sender and knows the operating frequency and other physical layer attributes (modulation, coding, etc.) can potentially decode the signal without the sender or the intended receiver knowing about such an interception [6]

[7]. The goal of security is to provide security services to defend against all the kinds of threat. In providing a secure networking environment, some or all of the following services may be required:

1. Confidentiality: Ensures that the intended receivers can only access transmitted data. This is generally provided by encryption algorithms to protect overall content or a field in a message.
2. Authentication: Both sender and receiver of data need to be sure of each other's identity. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates.
3. Integrity: Integrity defined as no modification, no addition, no deletion, no altering is done to the message. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.
4. Access control: prevents unauthorized access to a resource.
5. Non-repudiation: Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. Non-repudiation requires the use of public key cryptography to provide digital signatures. A trusted third party is required to provide a digital signature [8] [9] [10].

IV. Proposed Approach for Secure Routing in Ad hoc Networks

The secure routing protocol for mobile ad hoc network focused on one or more security services in the network layer to overcome the impact of one or more attacks against ad hoc network. The IP security is a powerful security solution for the network layer because of provision of the most important security services that needed to countermeasure the various types of attack and prevent the network from the malicious action. There are many routing protocols in the ad hoc environment and some of them contain secure extension to implement security solution. The routing protocols chosen for applying security requirements are; AODV, OLSR, and GRP. AODV and OLSR have either extension or specific protocol designed to provide security, but these solutions cover number of security services with lack of other services while GRP doesn't have any extension or specific protocols for security. The aim of combining IPsec protocol with these protocols is to give more security services than the existing secure routing protocols for AODV and OLSR protocol, and providing secure data communication between mobile nodes for GRP protocol which does not have any protocol or extension for security. Optimized Network Engineering Tools (OPNET) modular is used as a simulation tool to build the ad hoc network with routing protocols and its security.

V. Secure Mobile Ad hoc Network Design and Attacks

A. Design of Mobile Ad hoc Network

Mobile ad hoc network implemented for a campus consist of 30 mobile nodes, these nodes are distributed randomly in 800x800 m and each node moves in uniform distribution with 10 m/s with random mobility waypoint profile.

Random mobility defines a rectangular region in which a site will move during a simulation. Trajectories and orbits specify deterministic paths for mobile sites [11].

B. MANET Node Configuration

The mobile nodes that are deployed are (wlan_wkstn_advs). Each node of the first project has the common parameters that are used for each node in the network in all projects as shown in Table 1.Operation mode of the physical and media access control layers protocol is the IEEE 802.11 [4].The standard that is considered in the implementation is IEEE 802.11a operates under Orthogonal Frequency Division Multiplexing (OFDM) technology [12]. The data rate that will be used by the MAC for the transmission of the data frames via physical layer is 54 Mbps which is the maximum data rate for this technology with a radio frequency bandwidth 5 GHz. Transmission ranges for each node is 50-100 m within the network.

TABLE 1 MANET Node Configuration

Attribute	Value
Number of node	30
Standard of physical layer	IEEE 802.11 a
Data Rate	54 Mbps
Packet reception-power threshold	-95
Buffer Size (bits)	256000
Transmission Power (watt)	0.005
Trajectory	Vector
Node movement	10 m/s
Simulation time	900 s
Application	E-mail with high load
	FTP with medium load
	Voice (IP telephony 1 frame/sec)
Application Pattern	One profile contain three application in simultaneous order

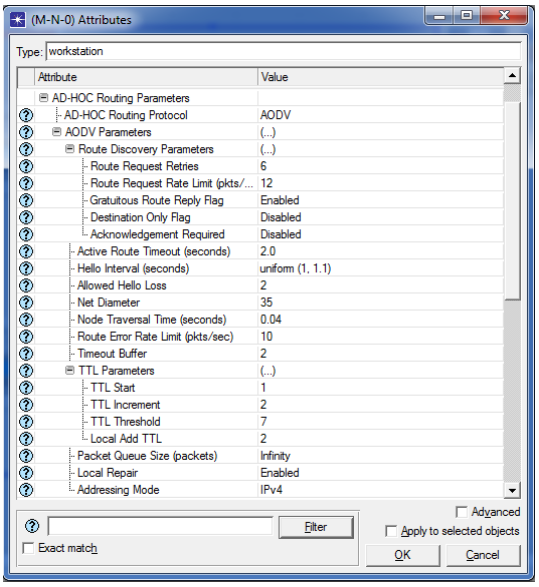
C. Implementation of Routing Protocols in MANET

