An Efficient Security Aware Routing Protocol for Mobile Ad Hoc Networks

K.VinothKumar, A.Rajaram

Research Scholar, Associate Professor

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) uses security routing scheme for establishing secure route and securely data transmission. The security issues in MANET are mostly concentrated in two parts. The main security threat in MANET is integrity, non-repudiation and privacy. To combat with these security threats, many secure routing protocols has been designed to reduce the security threats in MANET. In this paper we have proposed Privacy Aware Routing Protocol (ESARP) to enhance the security levels in the routing protocol to prevent the network attacks. The proposed work consists of three parts. In the first part each node perform a key exchange operation with its one and two hop distance neighbours, in the second step, secure route establishment and in the third step, secure data communication is performed. Key exchange operation is done in two steps; in the first step, source node (S) exchanges public key (e) with its one hop distance nodes and establish a secret key (SK), and in the second step, source node exchanges public key with its two hop distance nodes and establish a secret key. On establishing the key exchange process node can participate in routing process. In route establishment process, secure route will be established between the sender and receiver. In the third step, sender and receiver will exchange their public key securely and establish a secret key for communication and then data communication is performed.

Keywords

Privacy aware routing, active and passive attacks, integrity, non-repudiation, secret key.

1. INTRODUCTION

1.1. Mobile Ad Hoc Networks (MANETs)

Mobile ad hoc networks consist of wireless hosts that communicate with each other in the absence of a fixed infrastructure. Some examples of the possible uses of ad hoc networking include soldiers on the battlefield, emergency disaster relief personnel, and networks of laptops. Sensor networks are a similar kind of network that have recently been investigated. Nodes in a sensor network are lighter, computationally less powerful, and more likely to be static compared to nodes in an ad hoc network. Hundreds or thousands of such nodes may be placed to monitor and control a physical environment from possibly remote locations. These nodes frequently switch their activity status to preserve battery power, which poses additional challenges for the design of efficient data collection algorithms. Ad hoc and sensor networks are self-organized and collaborative. Due to propagation path loss, the transmission radii are limited. Thus, routes between two hosts in a network may consist of hops through other hosts in the network. The task of finding and maintaining routes in the network is nontrivial since host mobility causes frequent unpredictable topological changes.

1.2 Security issue in Mobile Ad-Hoc Networks

Most routing protocols for Mobile Ad-hoc Networks (MANET) were originally designed without having security in mind. In most of their specifications it was assumed that all the nodes in the network were friendly. The security issue was postponed and there used to be the common feeling that it would be possible to make those routing protocols secure by retrofitting preexisting cryptosystems. Nevertheless, securing network transmissions without securing the routing protocols is not sufficient. Moreover, by retrofitting cryptosystems (like IPSec) security is not necessarily achieved. Therefore, in MANET networks with security needs, there must be two security systems: one to protect the data transmission and one to make the routing protocol secure. There are already well studied point to point security systems that can be used for protecting network transmissions. But there was no much work about how make MANET routing protocols discover routes in a secure manner till recently.

Mobile ad hoc network is not free from different active and passive attacks [1]. Due to the lack of central authority and resource constrains it is much more vulnerable. Depending upon the malicious node location attacks are classified into two different type, namely internal attacks and external attacks. And depending upon the operation it is also classified into two types, namely active attacks and passive attacks [2, 3].

Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself

Manuscript received December 5, 2014
Manuscript revised December 20, 2014

doesn't get affected. Details of different passive attacks in MANET are given below .

a) Eavesdropping: It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes
b) Traffic Analysis and Monitoring: Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks. can be internal or external. Details of different active attacks in MANET are given below [1].

a) Jamming attack: Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.
b) Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.
c) Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.
d) Black hole attack: The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.
e) Byzantine: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.
f) Sybil attack: If a malicious node impersonates some non-existent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack.

2. RELATED WORK

K.Sanzgiri and all; proposed secure routing protocol called ARAN; ARAN is a on-demand secure routing protocol [7]. It detects and protects against authentication, message integrity and non-repudiation. It uses asymmetric key cryptography. ARAN requires trusted certification server, The certificate accommodates the IP address of the node, its public key and a time-stamp of when the certificate was created and a time at which the certificate expires along with the signature by certification authority. But the disadvantages of ARAN is it uses the central authority (Certification Authority) and it can't protect against worm hole attack.

