Integrated MANET Mutual Authentication System- A Review

*Ayushi Singhal[1], Amrendra Singh Yadav[2], Mayank Deep Khare[3], Rahul Kumar Sharma[4]
Department of Computer Science & Engineering
Noida Institute of Engineering & Technology Greater noida (U.P)
zealous.ayushi@gmail.com[1], yadavamrendrasingh@gmail.com[2],
mayankdeepkhare20@gmail.com[3], rahulsharma9045@gmail.com[4]

Abstract- **The Integrated MANET Mutual Authentication System (IMMAS) provides an implied mutual authentication of all routing and data traffic with in a Mobile Ad-hoc Network (MANET) by combining Elliptic Curve Cryptography a public-key crypto-system, with the MANETs Routing Protocol. IMMAS provides security by effectively hiding network topology from adversaries while reducing the potential for, among other things, traffic analysis and data tampering, all while providing a graceful degradation for each of the authentication components. Current research in MANET's tends to focus primarily on routing issue leaving topics such as security and authentication for future research. IMMAS focuses on achieving a higher level of security with the potential for substantial increases in efficiency of processing power and bandwidth compared to alternative exterior mechanism tacked on after protocol development and Standardization.**

Keywords- **MANET, AODV, IMMAS, RSA, ECC DSR, DSDV, OLSR, ZRP.**

I. INTRODUCTION

Due to recent advancement in computer technologies and wireless communication technologies, mobile wireless computing is become increasingly widespread. One type of network that is quickly evolving is the Mobile Ad-Hoc Network [1,2] (MANET). Unlike other mobile network paradigm, such as cell phone network with fixed radio station and centrally access routers and servers, MANETs have dynamically, rapidly-changing, random multi-hop topologies composed of bandwidth constrained wireless link with no centrally access to routers and servers. A MANET seek to take computing resources ranging from pocket sized wireless Personal Digital Assistance (PDA) to full size wireless network capable computers and expand the capabilities provided on the current wired Local Area Network (LAN). This will be performed even as these computers may be travelling in vehicles or aircraft with little or no fixed routers or infrastructure available.

*Author for correspondence

ROUTING IN MANET

Routing protocols [3] tells the way how a message is sent from source to destination. The mobile assumption implies a routing protocol that reacts speedily to topology changes. Routing is the process of moving information across an introduction from a source to destination. Routing involves basic activities- (i) Determining a node location. (ii) Determining optimal routing paths and packets switching. (iii) Nodes are mobile at both micro and macro scales. Optimality of the path can be described using various metrics like, number of hops, traffic, etc. As the network grows, various routing protocols perform differently. The amount of routing traffic increases as the network grows. An important measure of the scalability of the protocol, and thus the network, is its routing overhead. It is defined as the total number of routing packets transmitted over the network, expressed in bits per second or packets per second. In ad-hoc network each node acts as specific router itself. In mobile ad-hoc network the routing mostly done with help of routing tables.

There are several kinds of routing protocols for wireless ad-hoc networks. According to the routing strategy, the routing protocol can be categorized as proactive and reactive routing protocol. The ad-hoc routing protocol using combination of both proactive and reactive is called hybrid routing protocol.