After completing basic MANET network model design, Routing protocols for both nodes and server must be configured. Three Routing Protocols for MANET are implemented and supported by OPNET modular. Each protocol implemented in two scenarios in the first project, he first is for normal operation of the network and the second is the same parameters with integration of IPsec protocol.

1) Ad hoc On-Demand Distance Vector Routing protocol (AODV):

Ad Hoc On-Demand Distance Vector Routing (AODV) is a reactive routing protocol that minimizes the number of broadcasts by creating routes based on demand. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. The reply is sent using the reverse path. For route maintenance, when a source node moves, it can re-initiate a route discovery process. If any intermediate node moves within a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. Route maintenance is based on the periodic transmission of HELLO messages [13] [14]. The attributes of the AODV parameters are listed in table 2.

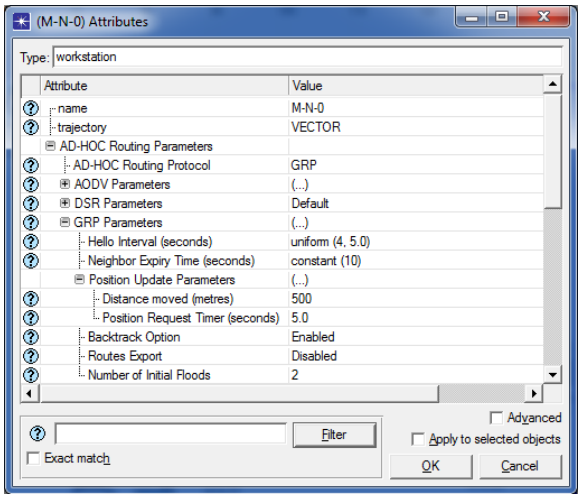
TABLE 2 AODV PARAMETERS



2) Geographic Routing Protocol (GRP):

Geographical Routing Protocol (GRP) is a proactive routing protocol with hop by hop routing. GRP protocol is source initialized protocol in MANET routing protocol in which all the routing path is created by source node in Mobile Ad hoc network. In this protocol, source node collects all the information about the route to the designation. A packet that named Destination Query (DQ) is used continuously to forward to each neighbor node until the destination is reached. When it reaches the destination, the destination node broadcasts a network information gathering (NIG) packet to its neighbors. The source node computes the best route according to the collected information and then immediately starts to transmit data packets. A node maintains its list of neighbor nodes by periodically broadcasting Hello messages, If a node does not receive a Hello message from a neighboring node for a period exceeding the specified "Neighbor Expiry Time," it assumes the link to the neighbor is lost. It is assumed that each node can determine its own position using a Global Positioning System GPS. The position of other nodes determined through flooding, when a node moves more than a specified distance, it sends out a flooding message with its new position [15] [16]. The attributes are listed in table 3.

TABLE 3 GRP PARAMETERS



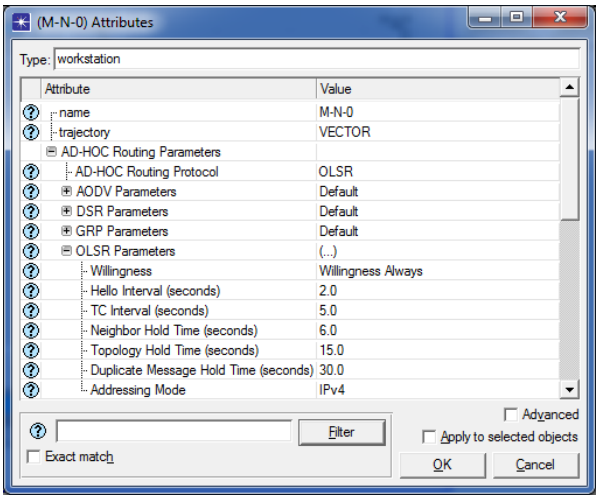
3) Optimized Link State Routing protocol (OLSR):

