ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Security Issues in ALARM Protocol for Mutual Authentication in MANET: A Review

Gagandeep Kaur Virk, Dinesh Kumar

M.Tech Student, Dept. of CSE, GZS PTU Campus, Punjab, India

Assistant Professor, Dept. of CSE, GZS PTU Campus, Punjab, India

ABSTRACT: MANET (Mobile Ad hoc Network) is the self configuring type of network in which mobile nodes can join or leave the network when they want as it is a decentralized type of network. Due to these unique properties of the MANET, it is much vulnerable to security attacks. ALARM protocol (Anonymous Location Aided Routing in MANET) is used in MANET to achieve the key security objectives, i.e. confidentiality, authentication, authorization, integrity. ALARM protocol is based on certain assumptions, such as, location of the mobile nodes, time at each node, range of mobile nodes etc. According to time assumption, clocks of the mobile nodes are weakly synchronized. Due to this weak synchronization of the mobile nodes replay attack is possible which degrades the reliability of the ALARM protocol. In this paper, we review the ALARM protocol, identify the problem related to time assumption of the ALARM protocol and propose a robust mechanism to isolate replay attacks in MANET.

KEYWORDS: ALARM, active attacks, GPS, MANET, privacy, passive attacks, Replay attacks, security.

I. INTRODUCTION

MANET stands for mobile ad-hoc network. It is a self-configuring infrastructure-less network. In MANET, all the devices are connected by wireless links. Every device in a MANET is free to move independently in all the directions. It can change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information which is necessary to route the traffic.

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. A passive attack obtains data exchanged in the network without disturbing the communication operation. The passive attacks are difficult to detect. These attacks compromise the confidentiality of the data [9]. Examples of passive attacks are snooping, eavesdropping etc. The active attacks are those in which any data or information is inserted into the network so that information may harm the normal operation of the network. These involve fabricating messages, dropping or modifying packets, replaying packets. Examples of active attack are spoofing, impersonation etc.

Replay attacks are passive attacks, in which an attacker instead of modifying packet‘s contents just replays stale packets in order to exploit battery power, bandwidth and computational constraint of mobile nodes. It leads to congestion in the network and confusion among the routing nodes because of conflicting information, thus, delaying packet delivery or preventing them from reaching destination.

In the absence of mutual authentication, there are several type of active and passive attacks possible like replay attack, sniffing, snooping etc. In our proposed work, we try to prevent these Replay attacks by using mutual authentication between the nodes in the network. For this, we used authentication based protocol called ALARM using cryptographic mechanism of digital signatures for carrying timestamp and location information of nodes privately in the network

The rest of the paper is organized as follows: Section II describes the related work followed by description of ALARM protocol in Section III. In Section IV & V, we presented problem formulation and our proposed technique respectively. And Section VI is the conclusion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

II. RELATED WORK

There are many routing protocols that can be used in MANETs. But most of them do not focus on Privacy, especially, tracking-resistance i.e. making nodes untraceable. If nodes become traceable by other nodes, privacy of the nodes is compromised and it may lead to occurrence of various attacks like eavesdropping, location fraud etc.

[1] Presents the ALARM protocol for mutual authentication to prevent Sybil and Location Fraud attacks. In this technique, the mobile node presents its secondary identity which helps the node to become untraceable by all the other nodes. In ALARM protocol, certain packets are exchanged for mutual authentication and messages are digitally signed. The digital signature approach leads to message integrity and confidentiality. Overhead and scalability of ALARM is also evaluated and shown that it performs close to other protocol (like OLSR)

In [2], elliptic-curve-crypto system based Trust Delegation mechanism is used to generate group pass code for mobile station authentication. This proposed mechanism requires less computations and less message exchange as compared to other authentication schemes.

Mutual authentication is achieved in WSN using Das' protocol [3] which is the hash-based authentication protocol. They have proposed certain enhancements in the Das' protocol and this enhanced protocol is reliable, energy efficient and provides more security to the sensor nodes in the insecure environment.

[4] Presents Hybrid Anonymous Location-Aided Routing Protocol for MANETs. This technique utilizes both proactive and reactive routing. The proactive method is applied for the nodes which are within the pre-defined radius and reactive method is applied for nodes which are outside the pre-defined radius. When the source wants to transmit the data to the destination, it is done using some encryption technique with the help of topology information. By simulating the results, they have shown that the proposed technique offers minimized overhead and delay and increased accuracy.