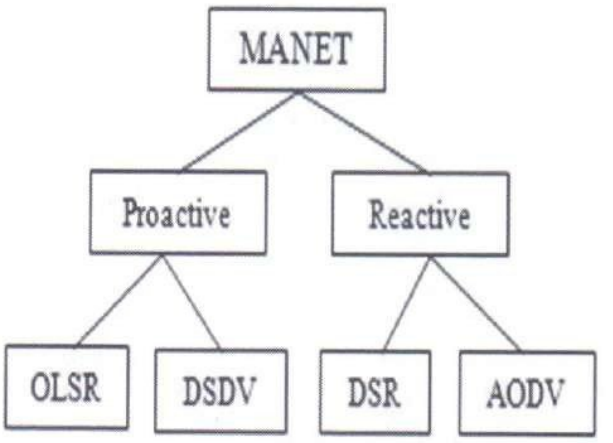


Fig 1

II. PROACTIVE ROUTING PROTOCOLS

Proactive routing protocol is also called "table driven" routing protocol. A proactive routing approach every node always maintains completes routing information of the network. Using a proactive routing protocol, nodes in a mobile ad-hoc network continuously evaluate routes to all reachable node sand attempts to maintain consistent, up-to-date routing Information. Therefore, a source node can get a routing path immediately if it needs one. When a network topology change occurs, respective updates must be propagated throughout the network to notify the change. So if we noted to network topology changes in MANETs, the control overhead to maintain up-to-date network topology information is relatively high. This is achieved by flooding network periodically with network information to find out any possible change in network topology. Examples of Proactive Routing Protocols are: Destination Sequenced Distance Vector Routing (DSDV) [4], OLSR (Optimized Link State Routing) [5]. When there is any requirement to send packet to any other mobile node in the network, therefore quick response to application program. But consume lots of network resources to maintain up-to –date status of network graph.

A. DSDV (Destination Sequenced Distance Vector)

The first MANET algorithm that we implemented as part of this work is called the Destination-Sequenced Distance Vector (DSDV) routing algorithm. It is a proactive routing algorithm. The DSDV algorithm is a Distance Vector (DV) based routing algorithm designed for use in MANETs, which are defined as the cooperative engagement of a collection of Mobile Hosts without the required intervention of any centralized Access Point (AP). Every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the next hop neighbor to reach the destination node, the timestamp of the last update received for that node. The DSDV update message considering three fields, Destination Address, Sequence Number and Hop Count. Each node uses 2 mechanisms to send out the DSDV updates. They are,

a) *Periodic Updates*- Periodic updates are sent out after every m periodic Update Interval (default: 15s). In this update the node broadcasts out its entire routing table.

b) *Trigger Updates*- Trigger Updates are small updates in-between the periodic updates. These updates are sent out whenever a node receives a DSDV packet that caused a change in its routing table. The original paper did not clearly mention when for what change in the table should a DSDV update be sent out. The current implementation sends out an update irrespective of the change in the routing table.

B. OLSR (Optimized Link State Routing)

The Optimized Link State Routing Protocol (OLSR) is developed for mobile ad hoc networks. It operates as a table driven and proactive protocol, thus exchanges topology information with other nodes of the network regularly. The nodes which are selected as a multipoint relay (MPR) by some neighbor nodes announce this information periodically in their control messages. Thereby, a node announce to the network, that it has reach ability to the nodes which have selected it as multipoint relay. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. The protocol uses the MPRs to facilitate efficient flooding of control messages in the net- work This Multipoint relay selector is obtained from HELLO packets sending between in neighbor nodes. These routes are built before any source node intended to send a message to a specified destination. Each and every node in the network keeps a routing table. This is the reason the routing overhead for OLSR is minimum than other reactive routing protocols and it provide a shortest route to the destination in the network. There is no need to build the new routes, as the existing in use route does not increase enough routing overhead. It reduces the route discovery delay. Nodes in the network send HELLO messages to their neighbors. These messages are sent at a predetermined interval in OLSR to determine the link status. A node chooses minimal number of MPR nodes, when symmetric connections are made. Symmetric connection is the one in which participating devices can send and receive message from each other.

III. REACTIVE ROUTING PROTOCOLS

Reactive routing protocols are more popular routing algorithms and are known as "on-demand" protocols, In a reactive routing protocol, routing paths are searched only when needed. When a source node wants to send packets to the destination but no route is available, it initiates a route discovery operation. In the route discovery operation, the source broadcasts route request (RREQ) packet. When the destination or a node that has a route to the destination receives the RREQ packet, a route reply

(RREP) packet is created and forwarded back to the source. Each node commonly uses hello messages to notify its existence to its neighbors. Therefore, the link status to the next hop in an active route can be monitored. When a node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbors, which in turn propagates the RERR packet towards nodes whose routes may be affected by the disconnected link. Then, the affected source can re-initiate a route discovery operation if the route is still needed. Compared to the proactive routing protocols, less control overhead is a distinct advantage of the reactive routing protocols. Thus, reactive routing protocols have better scalability than proactive routing protocols. DSR[6] and AODV[7] are main reactive routing protocols.