Adrian Perrig and all ; proposed secure routing protocol called ARIADNE, A secure on demand routing protocol for ad-hoc network (ARIADNE) is based on DSR routing protocol, it uses highly eficient symmetric cryptography [8]. It provides point-to-point authentication of a routing packets using a message authentication code (MAC) and a shared key between the two parties. For broadcasting RREQ packets it uses TESLA broadcast authentication protocol. TESLA keys are distributed to the participating nodes via an online key distribution center.

Yih-Chun Hu and all; proposed secure routing protocol called SEAD, Secure Eficient Ad-Hoc Distance Vector (SEAD) is based on destination-sequenced distance vector routing (DSDV) protocol [9].It is a proactive routing protocol. SEAD deals with attackers that modify routing information broadcast during the update phase of the routing information. SEAD makes use of eficient one-way hash chains rather than relying on expensive asymmetric cryptography operations. SEAD does not cope with wormhole attacks.

K.Sanzgiri and all; proposed routing protocol called A Secure Routing Protocol for Ad hoc Networks (SRP), relies on the availability of a security association (SA) between the source node and the destination node [10]. The SA could be established using a hybrid key distribution based on the public keys of the communicating parties. Source and destination can exchange secret key using each others public key [11].

Manel Guerrero Zapata; proposed a routing protocol called Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing, it is a extension of AODV protocol [12]. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and non repudiation. But in ad

hoc network each node will know the others public key its a challenge.

Seung Yi and all; proposed a secure routing protocol called Security-Aware Ad-Hoc Routing (SAR) [13]. SAR is the generalized framework for any on demand ad-hoc routing protocol. SAR uses Key distribution or secret sharing mechanism.SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected.

Panagiotis Papadimitratos and all; proposed secure routing protocol called Secure Link State Routing Protocol (SLSP) [14]. To function efiectively without central key management authority, SLSP enables each node to periodically broadcast its public key to nodes within its zone. To achieve these goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP.

Ranga Ramanujan and all; proposed a secure routing protocol called Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) [15]. TIARA mechanisms protect ad hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on datatrafic which are ow disruption and resource depletion. It requires online public key infrastructure.

Srdjan Capkun and all; proposed secure routing protocol called Building Secure Routing out of an Incomplete Set of Security Associations (BISS) [16]. The sender and The receiver can establish a secure route, even if, prior to the route discovery,only the receiver has security associations established with all the nodes on the location inaccuracy it will disconnect the graph and hence the packets will not be routed thereby decreasing packet delivery ratio. chosen route. It signs the request with its private key and includes its public key PKI in the request along with a certificate signed by the central authority binding its id with PKI.

Frank Kargl and all; proposed secure routing protocol called Secure Dynamic Source Routing (SDSR) Protocol [17]. It is based on DSR routing protocol. It checks the mutable and immutable field of the routing packets. and secure the authenticity of all nodes participating in a route .

A Sivakumar Kulasekaran and all; proposed a secure routing protocol called An eficient secure route discovery protocol for DSR [18]. It uses the peer review process to make to secure routing protocol secure but it uses only DSR routing protocol, packet size of the DSR routing protocol increase on passing by the intermediate nodes.

Phung Huu Phu and all; proposed a secure routing protocol called securing AODV routing protocol in MANET [19]. In this paper, each node tries to establish key exchange in with its neighbour but if any node provides any wrong information then it has to rely on it [20].

Calinescu Gruia; proposed a scheme to compute the two hop distance node in \Computing 2-Hop Neighborhoods in Ad Hoc Wireless Networks", it has been shown that a node can find out its two hop neighbour safe and securely. Bathini Eswar and all; uses two hop distance node to improve AODV Routing protocol [21]

The paper is organized as follows. The Section 1 describes introduction about MANET, Need for security aware routing in MANET. Section 2 deals with the previous work which is related to the security aware routing. Section 3 is devoted for the implementation of security Aware Routing Protocol. Section 4 describes the performance analysis and the last section concludes the work.

