Reliable Data Transmission in Anonymous Location Aided Routing in MANET by Preventing Replay Attack

Monika Khatkar[1], Nisha Phogat[2], Dr. Brijesh Kumar[3]

[1,2]*KIIT College of Engineering MDU,* [3]*Lingaya's University, India*

[1]khatkarmonika@gmail.com, [2]n.phogat@gmail.com , [3]muskanbrijesh@gmail.com

***Abstract*: Privacy and security are major issues in MANET, especially when used in sensitive areas. Secure routing protocols have been developed/proposed by researchers to provide security and privacy at various levels. ALARM protocol (Anonymous Location Aided Routing in MANET) provides both privacy and security features including confidentiality, authentication and authorization. Location based routing is based on some assumptions in MANET ie location of the mobile nodes (using GPS), Time Clock of mobile nodes are loosely synchronized, mobility and Nodes has uniform transmission range. In the current work an effort has been done to review the ALARM protocol and identify some of the security problems in MANET. Further the work suggests a mechanism to prevent malicious activity (replay attack) in MANET using monitoring method.**

***Keywords*- Alarm Protocol, Replay attack, MANET, Monitoring, Prevention**

I. INTRODUCTION

Mobile Ad-Hoc Network is self-organized, autonomous and distributed wireless system. Nodes in MANET are mobile, means they can change their position and move in/out of network freely. It is a temporary network without any form of centralized administration. In a MANET, mobile nodes have the capability to accept and route traffic through their intermediate nodes towards the destination so nodes can act as both routers and hosts. Because of MANET features like open channel, dynamically changing topology, lack of central security mechanism and wireless, MANETs frequently suffer from security attacks. Nodes communicate with each other through intermediate nodes on the basis of mutual trust and this characteristic makes it more susceptible towards security attacks as any intermediate node (attacker) can exploit the security. MANET plays a significant role in military, search and rescue and law enforcement. In these scenarios, security and privacy are of great concern. This required to provide communication links between mobile nodes which are reliable and protected in nature. Attackers can be outsider or insider of the network and purpose can be passive or active where either they can inject the information or just eavesdrops the communication and disrupt the overall performance. In MANET Black Hole, Worm Hole, selective packet drop/ forward, replay attack etc can take place by intermediate nodes. In our work we propose a mechanism to prevent these attacks (Replay attack) in mutual authentication based ALARM by adding monitoring in network to prevent malicious node from communication path. The work is organized into following sections: Section II describes the related work followed by description of ALARM protocol in Section III and overview of security attack in Section IV. Section V & VI & VII, contains the technique, simulation experiment results and conclusion respectively.

II. RELATED WORK

There are a numerous protocols and techniques proposed to address the issue of privacy and security in MANET's.

Steven M. Bellovin et.al. discussed about the limitation of Kerberos authentication system [1]. The two main limitation of Kerberos authentication protocol include its use of an authenticator to prevent replay attacks [1] and large number of message exchanges, for successful authentication. This approach degrades the performance. **Kyasanur et.al** proposed a protocol extension of 802.11. DCF protocol to detect the selfish behavior of the nodes. The Per proposed scheme allows a receiver to detect misbehaviour of sender [2]. **Marti et.al** used watchdog and pathrator [3] to identify the misbehaving nodes and to avoid routing packets through malicious nodes. When a node forwards a packet, the Watchdog on node verifies the next node also forward the data [3]. It listens other node's transmission promiscuously and sees if it is forwarding packet or not. If not then it is misbehaving node. The pathrator after knowing about malicious node choose other reliable path. **Tang et.al.** proposed efficient authentication mechanisms for low-power devices. This approach uses an elliptic-curve-cryptosystem which is based on trust delegation mechanism

