ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (49-54), Month: July - September 2015, Available at: www.researchpublish.com

An Approach to Preserve Anonymity for Security Enhancement in Mobile Ad Hoc Networks

Ramya K M[1], K N Rama Mohan Babu[2]

[1]M.Tech Student, [2]Professor, [12]Dept. of I.S.E, Dyananda Sagar College of Engineering Bangalore, India

Abstract: **Accomplishing anonymity in MANETs (Mobile Ad Hoc Networks) for secure and efficient routing plays a vital role in sensitive data communication. Anonymity is preserved in various ways such as source anonymity, Destination anonymity, usage of pseudonyms etc. Large scale Applications and emergency military operations encompasses the anonymity preserving task. In this paper, anonymity is preserved by means of "Anonymous Agents". Shortest path to destination is calculated using GPSR(Greedy Perimeter Stateless Routing) protocol. The source maintains a data cache table. Anonymous Agents are chosen in the path determined by GPSR. Digital Signature is used for authentication. From simulation results, Delay and Routing Performance is improved as well as security is preserved by the adopted scheme.**

Keywords: **Anonymity, Anonymous Agents, Digital Signature, GPSR, RSA, Security.**

I. INTRODUCTION

MANETs are victims to many security attacks. There are many routing protocols that poses security threat from various types of attacks such as active attacks like Masquerade attack, Denial of Service etc, passive attacks like traffic analysis and release of messages. Thus anonymous routing is adopted to confuse the attackers. This enhances the efficiency of routing as well. In this paper GPSR protocol is adopted for finding shortest path to destination and for routing as well. Route Request packets are sent from source to destination and the Route Reply packets in the reverse way in the established path before data transfer.

Anonymous Agents are chosen in the discovered path to protect the data leakage and corruption. Misleading attackers is successfully achieved using these agents. Location based anonymity and topology based anonymity are the two major types of anonymity preserving techniques. Many routing protocols like ALARM, PRISM, ALERT, MASK are proposed to preserve anonymity which has some drawbacks. Privacy preserving applications are benefitted by adopting these type of protocols. Random forwarding approach to forward data to destination encounters more delay overhead as well.

To overcome these limitations and defend attacks effectively the approach involving GPSR to find the shortest path is involved. Anonymous agents are used to preserve anonymity by confusing attackers. The number of such agents to be adopted is determined based on the number of nodes in the discovered shortest path from source to destination as well as the area of the network considered. Number of anonymous agents is directly proportional to the number of nodes in the discovered path and area of the network considered. After finding the shortest path, Route Request packet is sent to destination along the path which is acknowledged by Route Reply packet sent by the intended destination in the reverse direction to source along the same path. Encryption and decryption is done using RSA algorithm to provide anonymity and security. Authentication is provided by using digital signature. Hash MD5 algorithm is used to provide integrity.

II. RELATED WORK

There are various protocols in MANETs whereby anonymity is preserved. The working of ALERT, ALARM and MASK in MANETs is discussed over here. In paper [1] it partitions the network into alternative horizontal and vertical partitions called zones and chooses random relay nodes to forward data to the destination that resides in destination zone.

It effectively counters the intersection attacks and timing attacks. It hides the source and destination from several data initiators and receivers. It achieves better route anonymity protection at lesser cost as well. It provides source, destination and route anonymity. This is location-based routing technique. It produces high latency and cannot defend all types of attacks.

In paper [2] it preserves privacy and is a link state routing protocol. It secures the data from active and passive insider and outsider attacks. Active insiders are of two types. One is Sybil attack and location fraud. It uses group signatures to identify nodes by creating pseudonyms. It is suitable for mission-critical applications. It incurs lower traffic overhead compared to OLSR (Optimized Link State Routing). Although it prevents Sybil attack, it cannot prevent location fraud. LAM (Location Announcement Message) is flooded announcing the location of particular node which is always under risk of attack by intruder.

In paper [3] it effectively defends eavesdropping attack. It does not disclose the real IDs of nodes to attackers. Pairing-based cryptography is the basis of the paper. MAC Layer communications encompasses neighborhood authentication so that neighboring nodes in the group identify each other. Network Layer communications includes the maintenance of data structures, route discovery and data forwarding. Anonymous communications are enabled thus in both layers. It can defend attacks such as Message Coding Attack, Flow Recognition and Message Replay Attacks, Timing Analysis Attack. Due to random delay under normal traffic load it behaves worse.