3. Implementation of Privacy Aware Routing Protocol

In our proposed protocol, Efficient Security Aware Routing Protocol (ESARP), primary idea is to create a safe and secure path (route) for data communication between nodes. ESARP is a intermediate of AODV and SRP protocol. It follows all the steps of AODV. Unlike DSR, ESARP contains only two address fields in the routing packets where DSR accommodates all the intermediate nodes in the routing packets. The ESARP routing protocol “DA" represents Destination Address, “SA" represents Source Address, “HC" represents Hop Count and “SN" represents Sequence Number. In ESARP, two address fields is required, one is for accommodating super sender of packet with respect to the present node and other is for sender of the packet. We have considered all nodes follows RSA as public key crypto-system and every node has its own public key (e) and private key (d), symmetric key algorithm and hash algorithm. ESARP provides integrity, non-repudiation to the routing packets.

In ESARP, the key idea is to provide security to the routing protocol without the presence of central authority (CA/KDC). Each node in the network negotiates public key with its one hope distance neighbours and two hope distances. neighbours [22] [23]. With the help of public key each node establish a secret key to its one hope and two hopes distance neighbours by RSA public key crypto-system. After completing the negotiation and key agreements nodes are eligible to participate in communication. For data communication sender node initiates the route finding process to reach the destination node by generating and broadcasting route request (RREQ) packet. During the propagation of RREQ packet, each packet is verified by its previous two hope distance sender node and if it is maintained the integrity then the packet to be forwarded to next suitable node in the path. Once RREQ packet reaches the destination and successfully verified, destination node generates route reply packet

(RREP) and propagate it in the same route by following the similar verification process.

Design

The primary goal of ESARP scheme is to guarantee the integrity and non-repudiation of routing messages so that the

protocol can prevent many different kinds of active and passive attacks. Our protocol has three different steps to provide security, in the first stage key agreement process between one hop and two hope distance neighbours, in the second stage route request and route reply, and in the last stage public key exchange between the source and destination node and data communication. Details of the each steps are given bellow.

Key agreement between one hop distance neighbours

In the key agreement between one hop neighbours process, each node sends its public key (es) and a sing of hash of public key (hash(es)ds)to its one hop distance neighbours. Neighbour node receives the request and verify it. After verifying the packet, it generates a reply message which contains the public key (en) and a sing MDC (Modification Detection Code) of public key (hash(en)dn) of itself. After completing the negotiation of public key, initiator node generates a secret key (SK) and send it by encrypting the receiver's public key (encrypten(SK)). The steps are shown bellow, where S represents source node and N1 represents one hop distance node and " " represents direction of communication.

1. S → N1 : <Key Agreement Req,Request Id,Sender Addr,e_S,hash(e_S)^{d}S >
2. N1 → S : <Key Agreement Rep, Request Id,Sender Addr,Neighbour Addr, e_{N1} , hash(e_{N1})d_{N1}>e_S
3. Sender Node (S) generate a secret key (S_K)
4. S → N1 : < Key Offer Req;Request Id; (S_K); hash(S_K) >e_{N1}
5. N1 → S: < Key Offer Rep;Request Id; hashS_K(Request Id) >e_S

Key agreement between two hop distance neighbours

In the key agreement process of two hop distance nodes, each node gather information about the two hope neighbours and sends its public key (eS) and a sing of MDC of public key (hash(es)ds) to its two hop distance neighbours. After receiving the request neighbour node verify it and send acknowledgement, which contains Request Id, Sender and Neighbour address, Public Key(eN2) of itself, a sing of MDC of public key (hash(eN2)dN2) of the neighbour and the sing of MDC of public key (hash(es)ds) of the sender. The detail process are shown bellow, where S represents source node, N2 represents two hop distance neighbor and represents direction of communication.