978-1-4799-6896-1/14/$31.00 ©2014 IEEE

generating a delegation passcode for authentication of mobile station [4]. In the proposed scheme the mobile station only need to pass one packet for mutual authentication. This authentication mechanism defend many known attacks including the denial of service attack. **Chen et.al. d**iscussed about importance of mutual authentication for wireless sensor networks .In this Paper DES protocol is discussed along with security against the stolen-verifier, masquerade, replay, and guessing attacks and proposed enhanced scheme - Enhanced protocol for the two factor authentication in WSNs, which has three phases: registration, login, and verification [5]. **Shen et. al.** suggested Anonymous Location-based Efficient routing protocol (ALERT) [6]. It provides source, destination and route anonymity. It dynamically partitions the network into zones horizontally-vertically. After partitioning, it selects nodes in these zones dynamically as intermediate node for forwarding the data. This way it creates unpredictable route and provides network security. [6]

III. ANONYMOUS LOCATION AIDED ROUTING IN MANET - ALARM

Alarm protocol is *Anonymous Location-Aided Routing* in MANET [7]. It is based upon proactive and link-state routing. It constructs a secure MANET map using Nodes' current Location using LAM. Location information has available through GPS receivers. The main features of ALARM are - Privacy, security, data integrity, node authentication using group signature technique and anonymity. It periodically proactively updating network map using current location of nodes. It provides prevention against passive and active attacks.

Basic operation of ALARM:

1. Initialization:

A. The group manager (GM) adds eligible and legal MANET nodes in a group as group members after initialization of the group signature scheme. In this phase, each node generates its own private and corresponding public key. This Public key is exposed to GM only. Nodes uses private key to generate group signature. In addition to these two keys, each node knows group public key. This key is common to Group and used for group signature verification.
B. The GM may add new joinees or revoke the existing members, depending upon the specific group signature technique. [7]

2. Operation:

A. Time is distributed into slots of Length T. At the start of each slot, a node generates a temporary public private key pair- PK-TMP (public key) and SK-TMP (private key). Other members uses public key to encrypt the session keys.
B. The Location Announcement Message (LAM) is broadcasted by each node and flooded in MANET. The LAM contains its location, temporary public key (PK-TMP), time-stamp and group signature which has been computed over mentioned fields.
C. When a new LAM is received by a node, it checks whether it is received before or not. If not, then checks time-stamp and then verify group signature. In case both are found to be valid then node rebroadcasts the LAM for its neighbours. After collecting all latest LAMs, each node then creates a geographical map and node connectivity graph. Temporary pseudonym is used to locate the node in the interval between two successive LAMs. The Temporary pseudonym includes temporary location of the node and group signature of the last Location Announcement Message. TmpId = {Location||GSig}. Detail flow chart is in Figure 1.[7]
D. When a node wants to send a message to any other node at some location, it checks if the destination node exists in its proximity or not. If it exists, the node sends the data message to its pseudonym, TmpId, in the encrypted format. The data is encrypted with session key. Session key is also encrypted using public key (PK-TMP) of destination node and added with data message. On receiving the message, the destination node recovers the session key first and then decrypts the data message. [7]
E. Forwarding: As discussed, the current topology is disseminated by ALARM by periodically flooding of LAMs. After getting the entire network topology view, a node decides whether or not to communicate with other node. There is no linkage between Message forwarding and topology dissemination. The route can be computed by shortest path or any location-aided routing algorithm.[7]

Figure 1 shows basic LAM process in ALARM. Upon receipt of the new message, nodes verify timestamp of message. If Timestamp of message is not in allowed time slot then it rejects. This way ALARM protects from replay attacks but due to loose synchronization of clocks on mobile nodes, replay attack is still possible