Optimized Link State Routing (OLSR) is a proactive routing protocol with hop by hop routing. The important concept introduced in the protocol is the multipoint relays where only selected nodes, referred to as Relay Nodes (RNs) or Multipoint Relay Nodes (MPRs), forward the broadcast messages during the flooding process. The purpose of MPR nodes is to minimize the overhead of flooding messages in the network by reducing the number of duplicate retransmissions while forwarding a broadcast packet. According to MPR selection criteria, each node in the network selects a set of nodes from its one-hop neighbors as MPRs. The OLSR protocol uses HELLO messages for neighbor sensing and Topology Control (TC) messages to declare the MPR information. MPR nodes periodically announce information about the neighbors that have selected it as an MPR, by broadcasting a TC message. Upon receiving the TC messages, each node in the network stores the information in the topology table, and only the MPR nodes forward the TC messages to the next-hop neighbors until all the nodes in the network receive the message [1] [14].

Node willingness to forwarding traffic on behalf of other nodes is setting to always that indicates this node always should be selected to carry traffic on behalf of others. Willingness always value is 7 and is decrease during power battery capacity draining, so reduced gradually to Willingness height and default until it reach to never. The time interval between Hello packets is 2 second, hello messages are necessary to maintain adjacencies between nodes. It carries 1-hop neighbour and 2-hop neighbour

information. Each hello packet arrival, link expiry timer is reset. If a hello packet is not received on a link within 6 seconds, then the link is declared to be lost. If all links to a neighbour is lost, the neighbour is declared to be unreachable. Table 4 lists the parameters of OLSR protocol. Ad hoc network design completed and snapshot of the network is presented in fig1.

TABLE 4 OLSR PARAMETERS



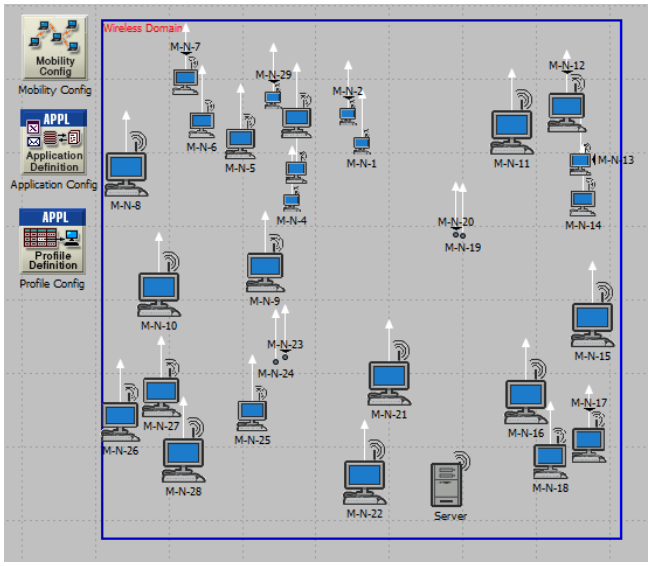


Fig 1. Snapshot of the Designed Mobile Ad hoc Network

D. *IP security Integration with Routing Protocols in the Network*

After designing a mobile ad hoc network with its applications, security solution with large number of services is presented. Provision of these services is done by using one of the best protocols that may give in one protocol for securing IP based communication focusing on authentication, confidentiality, integrity, access control and support perfect security forward. IP Security (IPsec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.

IPsec helps create authenticated and confidential packets for the IP layer. IP level security encompasses three functional areas: authentication, confidentiality, and key management [17] [18].IP Security can be an appropriate choice for MANET network layer to protect both routing information and data message. IPsec can be used in two different ways. It can be used in end-to-end, in which the source and destination hosts for a datagram are responsible for all cryptographic processing. It can also be used via gateways, in which a system near the source host is responsible for applying cryptographic operations on behalf of the source, while a system near the destination is responsible for checking and decryption. While MANET working without any support of fixed infrastructure such as base stations, wireless gateways or access points, the first implementation of the IPsec is appropriate for this type of network [19].