1. S → N2 : <Key Agreement Req,Request Id,Sender Addr,(eS),hash(e_S)^{d}s) >
2. N2 → S : <Key Agreement Rep,Request Id,Sender Addr,Neighbour Addr,(e_{N2}), hash(eN2)d_{N2} , hash(e_s)^{d}s > e_S
3. Source Node (S) Generate a secret key S_K
4. S →N2 : < Key Offer Req;Request Id; (S_K); hash(S_K) >e_{N2}
5. N2 →S : < Key Offer Rep;Request Id; hashSK(Request Id) > e_S

Route Request

For finding the route, source node, say S generate the route request(RREQ) packet and broadcasts it. RREQ message is propagated by the intermediates nodes until it reaches the destination node (D). After receiving RREQ message, intermediate node (I) checks whether the message needs to be re-broadcast or not. If it is needed to be re-broadcast it sends a message authentication request (unicast) to the super sender of the RREQ message. On receiving the message authentication request, super sender create a MAC (Message Authentication Code) of RREQ message (hashSK(RREQ)) by using the secret key (SK) and encrypting it using the intermediates public key (eI) and then send the entire message (hashSK(RREQ)eI) to the intermediate node. This process continues until the RREQ reaches the destination node.

Lets A, B and C are three consecutive nodes, where A is source and B and C are the intermediate node through which packets are relaid. On receiving the route request, B doesn't check it's integrity because its directly coming from the source node but C will check it by doing following steps.

1. C → A : <RREQ Authen Req, Broadcast Id,Sequence Number,Sender Addr>e_A
2. A → C : <RREQ Authen Rep, Broadcast Id, Sender Addr,Super Sender Addr, hashSK(RREQ)>e_C

Route Reply

On receiving the route request, destination node (D), generates route reply (RREP) message and send it (unicast) through the reverse path of the arrival path. During the propagation of the RREP packet, intermediate nodes check the authenticity and integrity of the route reply message in the similar way of authentication of RREQ message. Let X, Y and D are three nodes where D is destination node, which sending route reply packet through Y and X path. X is te one hop distance node so the there is no need of

checking the integrity of the packet. Y is two hop distance node so it will check the integrity of the message by sending the authentication request. Steps are shown bellow,

1. Y → D : <RREP Authen Req, Broadcast Id, Sequence Number,Sender Addr>e_D

2. D → Y : <RREP Authen Rep, broadcast Id, Sender Addr,Super Sender Addr, hashSK(RREP)>e_Y

Route Maintenance

In route maintenance process, during route finding if destination node is un reachable then a error message (RERR) is generated and propagated to the source node.During the RERR message propagation, it follows the message authentication process. Authentication steps are shown bellow. Let P,Q and R three nodes and R is the error message (RERR) generator, and it will propagate through p and Q nodes, steps are as follows,

1. Q → R : <RERR Authen Req, Host Unreachable Id, Sender Addr>e_R

2. R → Q : <RERR Authen Rep, Host Unreachable Id, Sender Addr,Super Sender Addr, hashS_K(REER)>e_Q

Data Communication Between Source and Destination

Public Key Exchange: Before start data communication source (S) and destination node (D) must know the public key of each other. To exchange the public key we considered the similar to RREQ message authentication process during the propagation of key exchange message

1. S → D : <Destin Addr,(e_S), hash(e_S)>

2. D → S : <Destin Addr,(e_D), hash(e_D)>e_S

Data Packet Exchange: On receiving the public key, source node (S) generate a share key (shK) and encrypt ((shK)ed) it by destinations public key (ed) and sends it followed by the data packet. On receiving the key packet, destination nodes decrypt it and get the shared key. Destination nodes decrypt all rest of the packets by using the shared key. The detail steps are shown bellow.

1. S → D:

{for secret key: < S_K >e_D
{for data packet: < data >S_K

Architecture

To describe the architecture of our proposed we have considered a MANET network, the network consist of {A, B, C,,,,K} nodes.