Anonymous On-Demand Routing protocol for MANETs is used in [5]. They have considered two types of attackers- external global passive attacker (who can observe all possible communications between all nodes in the network at all time) and cooperating node inside the network i.e. they have assumed that every node that is part of the network is a potential attacker. Anonymous nature of the protocol lies in the goals of the proposed protocol. Example-preventing a node from learning the destination of some message, preventing a node from determining whether another node is part of a path between two nodes. So, this protocol is based on reactive routing along with anonymity.

Proactive routing protocol based on Link State algorithm is used in [6]. This protocol is optimized in the sense that it reduces the size of information sent in the messages and number of retransmissions to flood these messages by using the concept of Multipoint Relays (MPR). OLSR protocol is preferred in dense networks and where the communication is assumed to occur frequently between large number of nodes.

In [7], comparison between two Link State algorithms namely OSPF and OLSR is done, for ad-hoc routing. They considered various parameters of ad-hoc networks like neighbourhood size of each node, overhead of retransmitting the link states, topology - change rate. This analysis is based on the assumptions that time is slotted and that mobile nodes are synchronized. In this work, it is shown that OSPF performs quite poorly in most cases as compared to OLSR and hence OLSR is best suited for ad-hoc environments.

III. ALARM PROTOCOL

Alarm protocol is *Anonymous Location-Aided Routing* in MANET.ALARM is a privacy-preserving and secure link-state based routing protocol. It uses node's current location value from Location Announcement Message (LAM) to construct a secure MANET map. Location information has become progressively more available through small and cheap GPS receivers. This technique utilizes proactive mode of location based routing. ALARM provides both security and privacy features by providing node authentication, data integrity, anonymity, and un-traceability. It also offers protection against passive and active insider and outsider attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Message-Type = LAM
Current-Location (8 bytes) (Location)
Current-Time-Stamp (4 bytes) (TS)
Temporary-Cryptographic-Key (~128 bytes) (PK-TMP)
Optional: *Transmission/Reception-Range (2 bytes)* *(TX-RX-RNG)*
Optional: *Public-Key-Signature (~ 250 bytes)*
GSig(Location || TS || PK-TMP) (~ 200 bytes)

Fig. 1. Location Announcement Message

A. Basic steps in ALARM's operation

1. Initialization (Offline)

- The group manager (GM) initializes the basic group signature scheme and admits all legal MANET nodes as group members. During this phase, each node member creates an inimitable private key that is not exposed to anyone. This key is desirable to produce valid group signatures. It also generates a corresponding public key (PK member), that is exposed only to the GM. GM is responsible for opening any contested group signatures and determining the actual signers.
- Based upon the specific group signature, GM might also hold joining of new members as well as revocation of the existing members. Revocation might not be feasible or desired.

2. Operation (Online)

- Time is divided into equal slots of duration T. At the beginning of each slot, each node s generates a temporary public-private key-pair PK-TMP (public) and SK-TMP (private), respectively [3].
- Each node broadcasts a Location Announcement Message (LAM), containing its location, time-stamp, temporary public key (PK-TMPs), and a group signature computed over these fields [3].
- Upon receipt of a new LAM, a node checks that it has not received the same LAM before. After that it verifies the time-stamp and group signature. Then node rebroadcasts the LAM to its neighbors if both are valid. Temporary pseudonym is used to locate the node in the interval between two successive LAMs. The pseudonym includes temporary location of the node and group signature of the last Location Announcement Message. Including location in the pseudonym speeds up the forwarding process and requires fewer look-ups [3].
- Whenever the communication is needed, the node checks to see if any node currently exists at (or near) that location. If it is so, the node sends the message to destination and this message is encrypted with a session key using a symmetric cipher like AES. The session key is, in turn, encrypted under the current public key (PK-TMP) included in the destination's latest LAM. When the destination receives the message, it first reacquires the session key and uses it to decrypt the rest. ALARM is not bound to any specific public key technique. However, Diffie-Hellman half-key is good choice.
- Forwarding: Message forwarding is independent of topology dissemination. The path can be computed using the shortest path algorithm or any other location-aided routing algorithm, such as Convex Hull, GeoCasting etc [3].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