The IP security demand which is represents the end-to-end IP security demand between the specific source and destination was used between each pair of nodes in the network to provide fully mesh connection to all nodes to provide security. Integration of IPsec protocol with each routing protocols that are used in this part of research (AODV, OLSR, and GRP) is to perform a secure medium for ad hoc environment. The simulation runs in two cases, the network with the routing protocol without IPsec and with IPsec to measure the effect in the overall performance of the network when adding a security services represented by IPsec protocol. When packet arrives from source node in the transport layer of the OSI reference model, chosen of IP routing algorithm is performed by implements one of the routing protocol for ad hoc network (AODV, OLSR, and GRP) in each case to establish route between nodes. Forwarded packet searches for security policy database to know which policy that are negotiated previously between any two nodes need to communicate. If policy matching was found, the sender begins to determine the policy; otherwise discard the packet. After that, searching for the parameters that are used to implements the needed policy. These parameters are algorithms and protocols used for encryption, authentication, and integrity. If no match was found, internet key exchange repeated until negotiation of parameters occurred; otherwise the processing of the algorithms and protocols for IPsec is completed and forwarded the packet to other layers in OSI model. When the destination node receives the packet, it passes from the physical and data link layer respectively and when reaches the network layer, it also searches for security policy and association database. If the matching occurs, determination of policies and parameters also demonstrated; otherwise the packet discarded. Routing protocols for MANETs is implemented and forwarded the packet to the upper layer in the OSI layers.

E. *Creation and Implementation of Intelligence Pulse Jamming Attack (IPJA)*

Second project that is designed and implemented contains six scenarios with three routing protocols and its integration with IPsec. Each pair of these scenarios consists of one routing protocol without and with IPsec integration

under IPJA. It is achieved under the same parameters to measure the impact of this type of attack on the network that are secure and unsecure.

Intelligence Pulse attack is the type of jamming attack that deny the network transmission service to authorized user by generating noise on the wireless medium in order to block the access for authorized nodes. Jamming attack keep sending the high frequency packet on the wireless medium in constant rate or pulse rate by prohibit the traffic flow to authorized node on the wireless medium. The reason for calling this type of attack as intelligence because it's pulse on and off time are the main parameter which act on jamming to behave on and off at certain time as defined to generate the transmission [20].Intelligence Pulse jamming attack is created and implemented in three routing protocol for mobile ad hoc network without and with integration of IPsec protocol. The node in OPNET model that are used to implement jamming attack is jam pulsed node model represents a pulsed jammer which can be deployed as fixed, mobile, or satellite node . The jammer provides transmission on a single fixed frequency band which is masked by a periodic pulse train in time. The source creates and transmits packets for the duration of a pulse. The jammer transmission power is set to 0.004 which is less than the transmission power of the normal node in the network to prove that the jammer with low transmission power can create impact on the operation on the network by degrading the overall performance on the network. The jammer bandwidth is set to 100000 MHz and the base frequency of the channel is 1402.

F. Creation and Implementation of Misbehavior Attack (MA)

Designing and implementing the third project that contains six scenarios with three routing protocols and its integration with IPsec. Each pair of these scenarios is attacked by 12 misbehavior attack out of 30 nodes in normal operation. The impact of MA on secure and unsecure network is measured for three routing protocol for MANETs under the same designed parameters.