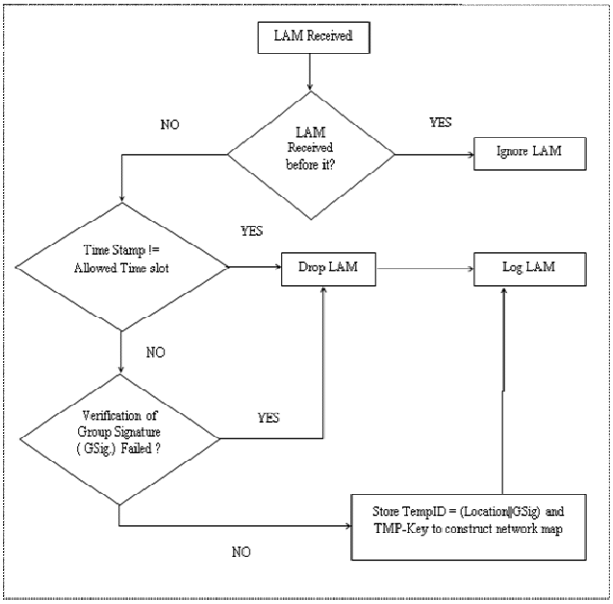


Figure 1. ALARM LAM receiver process.

For example – if the receiver clock is behind the sender clock, an attacker can replay the post-dated packet, when the timestamp of packet becomes valid as per the clock of receiver [8].

Let say source send a message with time stamp Ts in message and t0 is time at destination. Threshold allowed time limit is Δt. A packet is valid if $|Ts - t0| < \Delta t$

Assumptions of ALARM

(I) Location- Each node has device that gives accurate location of Node. For example by using GPS. (II) Mobility- There is a periodic movement of certain minimum number of nodes. (III) Time- The node's clocks are weakly synchronized. (IV) There is a uniform transmission Range of Nodes. A MANET can determine the node connectivity, when a node gets the current MANET map [7].

IV. SECURITY ATTACKS IN MANET

The Attacks in MANETs can be broadly divided into four categories: Active Outsiders, Active Insiders, Passive outsiders and Passive Insiders.

Passive attacks does not disturb the operation. Their main purpose is snooping of the exchange of data and violate confidentiality without any modification. Such type of attacks is handled by powerful encryption techniques whereas Active attacks try to disturb the operation by either dropping or forwarding the modified data in network. Active insiders are actually part of the network and are most powerful as they have all keys and authorization so it is very difficult to find out them. Overall, attacks in network degrade the performance of the network, privacy and security.

Following are some attacks scenarios that can be carried out by the active insider, namely:

Replay Attack: is an attack in which an attacker repeatedly re-transmits the valid data to the network that has been previously captured or Hold data for some time and then forward.

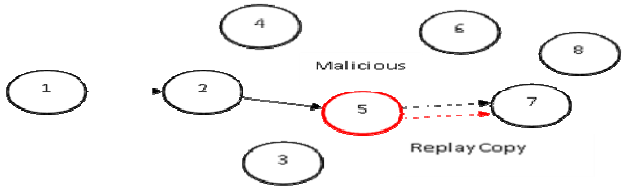


Figure 2: Replay Attack – Copy

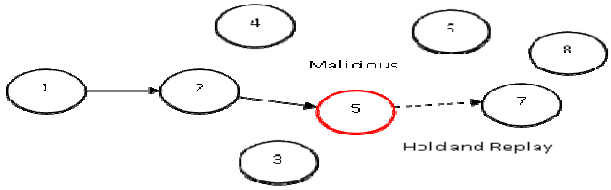


Figure 3: Replay Attack – Delay

Selective Packet Drop: In this type of attacks, intermediate nodes selectively drop some of the packets and forward rest of the packets to the destination.

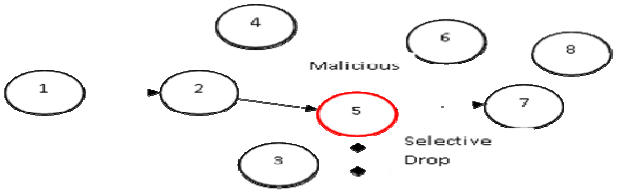


Figure 4: Selective Drop and forward

Black Hole: In this attack intermediate node drop all the received packets and does not forward to next destination.