B. Assumptions and Goals of ALARM

The following assumptions are necessary in ALARM:

- *Location:* Each node is provided with device that gives accurate positioning information of the node. Eg- GPS.
- *Mobility:* A certain minimum number of nodes move periodically such that group manager of new group extracts all the previous information about the node.
- *Time:* All nodes maintain weakly synchronized clocks.
- *Range:* Nodes have uniform transmission range. Once a node knows the present MANET map, it can determine node connectivity [3].

ALARM has the following goals:

- *Privacy:* There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations cannot be linked [3].
- *Performance:* Security and privacy goals must be achieved without compromising the performance.
- *Security:* The network must be resistant to passive and active attacks occurring from both outsider and insider malicious nodes [3].

IV. PROBLEM FORMULATION

Each device in a MANET is free to move in parallel in any direction, and will therefore change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route the traffic.

In MANET, inside and outside attacks are possible, which degrade the performance of the network. To prevent these attacks, a trust relationship must be developed in the network among the nodes. The nodes are mutually authenticated to each other to obtain a trust relationship. ALARM protocol is used for mutual authentication between the mobile nodes. There are basically three assumptions in ALARM protocol i.e. mobility range, location and time. In time assumption, clock of mobile nodes are weakly synchronized. Due to this, replay attack is possible in the network and the replay attack will reduce reliable data transmission between mobile nodes.

So, in this work, we will detect and isolate replay attack in mutual authentication based ALARM protocol.

V. PROPOSED TECHNIQUE

This work is about the Ad hoc network and to enhance the reliable data transmission in the MANET. For reliable data transmission, we use the ALARM protocol. ALARM protocol is used to provide mutual authentication between the mobile nodes. Suppose there are number of mobile nodes in the network and two nodes are defined as a source and destination node respectively. A path is established between source and destination through AODV routing protocol. After path establishment, source and destination become mutually authenticated with each other with the help of ALARM protocol. To test the route, source starts sending fake packets through a path. At that time source also sends ICMP (Internet Control Message Protocol) packets to all other nodes. Nodes which receive ICMP packets goes to Monitor Mode to check whether its adjacent node is forwarding data packets within threshold time period or not. If not, then its adjacent will be detected as a malicious node. The source node floods packets containing information about the malicious node to all nodes. Then all other nodes stop communication with malicious node after receiving packets from the source node and thus attack is isolated.

VI. CONCLUSION

In this paper, we conclude that due to the unique properties of the mobile ad hoc network many security attacks are possible which are prevented by various authentication protocols. In this paper, much popular ALARM protocol is revised and problems related to this protocol are highlighted and a novel technique is being proposed using AODV protocol with ICMP control messages to detect and isolate replay attack which is possible in ALARM protocol.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

REFERENCES

1. Karim El Defrawy, and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE transactions on mobile computing, Vol. 10, No. 9, September 2011.
2. CaimuTang, and DapengOilver, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE, 2011.
3. Tien-Ho Chen, and Wei-Kuan Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks" ETRI Journal, Vol. 32, No. 5, October 2010.
4. Y.V.S. Sai Pragathi, and S.P. Setty, "Hybrid Anonymous Location-Aided Routing Protocol for privacy preserving and authentication in MANET", Journal of Theoretical and Applied Information Technology, Vol. 55, No. 2, 2013.
5. S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks", International Journal Wireless and Mobile Computing, Vol. 3, No.3, pp. 145-155, 2009.
6. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad-hoc networks", pp. 62-68,2001.
7. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, " An overview of Mobile Adhoc Networks: Applications and challenges", SintPietersnieuwstraat 41, Belgium ,2005.
8. Paul Syverson, "A Taxonomy of Replay Attacks", 1994.
9. Tarunpreet Bhatia, and A.K.Verma "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue No. 6, June 2013.
10. Cédric Adjih, Emmanuel Baccelli, and Philippe Jacquet, "Link State Routing in Wireless Ad-Hoc Networks", Proc. IEEE Conf. Military Comm., Vol. 2, 2003.