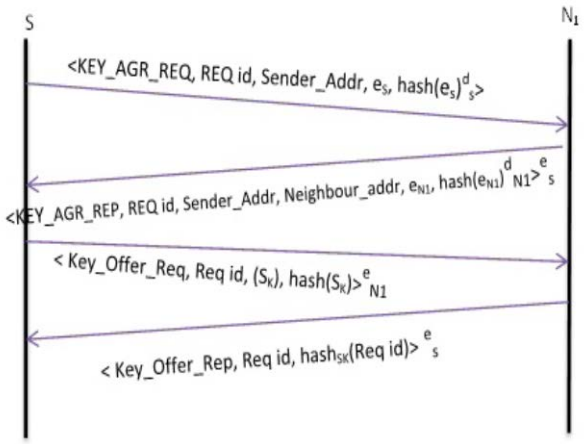

Figure 3.1: Key Exchange Process between one hop distance nodes

We discuss the details of each steps of our proposed routing protocol. In the first step of key exchange operation: each node perform key exchange operation with its one hop distance neighbour nodes; first each node exchange public key and then a shared secret key. The key negotiation process are shown in Figure 3.2 After negotiation and key exchange each node make a entry table, each node maintain a table to keep record of the details of its one hop distance nodes. It keeps the record of Node Id, Public key and Secret key. From the above network (Figure 3.1), we took an example of node "B" and shown the table entry for all of its one hop neighbors.

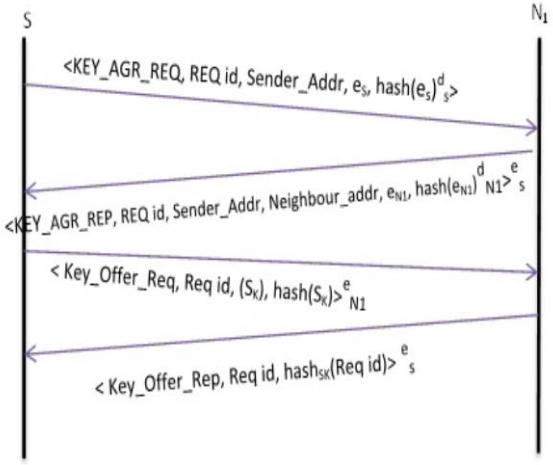

Figure 3.2: Key Exchange Process between one hop distance nodes

Table 3.1 shows the entry for its one hop distance neighbors. In the second step of key exchange operation: each node exchange their public key and a share key with its two hope distance neighbors.

Node ID	Public key(e)	Secret Key (S_K)
A	e_A	S_{K1}
C	e_A	S_{K2}
G	e_A	S_{K3}
H	e_A	S_{K4}

Table 3.1: Key Exchange Process between two hop distance nodes

The details of negotiation and key exchange operation are shown in Figure 3.2, where N1 and N2 represents one and two hop distance neighbour respectively. For each negotiation and key exchange, node will make a entry in the Table. Each node maintain a table to keep record of the details of its two hop distance neighbour nodes. From the above network (Figure 3.2), we took an example of node "C" and makes the table entry for all of it's two hop neighbours, Table 3.1 shows the entry for it's two hop distance neighbours. RREQ and RREP packet forwarding:
In the network (Figure 3.2), if node A, wants to send the data to node F, then route request (RREQ) packet is to be generated and broadcast to find the route to reach the destination.

Table 3.1: Table entries for two-hop nodes

Node I.D	Intermediate Node	Public Key (e)	Secret Key (S_K)
A	B	e_A	S_{K1}
G	B	E_G	S_{K2}
H	B	E_H	S_{K3}
E	D	e_E	S_{K4}
I	D	e_I	S_{K5}
K	D	e_K	S_{K6}

During the propagation of RREQ packet each time it will be reviewed by it two hop distance away sender. If is satisfy the review process then only it will be propagated to the farther nodes. The process are shown in Figure 3.2. Similarly, during route reply and route maintenance each RREP and RERR packet will be verified by peer review process by it two hop distance sender. Figure 3.2 shows the detail of route reply process.