A. DSR (Dynamic Source Routing)

Dynamic Source Routing (DSR) protocol is a reactive routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR operates on an on-demand behavior. Therefore, our DSR model buffers all packets while a route request packet (RREQ) is disseminated. We implement a packet buffer in dsr-rsendbuff.cc. The packet queue implements garbage collection of old packets and a queue size limit. When the packet is sent out from the send buffer, it will be queued in maintenance buffer for next hop acknowledgment Pass. These routes are stored in node memory called direction cache. It provides an advantage that intermediate hops need not to maintain routing information in order to route the packets as packets already contain routing information.

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery[8] is used only when S attempts to send a packet to D and does not already know a route to D. It determines path(s) for a communication between a source node and target node. Route discovery uses two messages' i.e. route request (RREQ) and route reply (RREP). When a node needs to send a message to some destination, it broadcast the RREQ packet in the network. The neighbor nodes in the broadcast range receive this RREQ message and add their own address to the packet header and rebroadcast it in the network until destination is reached. In the case if the message did not reached to the destination then the node which received the RREQ packet will look for any previously used route for the specific destination. Each node maintains its route cache which is kept in the memory for the discovered route. The node will check its route cache for the desired destination before rebroadcasting the RREQ message. If a route is found in that node route cache do not rebroadcast the RREQ in the whole network. So it will forward the RREQ message to the destination node. The first message reached to the destination has full information about the route. That node will send a RREP packet to the sender having complete route information.

Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D. If a node along the path of a packet detects an error, the node returns a route error (RERR) packet to the sender. When a route error packet is received, the hop in error is removed from any route caches and all routes which contain this hop are truncated. A route error packet can be returned to the sender by following ways: In case of bidirectional links- reverse the route contained in the packet from the original host. In case of unidirectional links- Salvage, Gratuitous route repair, Promiscuous listen methods are used. Use of DSR makes the network completely self-organizing and self-configuring, as it do not require any existing network infrastructure or administration.

B. AODV (Ad-hoc on-demand Distance vector)

AODV is an on –Demand routing protocol which is confluence of DSDV and DSR. Route is calculated on demand, just as it is in DSR via route discovery process. AODV is a Reactive Routing Protocol. Therefore, routes are determined only when needed. Whenever an AODV router or node receives a request to send a message, it checks its Routing Table for route existence. Each Routing Table entry consists of Destination Address, Next Hop Address, Destination SN and Hop Count. If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a message queue and then it initiates a route request to determine a route. Upon receipt of the Routing information, it updates its Routing Table and sends the queued message(s). However, AODV maintains a routing table where it maintains one entry per destination unlike the DSR that

maintains multiple route cache entries for each destination. AODV provides loop free routes while repairing link breakages but unlike DSDV, it does not require global periodic routing advertisements. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. AODV nodes use four types of messages: Route Request (RREQ), Route Reply (RREP), Route Error (RERR) and HELLO. First two messages are used for route discovery and last two messages are used for route maintenance.

RREQ - *A route request message* is transmitted by a node requiring a route to a node. As an optimization AODV uses an *expanding ring* technique when flooding these messages. Every RREQ carries a *time to live* (TTL) value that states for how many hops this message *should be* forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted should be buffered locally and transmitted by a FIFO principal when a route is set.

Source Address	Request ID	Destination Address	Source Sequence	Destination Sequence	Hop count

RREP - *A route reply* message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

Source Address	Destination Address	Destination Sequence	Hop Count	Life Time

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

HELLO – It is used to detect and monitor links to neighbors. In HELLO messages each active node periodically broadcasts a HELLO message that is received by its all neighbors. If a node fails to receive several HELLO messages from a neighbor, a link break is detected.

IV. HYBRID ROUTING PROTOCOL

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. It requires less memory and processing power than LSRP. ZRP (Zone Routing Protocol) is the example of hybrid protocol.