Misbehavior attack is the internal type of attack that can be launched on the ad hoc network. Misbehavior node is acting maliciously on the network by behaving abnormally under the same policies and rules of the other node in the network. It stops forwarding packet to other nodes by simply start dropping the packets, consuming the bandwidth of the network by broadcasting route when not necessary [20].The campus network with 30 node and 800 x 800 m2 range and each node moves in 10 m/s , the node using in this project is MANET station_adv node model represents a raw packet generator transmitting packets over IP and WLAN. Each node in the network configured according to the same parameters of the protocol and wireless LAN mentioned earlier. The traffic generating parameters for the normal operation of the node in the network is configured according the following attributes; the start time for packet generating is 40 second. Packet size is 1200 bit in exponential distribution which is equivalent to 150 byte according to IEEE 802.11 which is the range of packet size between 0 to 2304 plus 28 header filed. If the network packet size is larger than 2304 the source node discard the packet. The arriving time of the packet at the host is 0.05 second with exponential distribution. Implementing the misbehavior node in the network is done by making some of the 30 nodes work improperly with the other nodes in network, changing the packet size to 1600 which is equal to 200 byte. The packet inter-arrival time to 0.003 second that means each packet must be arrive at the other node in 0.003 second while the normal operation of MANET node of arriving packet is 0.05 second, this causing more packet receiving in other nodes with larger packet size because of malicious action of the attacker node in the network. Twelve misbehavior node acts maliciously designed in the network for all six scenarios.

VI. Simulation Results and Performance Analysis

Simulation results of the proposed network are presented. The performance of the network is examined. Many performance metrics are taken into consideration to discuss the behaviour of the network and the impact of the security solution. The effect of two types of attack in each scenario within the three projects mentioned before is performed. After running each project three times to get accurate result. fig 2 and 3 demonstrate average throughput and end to end delay for the network with IPsec, respectively. The average throughput for GRP with IPsec is the best throughput among the other routing protocols for ad hoc networks that are designed and implemented as shown in fig 2. The IPsec-AODV is the highest delay during the first half of the simulation, in the second part the delay of IPsec-AODV begins in decrease and the average delay for IPsec-GRP becomes the biggest as shown in fig 3.

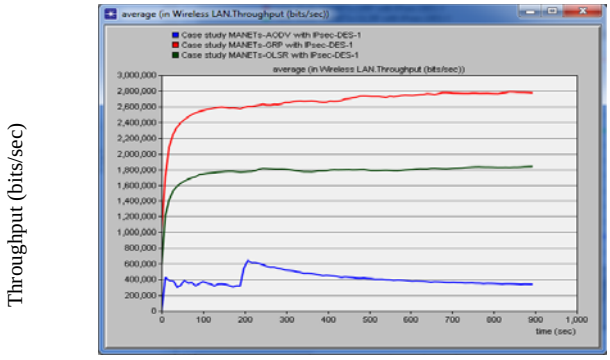


Fig 2. Throughputs for IPsec-AODV, IPsec-GRP, and IPsec-OLSR.

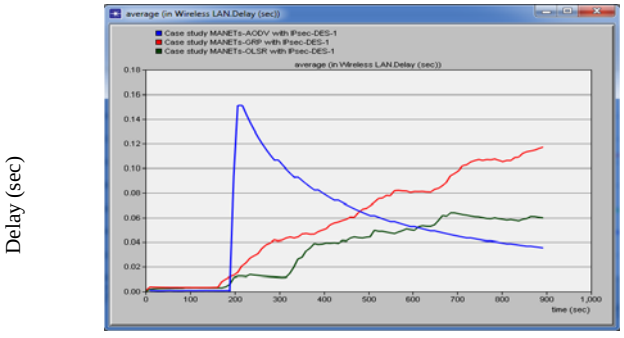


Fig 3. Delays for IPsec-AODV, IPsec-GRP, and IPsec-OLSR.

The arithmetic mean of values of the results are calculated and the percentage of variation in overall performance of the network was presented in table 5.The table indicates different statistics changed when the ad hoc network became secure and also demonstrate the impact of implementation IPsec in the network.