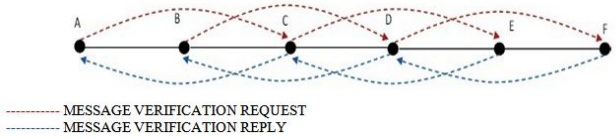

Figure 3.3: Peer Review process of RREQ packet

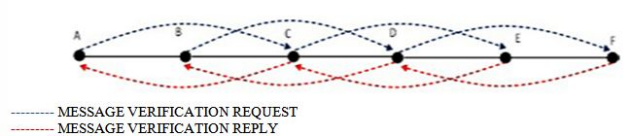

Figure 3.4: Peer Review process of RREP packet

In this chapter each steps of design and architecture of our proposed ESARP protocol are carefully shown. It preserves integrity, non-repudiation and confidentiality of Routing packets as well as data packets

4. PERFORMANCE ANALYSIS

In this section, we have compared our proposed routing algorithm with the popular existing routing algorithm. we have taken some security threats and analyse those security threats in our proposed routing protocol with the existing secure routing protocols.

Comparison with other secure routing protocols

We have compared our proposed (ESARP) protocol with the existing popular routing protocols. The comparison is based on security threats, encryption algorithm, MANET Protocol are shown in Table 4.1. In comparison we have shown our proposed protocol is providing integrity, non-repudiation and confidentiality but the central advantage of our protocol is it doesn't need any central authority.

Table 4.1: Comparison between ESARP and other existing secure routing protocols

Protocol	ARAN	ARIADNE	SEAD	ESARP (Proposed)
Encryption Algorithm	Asym metric	Sym metric	Sym metric	Asym metric
Protocol	AODV/DSR	DSR	DSDV	AODV/ DSR(Modified)
Central Trust Authority	Certificate Authority (CA)	Key Distribution Center (KDC	Certificate Authority (CA)	No Central Authority
Authentication	YES	YES	YES	YES
Confidentiality	YES	NO	NO	YES
Integrity	YES	YES	NO	YES
Non-Repudiation	YES	NO	NO	YES
Black-hole Attacks	NO	NO	NO	NO
Dos Attacks	NO	YES	YES	NO

Average Transmission Delay Comparison

In this section we have compared our secure routing protocol with AODV routing protocol with respect to the average end-to end transmission delay. We have considered 15 node in the area of 500m X 500m. We have considered the channel bandwidth is 11 Mbps and packet size 512 KB. We have simulated the our algorithm with 50, 100,150 and 200 number of packets and took average of it.

Figure 4.1 shows the bar graph of average packet transmission delay vs number of packet.

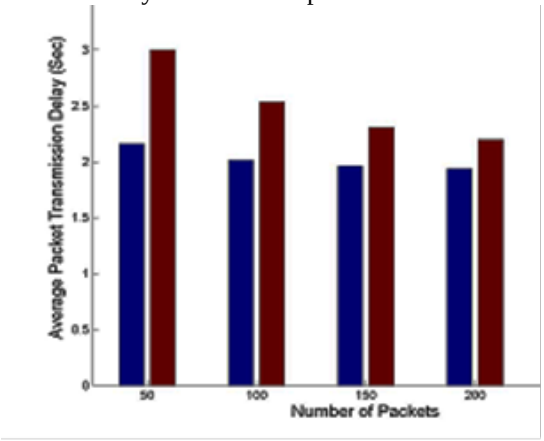

Figure 4.1 shows the bar graph of average packet transmission delay vs number of packet

5. CONCLUSION

Security in routing protocol in MANET is very essential. No existing secure routing protocol is fully capable of preventing all security threats. The security issues in MANET are mostly concentrated in two parts, establishing secure route and securely data transmission. The main security threats in MANET are integrity, non-repudiation and privacy. To combat with these security threats, many secure routing protocols has been designed to reduce the security threats in MANET. In this paper we have proposed an Efficient Security Aware Routing Protocol (ESARP)" to enhance the security levels in the routing protocol to prevent the network against active and passive attacks without the presence of central authority. A peer review process has been introduced to check the integrity and non-repudiation of the routing packets and key exchange packets. In the first step each node will exchange keys with their neighbours, in the second step routing packet delivery is done by the peer review process and in the final stage data delivery is done by encryption/decryption mechanism using session key.