A. ZRP (Zone Routing Protocol)

ZRP was designed to speed up delivery and reduce processing overhead by selecting the most efficient type of protocol to use throughout the route. ZRP uses IARP as pro-active and IERP as reactive component. Intra-zone Routing Protocol (IARP) is used inside routing zones but Inter-zone Routing Protocol (IERP) is used between routing zones. IARP uses a routing table. Since this table is already stored, this is considered a proactive protocol. IERP uses a reactive protocol. Any route to a destination that is within the same local zone is quickly established from the sources proactively cached routing table by IARP. Therefore, if the source and destination of a packet are in the same zone, the packet can be delivered immediately.

V. PROBLEM DEFINITION

In a Manet, there are no central servers or routers from which trusted information can be obtained or that can be used to ensure data can be properly routed or received. These functionality must be obtained from the trusted corporation of nodes with in Manet. However for Manet nodes to trust other nodes and co-operate with them, they must be able to authenticate each other as valid and trusted nodes. Achieving this authentication for data transmission with in a MANET is a significant problem. Mutual authentication ensures that good authentication is established in both directions, that is, for sending nodes and receiving nodes. This paper address the problem of mutual authentication and security within a Manet and cost associated with incorporating the public key cryptography in routing protocols.

A.Goals and hypothesis

The primary goals of this paper are:

1. Develop an efficient mutual authentication system

2. Determine what performance impact the authentication has on the manet.

It is hypothesized that incorporating authentication and

high level of authentication and security while maintaining a adequate "GOOPUT RATIO" as well as acceptable end-to-end delay of packets. Goodput ratio is defined as ratio of data bits successfully received, dbr, to all routing overhead bit's are transmitted, rbt, plus the data bit's successfully received or

$$\frac{dbr}{rbt + dbr}$$

B. Approach

To accomplish stated goals above, following steps are needed:

1. Select a representative Manet routing protocols.
2. Perform verification and validation.
3. Complete a baseline performance analysis.
4. Develop a new protocol with authentication and security built in.
5. Present analysis and conclusion.

C. System boundaries

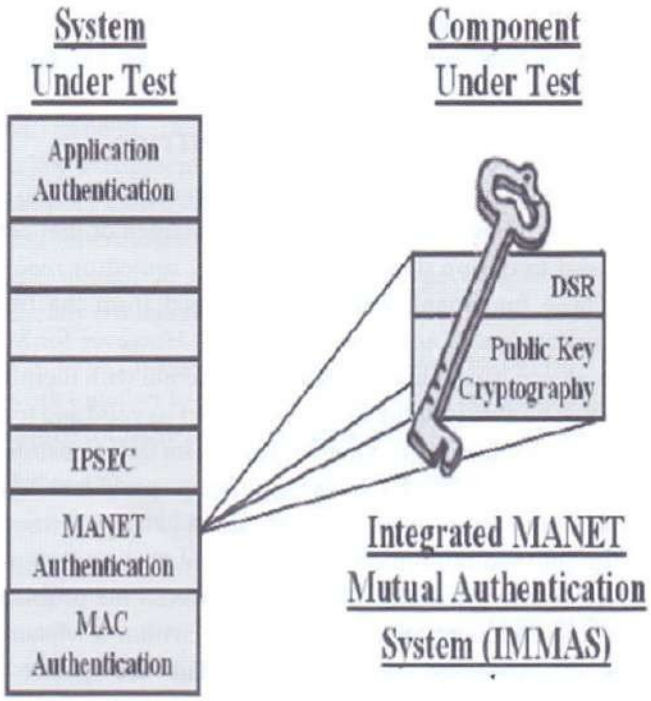


Fig. 2 Methods of Authentication for Manet

As depicted in fig.2 the System Under Test (SUT) for this study includes all authentications involved in a Manet node. This includes the authentication mechanism and system used by the applications, Internet Protocol (IP), the routing protocol, as well as Medium Access Control (MAC) Protocol. This approach produced an System (IMMAS).