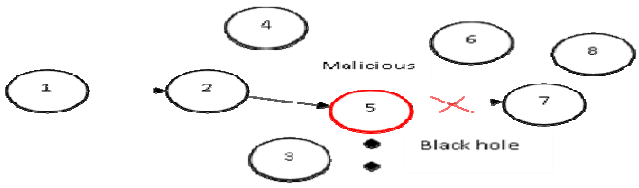


Figure 5: Black Hole

As a part of our work on replay attack prevention, we considered all above mentioned scenarios as well in our study and simulation.

V. PROPOSED METHODOLOGY

As discussed above, there are number of passive and active attacks which can occur and degrades the overall performance of the network. To prevent these attacks a trust relationship among the nodes can be achieved using ALARM. Any intermediate Active insider attacker who has all the keys and authentication can still disturb the communication in MANET by dropping packets selectively or drop all packets. As per the assumption in ALARM that clock of nodes are weekly synchronized so attackers can replay the messages and/or hold for some time and then replay. Such malicious node reduces reliability of data transmission in network. To isolate such malicious nodes from communication path, we propose a monitoring methodology to isolate malicious node path in MANET based upon mutual authentication based ALARM protocol.

Our proposed methodology checks the throughput of the network. When the throughput of the network is less than certain defined threshold value, nodes in the network will go to monitor mode and checks the throughput of the nodes in path. If found issue then inform to source for redirection.

Detection of Malicious node:

1. After the deployment of the network with finite number of nodes, A routing path is established between source and destination through routing protocol.
2. Source sends fake packets through a path to test the route. All other nodes are set in monitoring mode.
3. Monitoring nodes starts monitoring their neighbour nodes using ICMP Packets.
4. There is a malicious node in path. It is intermediate node and receives the packet for forwarding to next node in path. Instead of forwarding immediately, it hold it for some time and then further forward it after some delay, this is known as replay attack. Due to this overall end-to end delay increases.
   To Set a node as malicious in simulation, a signal was sent to system to hold the packet for some defined time and then forward.
5. The Monitoring Node near to this malicious node sends the ICMP Packet to malicious node and checks the throughput. It checks the throughput for some time.
6. If the returned throughput is less than defined threshold value then it detect node as malicious node.