REFERENCES

[1] Sudhir Agrawal, Sanjeev Jain, and Sanjeev Sharma. A survey of routing attacks and security measures in mobile ad-hoc networks. arXiv preprint arXiv:1105.5623, 2011.

[2] POWAH YAU, Shenglan Hu, and Chris J Mitchell. Malicious attacks on ad hoc network routing protocols. Information Security Group.

[3] Djamel Djenouri, L Khelladi, and N Badache. A survey of security issues in mobile ad hoc networks. IEEE communications surveys, 7(4), 2005.

[4] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, pages 90{100, 1999.

[5] David B Johnson, David A Maltz, Josh Broch, et al. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5:139{172, 2001.

[6] Ranvijay Karan Singh, Rama Shankar Yadav. A review paper on ad hoc network security. International Journal of Computer Science and Security, 1(1), 2009.

[7] K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. Authenticated Routing for Ad Hoc Networks. Selected Areas in Communications, IEEE Journal, 23(3):598{610, 2005.

[8] Adrian Perrig Yih-Chun Hu and David B. Johnson. Ariadne:a secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11(1-2):21{38, 2005.

[9] Yih-Chun Hu, David B Johnson, and Adrian Perrig. Sead: Secure e_cient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1):175{192, 2003.

[10] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, pages 78{87, 2002.

[11] Hamed Jalali Qomi and Mohammad Hesam Tadayon. Securing routing protocols against active attacks in mobile ad hoc networks. International Journal of Computer Technology and Applications, 2(5):1667{1673, 2011.

[12] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3):106{107, 2002.

[13] Seung Yi, Prasad Naldurg, and Robin Kravets. Security-aware ad hoc routing for wireless networks. In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, pages 299{302. ACM, 2001.

[14] Panagiotis Papadimitratos and Zygmunt J Haas. Secure link state routing for mobile ad hoc networks. In Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pages 379{383. IEEE, 2003.

[15] Ranga Ramanujan, Atiq Ahamad, Jordan Bonney, Ryan Hagelstrom, and Ken Thurber. Techniques for intrusion-resistant ad hoc routing algorithms (tiara). In MILCOM 2000. 21st Century Military Communications Conference Proceedings, volume 2, pages 660{664. IEEE, 2000.

[16] Srdjan _Capkun and Jean-Pierre Hubaux. Biss: building secure routing out of an incomplete set of security associations. In Proceedings of the 2nd ACM workshop on Wireless security, pages 21{29. ACM, 2003.

[17] Frank Kargl, Alfred Geis, Stefan Schlott, and Michael Weber. Secure dynamic source routing. In System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on, pages 320c{320c. IEEE, 2005.

[18] Kulasekaran A Sivakumar and Mahalingam Ramkumar. An e_cient secure route discovery protocol for dsr. In Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE, pages 458{463. IEEE, 2007.

[19] Phung Huu Phu, Myeongjae Yi, and Myung-Kyun Kim. Securing aodv routing protocol in mobile ad-hoc networks. In Active and Programmable Networks, pages 182{187. Springer,2009.

[20] Pushpita Chatterjee. Trust based clustering and secure routing scheme for mobile ad hoc networks. International

Journal of Computer Networks and Communications, 1(2), 2009.

[21] Gruia Calinescu. Computing 2-hop neighborhoods in ad hoc wireless networks. In Ad-Hoc,Mobile, and Wireless Networks, volume 2865 of Lecture Notes in Computer Science, pages 175{186. Springer Berlin Heidelberg, 2003.

[22] Gruia Calinescu. Computing 2-hop neighborhoods in ad hoc wireless networks. In Ad-Hoc,Mobile, and Wireless Networks, volume 2865 of Lecture Notes in Computer Science, pages175{186. Springer Berlin Heidelberg, 2003.

[23] Eswar Bathini and Roger Lee. Using dominating sets with 2-hop neighborhood information to improve the ad-hoc on-demand distance vector routing. In Roger Lee, editor,Computers,Networks, Systems, and Industrial Engineering 2011, volume 365 of Studies in Computational Intelligence, pages 1{9. Springer Berlin Heidelberg, 2011.