D. System services

Authentication is one of the several services that must be offered by a network for it to be considered to be secure [08]. IMMAS enable a node to verify the identity of a peer node from whom it communicating. The primary service and their respective outcome include:

1. Peer Authentication.

Success : Packet received from valid network node (packet accepted).

Failure : Unable to establish that packet come from valid network node (packet dropped).

2. Routing Authentication.

a. Success: Packet forwarded by valid node.

b. Failure: Unable to establish that packet forwarded by valid node.

3. Payload authentication:

a. Success: Packet payload from valid network node.

b. Failure: Unable to establish that packet come from valid network node (packet dropped).

E. Performance Metrics

The performance is depending on following metrics:

Throughput: is defined as $S = \frac{b_{tx}}{t \times N}$ where S is the throughput in bits per second per node, b_{tx} is the no. of successfully transmitted bits, t is the observation period, and N is the no. Nodes in the Manet.

Goodput Ratio: Goodput ratio is defined as G= $\frac{db_{rx}}{rb_{tx} + db_{rx}}$ where is the ratio, *dbrx* is the total no. Bits received successfully, and rb_{tx} is the total no. of routing bits transmitted.

3. *End to End Delay:* ETE delay is measured in seconds. It is defined to be elapsed time from when a packet arrives at the source node's routing layer to when the packet is received by the routing layer to destination node.

F. Factors

The following factors and their corresponding level considered as most significant for this paper:

1. Authentication system:

a. No Authentication: this provided baseline analysis performance for routing protocols.

b. IMMAS using ECC: IMMAS implemented with

Elliptic Curve Cryptography using a key strength of 160 bits.

c. IMMAS using RSA: IMMAS implemented with RSA using a key strength of 1024 bits.

2. *Number of MANET source node:*

a. Lightly loaded Manet: it contains 20 source nodes.

b. Heavily loaded manet: it contains 30 source nodes.

3. *Manet node Mobility:*

a. Low Mobility: node moving with a pause time of 300 seconds.

b. Medium Mobility: node moving with a pause time of 60 seconds.

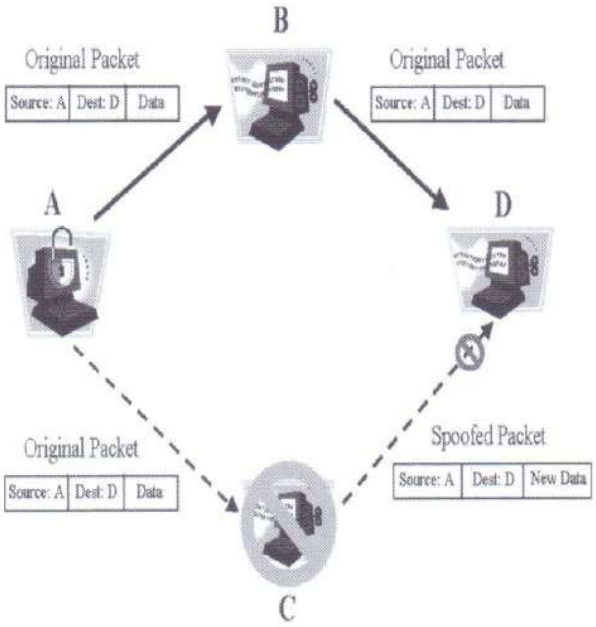
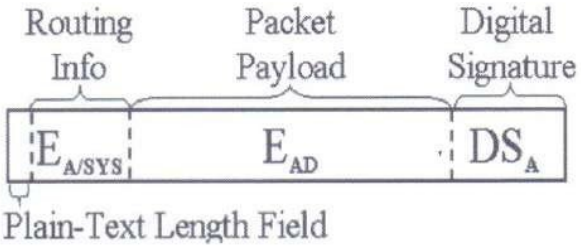


Fig 3. Mutual Authentication

Node A wants to send an authentication message to need D



via route A-B-D. Prior to accepting the message, node D must be sure it is truly from Node A and it cannot be tampered with by node B or C. Conversely, node A must also be assure that node D will receive the message unaltered by nodes B or C to achieve mutual authentication between nodes A and D.