III. PROPOSED SYSTEM

This section provides the brief description about the proposed method to improve the routing efficiency, security and delay in MANETs by providing anonymity.

The work comprises of different stages as referred in Figure [1]: Session key establishment, Digital signature generation and verification for authentication, Shortest path discovery using GPSR that encompasses Route Request phase and Route Reply phase, Privacy and Security preservation.

A. Session Key Establishment:

Diffie-Hellman Key Exchange is used for this purpose. It is a public key cryptographic technique that exchanges the private key over public channel. Before transferring control and data packets, session has to be established between communicating parties using private and public keys.

B. Digital Signature Generation and Verification for Authentication:

The communicating entities should be those which are supposed to be, hence authentication plays a vital role. Digital signature is used to accomplish this purpose. Message is hashed with MD5 to generate digest. The produced digest is encrypted with AES which is a symmetric key technique to generate the digital signature finally. Here MD5 is used to provide message integrity. To verify digital signature the digest received and digest recalculated is compared. If both digests are same then the received signature is correct or else it is incorrect.

C. Shortest Path discovery using GPSR that encompasses Route Request Phase and Route Reply Phase:

Greedy Perimeter Stateless Routing is used to compute the possible shortest path to destination. Greedy mode calculates the shortest path to destination through a neighboring node, whereas perimeter mode finds for the node that is nearest to destination being shortest path from that particular node, without involving neighboring node to source as that does not become the shortest route. If both the distance calculated by greedy and perimeter modes are equal then the path that involves the immediate neighboring node that is in clockwise direction to the source.

Once the path has been decided the number of agents depends on two factors: The number of nodes along the routing path and area of the network considered Number of agents is proportional to ‘a’ as well as ‘n’ Number of Agents **α** Area of Zone Number of Agents **α** Number of nodes in the desired route.

Route Request Phase involves sending of REQ (Route Request) packets from source to destination after establishing the shortest path. REP (Route Reply) packets are sent in the reverse direction to source from destination. Corresponding data structures like Routing Table, Neighborhood tables are updated.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (49-54), Month: July - September 2015, Available at: www.researchpublish.com

D. Privacy and Security preservation:

To ensure privacy of data and preserve security, RSA algorithm is used for cryptographic encryption and decryption at source, destination and anonymous agents. REQ , REP packets and data are encrypted. Hash MD5 is used to preserve integrity.