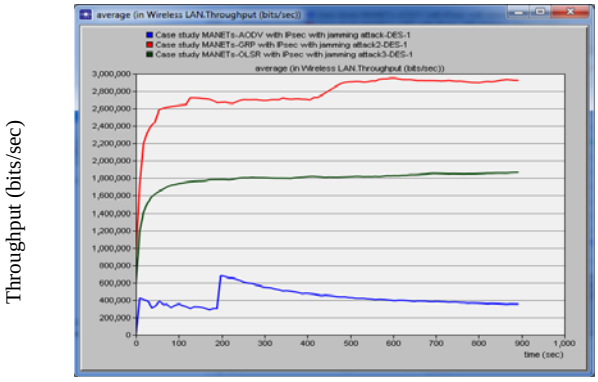
TABLE 5 PERFORMANCE METRICS OF SECURED AND UNSECURE AD HOC NETWORKS

Performance Metric	AODV	GRP	OLSR
Throughput	- 79.28 %	- 0.9607 %	- 0.072 %
Delay	+ 135.7 %	+ 26.67 %	+ 12.86 %
Data Dropped	- 52.46 %	+ 24.35 %	- 7.169 %
Number of Hops	+ 44.22 %	- 0.944 %	——
Route Discovery Time	+ 268.4 %	——	——
Retransmission Attempts	+ 109.5 %	+ 0.610	- 2.142 %
Routing Traffic Sent	- 11.91 %	- 0.108 %	+ 5.402 %
Routing Traffic Received	- 27.31 %	- 0.545 %	- 0.452 %
E-mail Download Response Time	+68.84 %	+ 137.2 %	- 38.59 %
Total TC Messages	——	——	+ 51.46 %

Hint:

1. Performance metrics with +ve sign means increasing by the mentioned value when the network became secure.
2. Performance metrics with -ve sign means decreasing by the mentioned value when the network became secure.

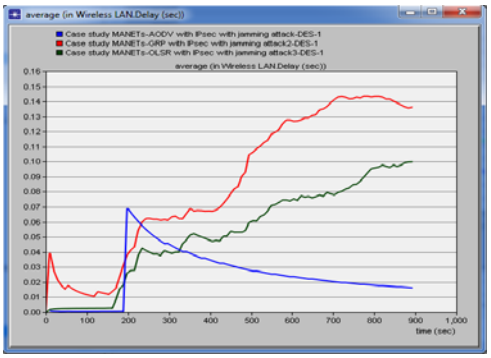
Throughput for the network without IPsec is more than the throughput with IPsec. The degradation of throughput in case of security solution due to more overhead on the network is added by IPsec protocol. The delay in the network with IPsec is higher than the delay without IPsec because IPsec protocol is consuming more time for processing and transmitting packet from source to destination. This time has an influence on the overall delay in the network. The time taken to establish route between two mobile nodes in case of the network with IPsec integration is greater than as compared with the vulnerable network. Fig 4 presents the throughput of the three routing protocol with security services under the effect of IPJA. The figure shows that throughput in case of IPsec-GRP is the best throughput among these routing protocol. Fig 5 illustrates that the average end to end delay for IPsec-GRP is the highest delay. The network in case IPsec-AODV is the best delay value for the three routing protocol with IPsec protocol integration under the effect of IPJA.



Throughput (bits/sec)

Simulation Time (sec)

Fig 4. Throughputs for IPsec-AODV, IPsec-GRP, and IPsec-OLSR under the influence of IPJA.

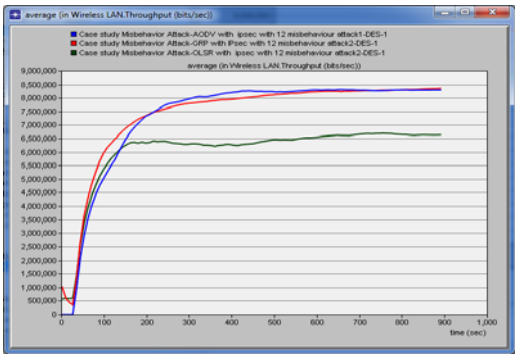


Delay (sec)

Simulation Time (sec)

Fig 5. Delays for IPsec-AODV, IPsec-GRP, and IPsec- OLSR under the influence of IPJA.