To get to node D, the message must pass through node B.

c. High mobility: node moving with a pause time of 0 seconds (constant mobility).

VI. IMMAS implementation

In a Manet, there are no central servers or routers from which trusted information can be obtained so that sender is not ensure that data can be properly routed or received. These functions must be obtained from the trusted corporation of nodes with in Manet. "Good" authentication provides evidence of particular secret without having revealed the secret [09]. Consider the scenario in fig 3: node.

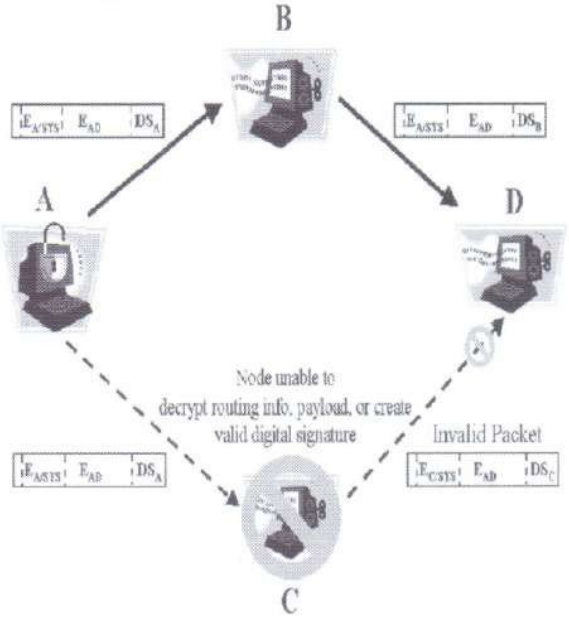


Fig 4. IMMAS Implementation

For security reasons, node A must be able to authenticate that node B is a valid MANET node and that only node B can route data to D using the source route of A-B-D. Node B must be assured the message received came from node A, that node A is a valid MANET node, and that node A is either the source of the packet or in the source route for the packet.

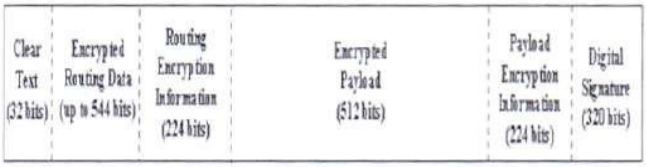
To accomplish this, node A,B and D must have some secret that can be used to create shared secrets for node pairs (A,D),(A,B) and (B,D) such that only receiver nodes can verify the sender node's secret was used to create the shared secret all without having to know what the sender node's secret is. This process will provide the Mutual Authentication between each pair of nodes along the route as well as mutual authentication between the source and destination nodes.

1. IMMAS with Elliptic Curve Cryptography (ECC)

To illustrate how IMMAS work's consider fig 4 Where node A wants to send a packet to node D.

A. Node A uses Elliptic Curve Integrated Encryption Scheme (ECIES) [10] to encrypt the payload data using its private key and node D's public key. This is shown in as E_{AD} in

Fig 5.Fig.5. Generic IMMAS packet



B. The Elliptic Curve Signature Scheme with Appendix (ECSSA) [10,11] is applied to the entire packet which produce node A's 320 bit digital signature for that packet. This signature is appended to the end of the packet (DSA).

C. The routing information except for the first $ octets, is encrypted with Node A's private key and the system public key (EA/SYS). This is a known security risk since every node within a MANET has a copy of both the system private and public keys as well as Node A's public key. However, since this information still does not decrypt the payload it is a manageable risk.

The first 4 Octets of the routing protocol header remained unencrypted since they contain the payload length field. This information is needed by the receiving nodes to properly decrypt the header.

IMMAS allow only nodes belonging to the MANET to decrypt the plaintext routing information. Throughput this process, no node other than the destination can decrypt and read the payload data. As the packet shown

Fig 7.4 IMMAS packet Transmitted by Node A

1. The packet routing information is decrypted using node A's public key and the system's private key to gain the plaintext routing information ®, as shown in Figure 6. If node B is not in the source route the packet is dropped.