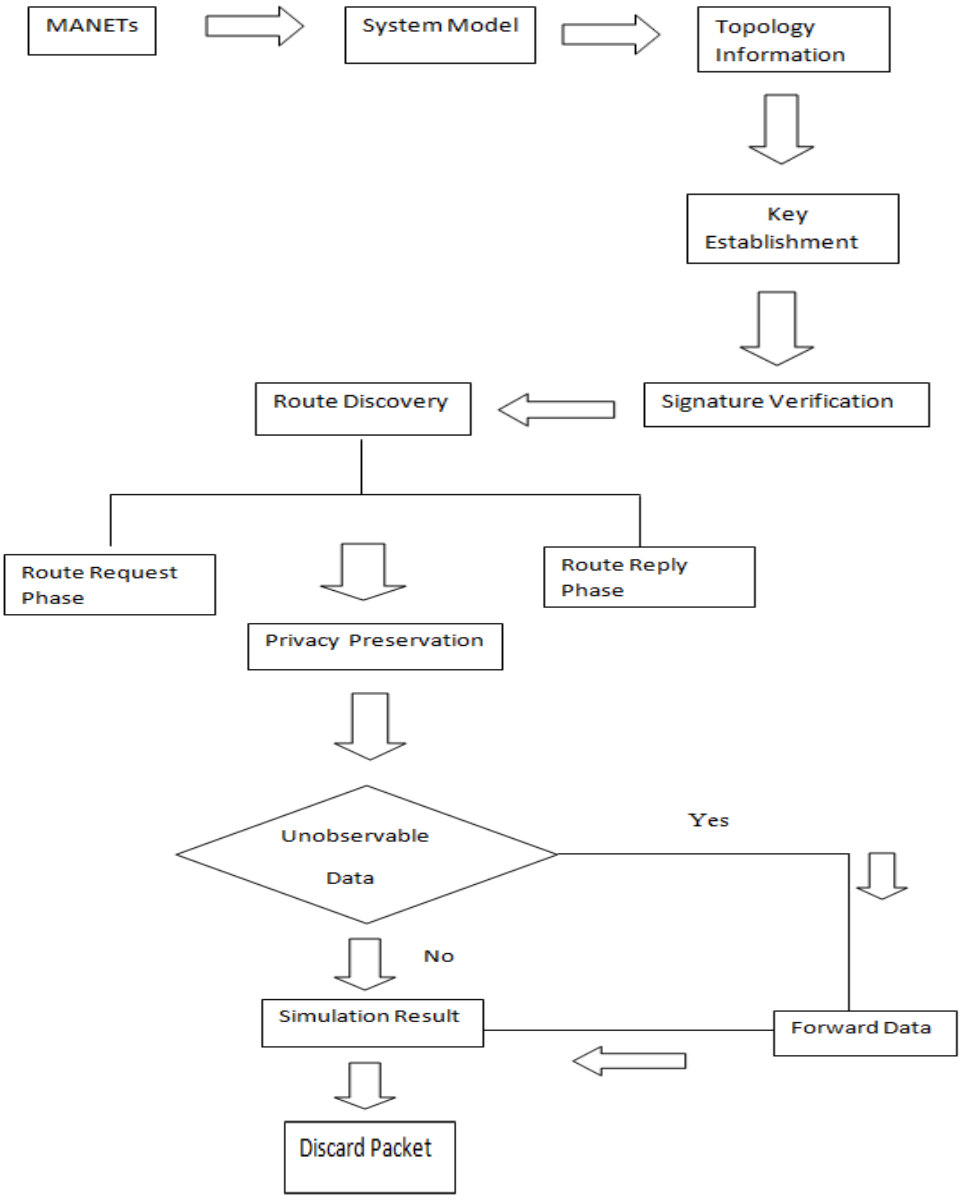

Fig 1: The workflow of proposed system

E. Algorithm:

The following algorithm gives the brief description on the route request generated at source and its forwarding.

//Route Discovery:

//At source:

Step 1: Shortest path for destination is discovered through GPSR (Global Perimeter Stateless Routing).

Step 2: The Source maintains a data cache table to record the encountered nodes in the path.

Step 3: The source encrypts its identity by using RSA algorithm.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (49-54), Month: July - September 2015, Available at: www.researchpublish.com

The following algorithm gives the request forwarding through intermediate node that transfer it to next hop neighbor.

//At intermediate node:

Step 1: The node knows only the next node to which the data has to be forwarded

Step 2: The source and destination information is not disclosed to intermediate nodes

The following algorithm shows request forwarding at agents and its decryption.

//At Agents:

Step1: Agents can decrypt the source address.

Step 2: It forwards the route request packet to next nearest node to destination

The following algorithm shows the receipt of request and its decryption at destination.

// At destination:

Step 1: Destination decrypts the route through RSA algorithm.

Step 2: By maintaining destination table it indicates that the data is intended for it

//Route Reply:

The above procedure is followed in the reverse manner where every encryption is replaced with decryption using RSA algorithm to respond to the request.

//Data forwarding:

Data is forwarded as per the discovered route using RSA encryption at agents

IV. SIMULATION RESULTS

NS-2 simulator is used for simulation. The test bed for simulation has to be set up. The connection configurations, protocols of transport layers are involved. Agents are used to connect nodes in different layers to communicate. This simulation consists of route request and route reply phases. The X-graph shows the final comparative study of performance.

A. Route Request Phase: From Fig. 2 the nodes which are in green color are source nodes and which are blue in color are destination nodes. The nodes that are red are agents and the black colored node is malicious. This snapshot shows the route request phase where packets are generated to request the route. Encrypted keyword through hashing and another encrypted keyword using RSA is displayed and verified.