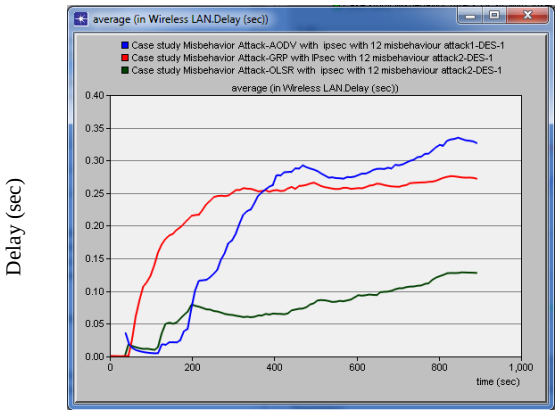
Average throughput of the secured network for three routing protocols with the presence of 12 MA out of 30 nodes is illustrated in fig 6. The figure indicates the throughput for IPsec-AODV is the best among these protocols and the difference compared with IPsec-GRP does not high. Fig 7 shows the average end to end delay for IPsec-GRP in the first half of the simulation is higher than IPsec-AODV; second part of simulation time shows IPsec-AODV is the highest delay among the other protocols .Network in case of IPsec-OLSR is the best delay compared with other designed protocol with presence of 12 MA.



Throughput (bits/sec)

Simulation Time (sec)

Fig 6. Throughputs for IPsec-AODV, IPsec-GRP, and IPsec-OLSR under the influence of 40 % MA.



Simulation Time (sec)

Fig 7. Delays for IPsec-AODV, IPsec-GRP, and IPsec-OLSR under the influence of 40 % MA.

Table 6 shows the percentage differences in two cases using arithmetic mean of values obtained from collecting statistics of OPNET modeler 14.5 .The first case is the combination of IPsec protocol with routing protocol for mobile ad hoc network under the impact of IPJA and the second are the combination IPsec protocol with the routing protocol for mobile ad hoc network under the impact of MA. Secure network under the effect of MA has more throughputs and delay as compared with the same network under the influence of IPJA. Routing traffic sent and received increase for AODV protocol with MA as compared with IPJA, while Routing traffic sent and received decreased for OLSR and GRP. Number of hops of AODV protocol increase in case of MA compared with IPJA because the malicious action of nodes causes change in route and taking more number of hops. Data dropped for the secured network under IPJA decreased as compared with MA. Topology control that is sending in case of OLSR protocol increase in case of IPJA due to jamming signal sends by this type of attack.

TABLE 6 NETWORK PERFORMANCE UNDER THE EFFECT OF IPJA AND MA.

Performance Metric	IPsec-AODV IPJA + MA	IPsec-GRP IPJA + MA	IPsec-OLSR IPJA + MA
Throughput	**Rise high**	**+ 165.7 %**	**+ 236.2 %**
Delay	**Rise high**	**+ 164.5 %**	**+ 43.21 %**
Data Dropped	**Rise high**	**+ 12.38 %**	**+ 275.5 %**
Number of Hops	**+ 27.61 %**	**- 4.702 %**	**——**
Routing Traffic Sent	**+ 286.6 %**	**- 4.540 %**	**- 9.156 %**
Routing Traffic Received	**+ 323.4 %**	**- 11.37 %**	**- 4.773 %**
Total TC Messages	**——**	**——**	**- 36.24 %**

Hint:

1. Performance metrics with +ve sign means increasing by the mentioned value in secure network under effect of MA as compared with IPJA.
2. Performance metrics with -ve sign means decreasing by the mentioned value in secure network under effect of MA as compared with IPJA.

VII. CONCLUSIONS

Integration of IPsec protocol with three routing protocols for MANETs is achieved. Provision of main security services such as confidentiality, authentication, integrity, and access control to resists many types of attacks and making ad hoc environment more secure was accomplished. The following points are concluded from this work:

1. Security services provision by IPsec protocol to the three routing protocol of mobile ad hoc network effect on the overall performance of the network. Average throughput is decreased by 79.28 % in secure network for AODV protocol compared with 0.9607 and 0.072 % for GRP and OLSR, respectively. The average end-to-end delay rises by 135.7 % in secure network for AODV protocol compared with 26.67 % and 12.86 % for GRP and OLSR, respectively. This is due to more computational operation consuming that make more overhead on the network.
2. Best throughput is obtained from these three routing protocol with IPsec integration is IPsec-GRP and the worst is IPsec-AODV.
3. IPJA making denial of services attack on the network and can be considered as external attack. This attack causes impact on the overall performance on the network. When the network attacked by IPJA in IPsec-AODV and AODV only, the average end to end delay improved by 63.04 % using IPsec under the effect of IPJA which gives better performance. The delay of OLSR is also enhanced by 21.04 % under the effect of IPJA by combining of IPsec protocol.
4. Designed mobile ad hoc network in two cases attacked by 12 MA out of 30 MANETs node in each protocol chosen. This is makes 40 % of MANET nodes acting malicious and is considered as internal attack. Throughput of mobile ad hoc network with security services under the effect of MA is better than compared with the network under the effect of IPJA, while the end to end delay for the network under IPJA is less than as compared with MA influence.

REFERENCES

[1] J.Sarangapani, "Wireless Ad Hoc and Sensor Networks Protocols, Performance, and Control", Taylor & Francis Group, LLC, 2007.

[2] R.Chadha and L.Kant, "Policy-Driven Mobile Ad hoc Network Management", John Wiley & Sons, Inc., Hoboken, New Jersey,2008.

[3] S. Sarkar, T. Basavaraju, and C. Puttamadappa, "Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications", Auerbach Publications,Taylor & Francis Group, LLC, 2008.

[4] S.Basagni, M.Conti, S.Giordano, and I.Stojmenovic, "Mobile Ad Hoc Networking", John Wiley & Sons, Inc., Publications, 2004.

[5] H.Yang, H.Luo, F.Ye, S.Lu, and L.Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol - 11, Issue - 1, pp. 38-47, 2004.

[6] F.Anjum and P.Mouchtaris, "Security for Wireless Ad hoc Networks", John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

[7] A.Mishra, "Security and Quality of Service in Ad Hoc Wireless Networks", Cambridge University Press, New York, 2008.

[8] E.Cayirci and C.Rong, "Security in Wireless Ad Hoc and Sensor Networks", John Wiley and Sons, Ltd, Publication,2009.

[9] R.Gupta, "Mobile Ad hoc Network (MANETS): Proposed solution to Security Related Issues", Indian Journal of Computer Science and Engineering (IJCSE), Vol - 2, Issue - 5, pp. 738-746, 2011.

[10] S.Kaushik and M.Kaushik, "Analysis of MANET Security, Architecture and Assessment", International Journal of Electronics and Computer Science Engineering, Vol - 1, Issue - 2, pp. 787-793, 2012.

[11] OPNET helps Documentation, OPNET Technologies, Inc., 2008.

[12] P.Mittal, P.Singh, and S.Rani, "Performance Analysis of AODV, OLSR, GRP and DSR Routing Protocols with Database Load in MANET", International Journal of Research in Engineering and Technology (IJRET), Vol - 2, Issue - 9, 2013.

[13] S.Misra, I.Woungang, and S.Misra, "Guide to Wireless Ad Hoc Networks", Springer Science + Business Media, London, 2009.

[14] M.Ilyas, "The Handbook of Ad Hoc Wireless Networks", by CRC Press LLC, Florida, 2003.

[15] S.Dhawan and V.Saroha, "Optimize the Routing Protocol (GRP, OLSR, DSR) Using OPNET and Its Performance Evaluation", International Journal of Advances in Engineering and Technology, India, 2013.

[16] H.kaur and Er. J.Singh, "Performance comparison of OLSR, GRP and TORA using OPNET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol - 2, Issue - 10, 2012.

[17] W.Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Inc., publishing as Prentice Hall, US, 2011.

[18] B.Forouzan, "TCP/IP Protocol Suite", Fourth Edition, McGraw-Hill Companies, Inc., New York,2010.

[19] Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Aruna, "Hybrid Routing Protocols to Secure Network Layer for Mobile Ad hoc Networks" IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-4, 2010.

[20] S.Salim, "Mobile Ad hoc Network Security Issues", University of Central Lancashire, Lancashire, England,2011.