Fig.6 Node B Decrypts IMMAS Packet Routing Information

2. The digital signature at the end of the packet is achieved to verify that the packet came from node A. If this fails the packet is dropped and ignored.

3. If the packet header has information pertaining to node B, such as a route request or passing a data packet, it is processed accordingly and the appropriate header fields are updated.

4. Node b produces its digital signature for the packet and overwrite node A's digital signature at the end of the packet as shown in Fig.7

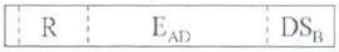


Fig.7 Node B overwrites IMMAS packet Digital Signature

5. Node B re-encrypts the header, Minus the first 4 Octets with its private key and the system public key as shown in fig 8

Fig.8. IMMAS Packet Transmitted by Nodes

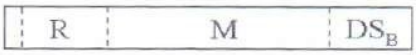
6. The packet is then transmitted to node D.

Node D will process the packet as follows-

a. The packet is received and the routing information decrypted using node B's public key and the system's private key to gain the plain text routing information (R) as seen in Fig 9. If node D is not in the in the source route the packet is dropped.

Fig 9 Node D Decrypts IMMAS Packet Routing Information

b. The Digital Signature at the end of the packet is checked to verify that the packet came from node B. If this fails,



the packet is dropped and ignored.

c. Since node D is the destination the packet payload is then decrypted with A's public key and D's private key to gain back the original plaintext message (M) as seen in Fig.10

VII. IMMAS Security Options

The Integrated MANET Mutual Authentication System provides various level of security shown in Figure8.1.

Each level considered optional for implementation based on assessed security risk of the network. These security levels are all based on the assumption that some type of trusted

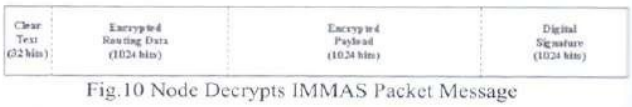


Fig.10 Node Decrypts IMMAS Packet Message

A. The packet is then processed by D accordingly. Fig.11 IMMAS packet using Elliptic Curve Cryptography

As described above, the 2 encryption and 1 digital

signature will produced a total of 768 bits of overhead 150% of a 64 byte data packet. However, this cost is far below the 1024-bit overhead for each encryption of the RSA algorithm.

B. IMMAS with Rivest, Shamir, Adleman (RSA) Cryptography

RSA Cryptography is implemented just like the ECC Cryptography in IMMAS except that the final size of the field will be different. According to RSA [11], with a 1024-bit key strength, will produce 1024 bits for every 696 bits of data to be encrypted. Thus

IMMAS will produce data packets like Fig 7.11 for 512 bits (64byte) data packet as was implemented in this research. So in the case of IMMAS using RSA the final size of a data packet will be 3072 bits-a 600% increase in the size of the data packet.

certificate authority is available for the key generations and a secure method of key generations and management are applied. These areas will be addressed in future research, but for this they will be assume.

For routing packets, only the digital signature and routing encryption overhead is added to the packet since there is no data payload. This research uses the IMMAS system with all options to give a worst case scenario on results and

IMMAS Option	Security Level	Security Effects
No IMMAS System	Low	No Authentication or Security Provided
A	Low/Medium	Payload Security / No Authentication
B	Low/Medium	Peer Authentication / No Security
C	Low/Medium	Routing Security / No Authentication
A & B	Medium	Payload Security and Peer Authentication / No Routing Security
A & C	Medium	Payload and Routing Security / No Authentication
B & C	Medium	Routing Security and Peer Authentication / No Payload Security
A & B & C	Medium/High	Security and Authentication Provided

A = Payload Encryption
B = Digital Signatures
C = Routing Encryption

Fig12. IMMAS Implementation using RSA Cryptography

to provide what is believed to be an adequate level of security.

For routing packets, only the digital signature and routing encryption overhead is added to the packet since there is no data payload. This research uses the IMMAS system with all options to give a worst case scenario on results and to provide what is believed to be an adequate level of security.