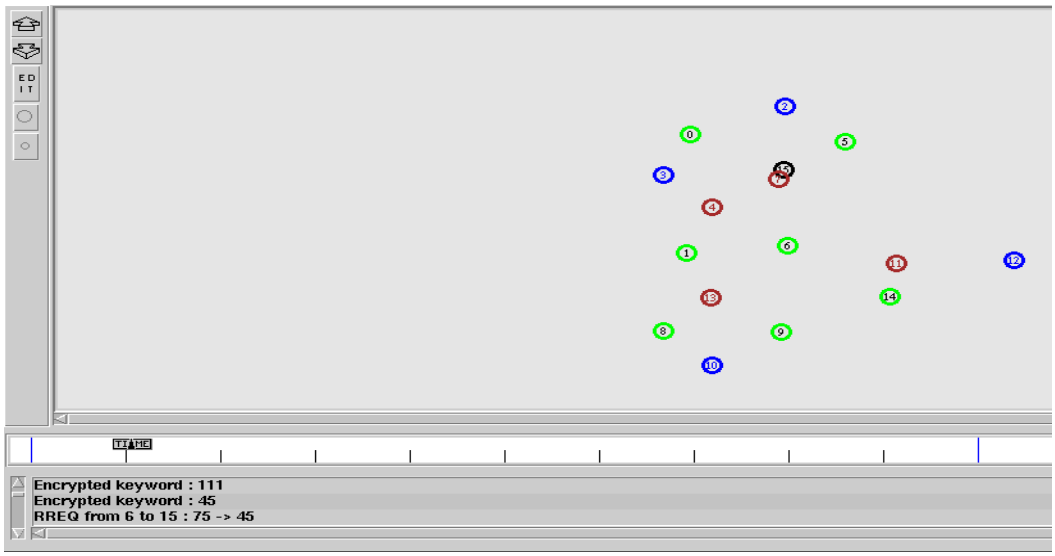

Fig 2: Route Request Phase

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (49-54), Month: July - September 2015, Available at: www.researchpublish.com

B. Route Reply Phase: The snapshot in Fig. 3 shows the route reply phase where request for route is acknowledged. The verification of encrypted keywords happens by adopting decryption techniques.

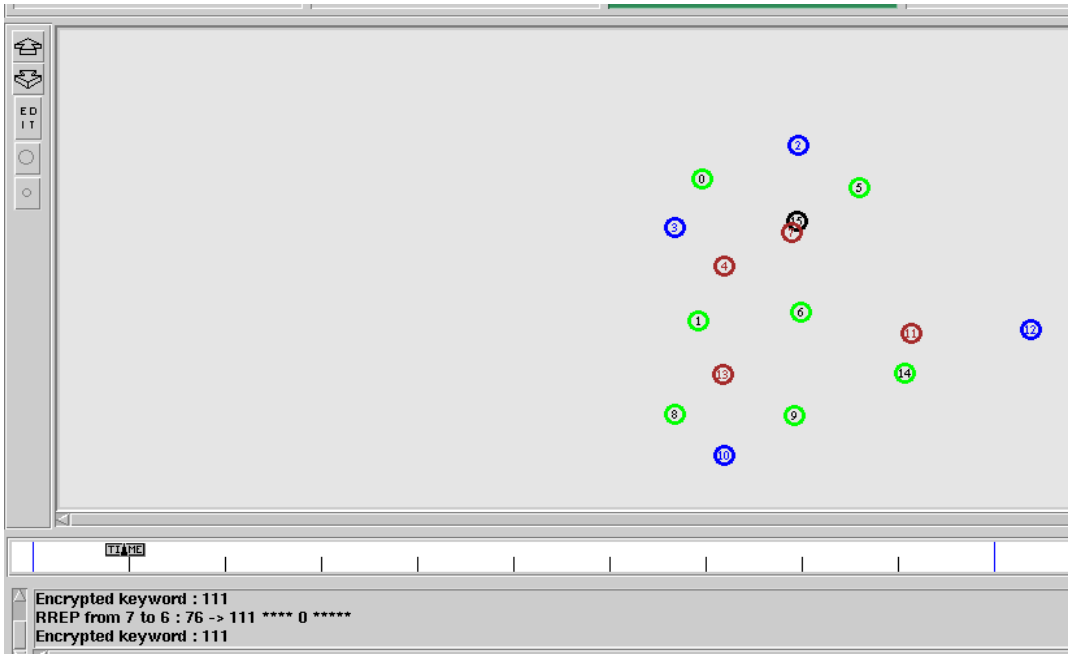

Fig 3: Route Reply Phase

C. X-Graph: It gives a overview of the multiple variables dependence and moreover takes inputs from different files. In the below graph plotted, X axis indicates the number of iterations which involves request, reply and data transfer. Y axis indicates the key complexity involved that is the key size of AES. The red straight line shows the linear variation of key complexity with iterations that is in normal condition and the enhanced key complexity by adopting the proposed scheme is shown by green straight line.