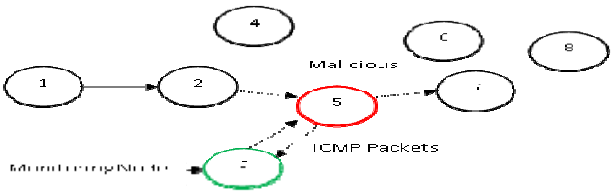


Figure 5: Monitoring

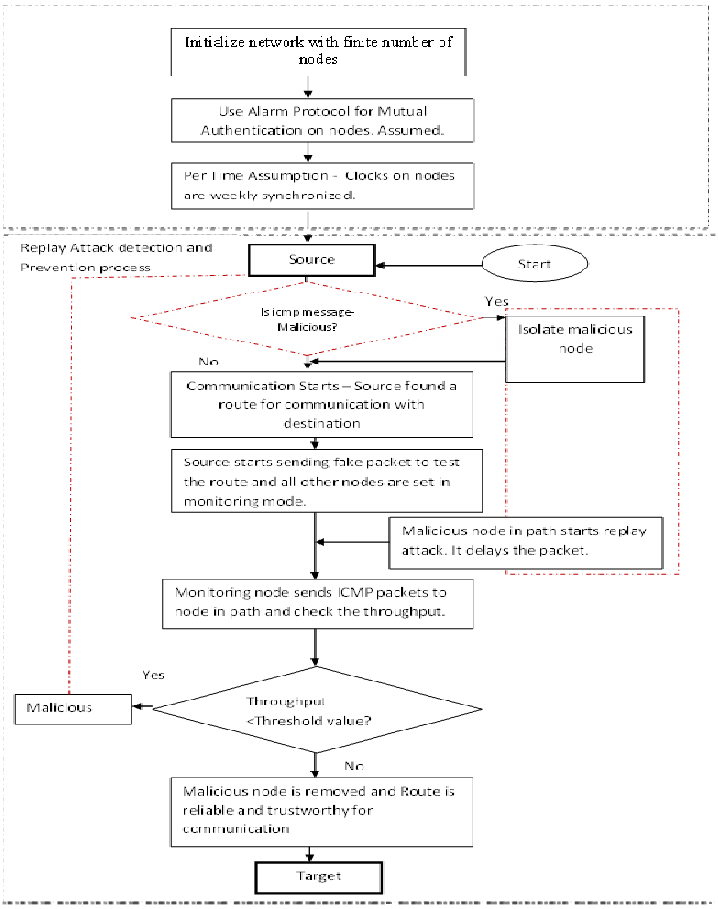


Figure 6: Flowchart of methodology

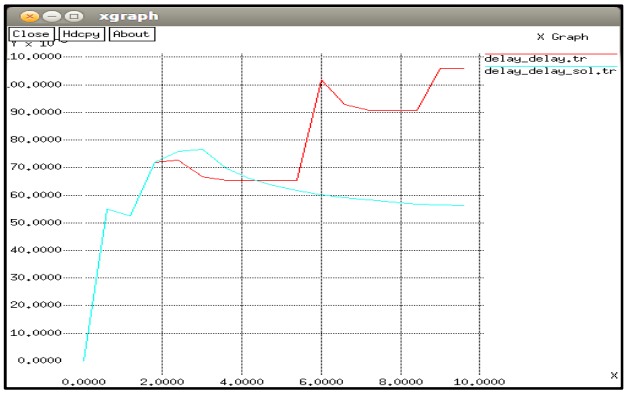
Isolation of the malicious node:

1. After deciding the node is malicious node in path, Monitoring node informs the same to source.
   In simulation, "Error Report" signal on malicious node was sent to remove this node from path.
2. Malicious node from path is isolated and source selects new path for the communication.
3. Now it isolates the path and source starts communication with destination on new reliable path.

To simulate the other scenario of replay attack, where malicious node records the copy of massage for re-transmission (in above step 3 of detection), we sent a signal to system to keep a copy of the original packet and replay the recorded copy.

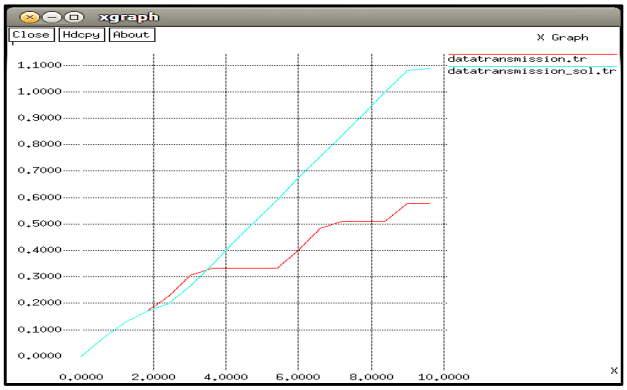
VI. EXPERIMENTAL RESULTS

The proposed methodology was implemented in Network Simulator version 2.35. The existing ALARM Protocol is simulated with the help of AODV routing protocol. As per our simulation, it is analyzed that by removing the malicious node from path which is degrading the network by replay attack will decrease the delay and increases the overall performance of network. We experimented this with other attacks as well e.g. Black hole and selective drop/forwarding (Gray) attacks. Overall network will more secure and reliable against security threats.