For routing packets, only the digital signature and routing encryption overhead is added to the packet since there is no data payload. This research uses the IMMAS system with all options to give a worst case scenario on results and to provide what is believed to be an adequate level of security.

VIII. CONCLUSIONS AND FUTURE WORK

Security and authentication of transmitted data within a MANET are of utmost importance. Elliptic Curve Cryptography Integrated into the MANET routing protocols provides an efficient means to produce the required level of security and authentication desired by most any mobile organization. IMMAS provides mutual authentication and security while not overtaxing the processing and bandwidth capabilities of wireless network. In addition to mutual authentication, IMMAS also provides Multi-level encryption which ensures the integrity, confidentiality, and non-repudiation for data packets every step along the way. The security provided by IMMAS makes an effective and efficient use of routing protocols and Elliptic Curve Cryptography. IMMAS using ECC provides the same level of authentication and security with the least expensive cost for this security compared to IMMAS using RSA.

Future Research needs to be done in four broad areas:

- Key Distribution and Management for MANET's.
- Encryption processing requirements for MANET's.
- Testing other authentication system using MANET Routing Protocols.
- Researching the effects of IMMAS with other MANET routing Protocols.

REFERENCES

[1] C. Perkins, Ad Hoc Networking, New York: Addison Wesley, 2000.

[2] C. K. Toh, Ad Hoc Mobile Wireless Networks Protocols and Systems, New Jersey: Prentice Hall, 2002.

[3] E.M Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," *IEEE Pers. Comm. Mag, 1999.*

[4] C. E. Perkins and Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–44.

[5] P. Jacquet et al., "Optimized Link State Routing Protocol for Ad Hoc Networks," Proc. 5th IEEE Multi Topic Conf. (INMIC 2001), 2001.

[6] C. E. Perkins, E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.

[7] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in ad hoc Wireless Networks," Mobile Computing, Kluwer Academic Publishers, 1996, vol. 353, pp. 151.

[8] C. Perkins and P. Bhagwat, "Routing over Multi-hop wireless Network of Mobile Computers," SIGCOMM '94, Computer Commun. Review, vol. 24, no. 4, Oct. 1994, pp. 234–44.

[9] Patiyoot, D. and S.J Shepherd. Authentication Protocols for wireless ATM Networks. In First, IEEE International Conference on ATM, 1998.

[10] IEES Standard Dept. IEEE STD 1363-200 Standard Specification for Public Key Cryptography. Institute of Electrical and Electronics Engineers Inc., New York, August 2000.

[11] IEEE Standard Dept. IEEE P1363a/D9 (Draft Version 9) – Standard Specification for Public Key Cryptography: Additional Techniques. Institute of Electrical and Electronics Engineers Inc. , New York, August 2001.

[12] Zhou, Lidong and Zygment J.Haas. Securing Ad-Hoc Networks. IEEE Network, December 1999.

Ayushi Singhal is Assistant Professor of Computer Science & Engineering at Noida Institute of Engineering & Technology, Greater Noida. She recieved his Masters degree in Infomation Technology from Madan Mohan Malaviyan University of Technology, Gorakhpur (U.P) Her Research interests include Mobile ad-hoc network, wireless sensor network. She has three research papers in national and international journals and conference.

Amrendra Singh Yadav is Assistant Professor of Computer Science & Engineering at Noida Institute of Engineering & Technology, Greater Noida. He received his Masters degree in Information Technology from Madan Mohan Malviya University of Technology, Gorakhpur (U.P) His Research interests include Mobile ad-hoc network, wireless sensor network. He has five research papers in national and international journals and conference.

Mayank Deep Khare completed M. Tech (Information Technology) from Madan Mohan Malviya University of Technology, Gorakhpur in 2015. He is working at NIET, Greater Noida for last one year as Assistant Professor in department.

Rahul Kumar Sharma completed M Tech (Computer Science) from Madan Mohan Malviya university of Technology, Gorakhpur in 2015. He is working at NIET, Greater Noida for last one year as a dynamic, successful and responsible faculty