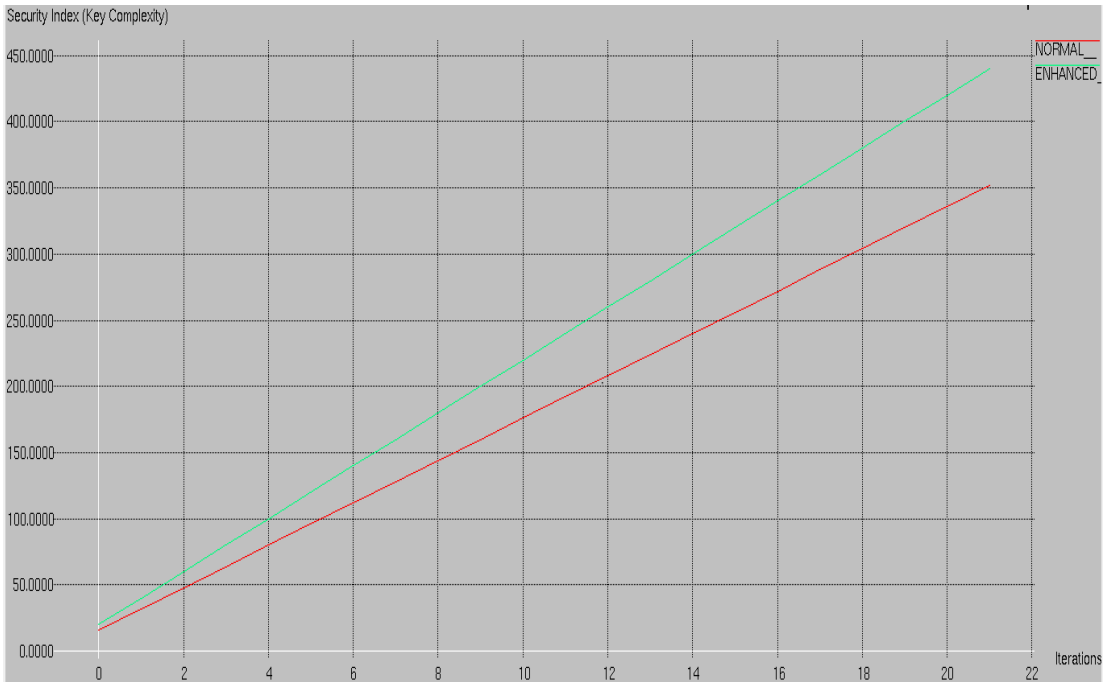

Fig 4: X-Graph for Iterations versus Security Index

D. Experimental Results:

The Table 1 shows the increase in percentage of security and throughput with increase in number of iterations.

TABLE I: TEST CASES

Number of Iterations	% of Security	% of Throughput
2	2%	0.4%
4	3.3%	0.56%
6	4.7%	0.82%
8	5.6%	0.9%
10	6.4%	1.52%
12	7.1%	1.67%
14	8.2%	1.79%
16	9.3%	1.92%
18	10%	2%

V. CONCLUSION AND FUTURE WORK

The proposed work is adopted to preserve the anonymity in mobile ad hoc networks by effectively defending all types of attacks. This scheme accomplishes the security to be preserved to enhance effective routing. Key complexity is enhanced by adopting and integrating various encryption techniques such as RSA, Diffie Hellman Key exchange and AES algorithms. Key size is increased for the same number of iterations and an enhancement in security of 10% is noticeable which in turn provides 2% of increase in throughput too. The limitation of the proposed scheme is delay increases as the encryptions are involved at every stage to preserve security. The future work has to overcome this by using fast processing cryptographic schemes that reduces delay and provides security.

REFERENCES

[1] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang. "MASK: Anonymous On- Demand Transactions on Wireless Communications, VOL. 5, NO. 9, September 2006

[2] Karim El Defrawy, Gene Tsudik. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs". In IEEE Transactions on Mobile Computing, VOL. 10, NO. 9, September 2011.

[3] Haiying Shen, Lianyu Zhao. "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs". In IEEE Transactions on Mobile Computing, VOL. 12, NO. 6, June 2013

[4] Ada, C. Castelluccia, J.P. Hubaux, Packet coding for strong anonymity in ad hoc networks, in: Proc. of IEEE SecureComm'06, Baltimore, MD, USA, 2006.

[5] Y. Zhang, W. Liu, W. Lou, Anonymous communications in mobile ad hoc networks, in: Proc. Of the IEEE INFOCOM'05, Miami, USA, 2005,pp. 1940–1951

[6] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.

[7] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.