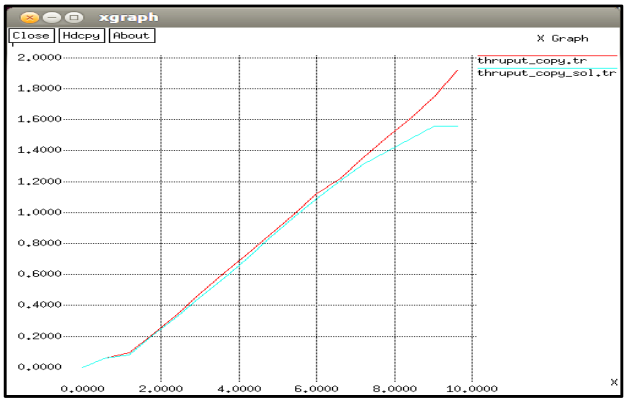


Graph 1: Delay comparison graph

As above figure illustrate, by isolating malicious node from communication path there is less delay in packet transmission.

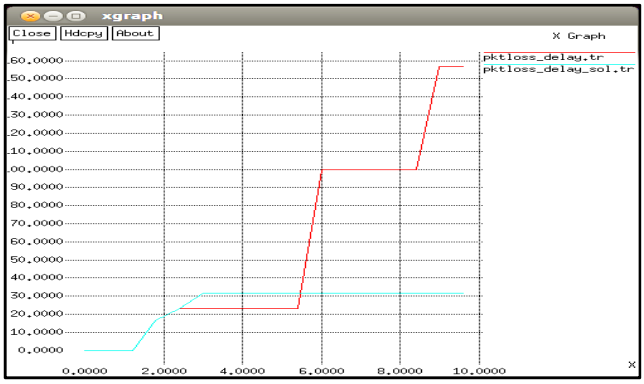


Graph 2: Message Exchange comparison while replay attack holds the packet for some time and then Replay the same packet.



Graph 3: Message Exchange comparison while replay attacks record the packet and retransmit the copy of the packet.

Above figure 3 illustrate that due to replay attack, message exchange is more (red line) as replay attack re-transmit the copy of original message. In other case of replay attack (Figure 2 – red line), replay attack hold data for some time and then send it later, so message exchange is less at a particular point of time. Green line shows no. of message exchange after solution.



Graph 4: Packet loss Comparison

In above figure graph shows that after removing malicious node from path number of packet loss is less.

VII. CONCLUSION

Use of MANETs in mission critical applications requires secure and efficient routing of packets. Alarm Protocol provides security against insider and outsider attacks using mutual authentication. In MANET there are many insider threats of security such as: Replay Attack, Black hole and Selective Packet Drop, which degrades the performance of MANET even after strong integrity and authentication, is used.

In this paper, we proposed a mechanism to prevent these attacks (Replay attack) in mutual authentication based ALARM using

monitoring technique. It helps in isolating the malicious node from path and make communication reliable.

Experimental results show that removing of the malicious node from path increases the performance and make data transmission more secure and reliable in MANET.

ACKNOWLEDGEMENT

The authors would like to thank Mr. Jogender Singh Khatkar, Infogain India (P) Ltd., for providing us with the entire necessary technical and moral support in working in this area. Without his support, this work would have not been possible.

REFERENCES

[1] Steven M. Bellovin. and Michael Merritt "Limitations of the Kerberos Authentication System ", USENIX – winter 1991

[2] Kyasanur P. "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005

[3] Marti S., Giuli T-.J., Lai K., and Baker M. "Mitigating routing misbehavior in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[4] C.Tang and D. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE, 2008

[5] Chen T.-H. and Shih W.-K. , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks, ETRI Journal, Volume 32, Number 5, October 2010

[6] Shen H. and Zhoa L. "ALERT : An Anonymous Location – Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, Vol. 12, no. 6, june 2013.

[7] Defrawy K.E., and Tsudik G. , "ALARM: Anonymous Location-Aided Routing in Suspicious MANETS" , IEEE Transactions on mobile computing, vol. 10, no. 9, September 2011

[8] Gong L., A security risk depending on synchronized clocks. ACM Operating System Review, 26(1):49–53, 1992.