Enhancement the Security of WSN using ALARM Protocol to Prevention from Reply Attack

Neelam Shekhawat[1], Moumita Ghosh[2]
[1]*Faculty of Engineering, Mody University of Science & Technology*
Laxmangarh (Sikar), India
er.neelamshekhawat@gmail.com
[2]*Faculty of Engineering, Mody University of Science & Technology*
Laxmangarh (Sikar), India
mom2001@gmail.com

ABSTRACT

The wireless Ad hoc network is the self configuring type of network. In self configuring type of networks mobile nodes can leave or join the network when they want .In such type of networks many inside and outside attacks are possible. Inside and outside attacks are broadly classified as active and passive attacks. To prevent inside and outside attacks trust relationship between the mobile nodes must be maintained. The trust relationship between the mobile nodes is provided by mutual authentication. ALARM is the protocol for providing trust relationship between the mobile nodes. In this protocol the clocks of the mobile nodes are weakly synchronized by using GPS. In such case reply attack is possible. To prevent reply attack clocks of the mobile nodes must be strongly synchronized. In our new proposed technique, we are enhancing t the ALARM protocol to provide strong clock synchronization between the mobile nodes. Our new technique will be based on the NTP (network time protocol).

Keywords: ALARM, Attacks, clock Synchronization, GPS, NTP

1. INTRODUCTION

Ad hoc network is a decentralized type of wireless network. In ad hoc network there is no pre-existing infrastructure, such as routers in wired networks or access points in wireless networks. In ad hoc network each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. Basically it's a network which is used in emergency causes. Here is No fixed infrastructure in ad hoc network like base stations as mobile switching. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. 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.

- Passive attacks: A passive attack does not disrupt the normal operation of the network; the attacker spoof the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated.
- 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. External attacks are carried out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Impersonation, modification, fabrication, and replay of packets.

To prevent inside, outside active and passive attack mobile nodes must be mutually authenticated. To provide mutual authentication between the mobile node ALARM protocols is used. ALARM protocol have many assumptions among all one is that clock of the mobile nodes are weakly synchronized by using GPS .In such case the reply attacks can be Possible. ALARM protocol use two technique first is link state routing and other is group signature to provide mutual authentication. If the clocks are strongly synchronized various reply attacks can be prevented .In our work we are using NTP (network time protocol) to provide strong clock synchronization between the mobile nodes.

In this paper ,Literature Review is presented in the section 2. ALARM protocol is discussed in the section 3. New proposed technique is written in the section 4. In the last section future work and conclusion is discussed.

2. LITERATURE REVIEW

In this paper, author had proposed efficient authentication mechanisms for low-power devices. In the proposed scheme the mobile station only need to pass one packet for mutual authentication. They used the elliptic-curve-crypto system based trust delegation Mechanism to generated legation pass code for mobile station authentication. With the use of this authentication mechanism many active and passive attacks will be prevented including denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one packet .This purposed mechanism is required less computations and less message exchange as compared to other authentication schemes [1].

In this paper, they had discussed about the mutual authentication that why mutual authentication is important for wireless sensor networks .They also discussed about the Das protocol which is the

hash-based authentication protocol, this protocol provides the security against the masquerade, stolen-verifier, replay, and guessing attacks. In this paper they had also discussed about the weakness of the das protocol, they had proposed an certain enhancements in the das protocol. The enhanced das protocol is efficient than the traditional das protocol. Enhanced das protocol is reliable protocol and provides more security to the sensor nodes in the insecure environment. The proposed protocol is the energy efficient protocol and require less message exchange and less computations for mutual authentication [2].

In the mobile ad hoc network ,mobile nodes can freely mobile in the environment ,the environment can be secure as well as unsecure. In the unsecure environment ,the certain inside and outside attacks are possible. To prevent the inside and outside attacks we require mutual authentication. If the mobile nodes are mutually authenticated they the inside as well as outside attacks can be prevented. In this paper author had presented the ALARM protocol for mutual authentication in which the mobile presents its secondary identity which will leads to identity untraceable. In this paper the ALARM protocol is for mutual authentication in which certain packets are exchanged for mutual authentication and messages are digitally signature .The digital signature approach will leads to message integrity and confidentiality. It also offers protection against passive and active insider and outsider attacks. [3].

In this paper they had discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes. They had also discuss PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In this paper author proposed a new authentication scheme named as MOCA which hybrid type of scheme and use both PKI and asymmetric schemes for mutual authentication [4].

The main limitation of Kerberos authentication protocol is much number of message exchange is needed for successful authentication and this approach will degrade the battery performance of the hand held devices. Second, disadvantage is the assumptions of the Kerberos authentication protocol when environment changes assumptions are need to change for efficient working of Kerberos protocol. Reply attack, login spoofing, session key expose, password guessing attacks are possible in Kerberos authentication protocol [5].

In this paper author discussed the problem of efficient ALARM protocol for ad-hoc radio networks consisting of devices that try to gain access for transmission through a shared radio communication channel. The problem arises in tasks that sensors have to quickly inform the target user about an alert situation such as presence of fire, dangerous radiation, seismic vibrations, and more. In this

paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots [6].

3. ALARM PROTOCOL

Following are the various assumptions of ALARM protocol

- Location. Universal availability of location information: Each node is deployed in such way that provides accurate positioning information. For example GPS.
- Mobility. Sufficiently high mobility: A certain minimum fraction (or number) of nodes move periodically, such that tracking a given mobile node from one topology snapshot to the next requires distinguishing it among all nodes that have moved in the interim [7].
- Time: All nodes maintain loosely synchronized clocks. This is easily obtainable with GPS [7].
- Range: Nodes have uniform transmission range. Once a node knows the current MANET map, it can determine node connectivity [7].

Goals of ALARM Protocol

Following are the various Goals of ALARM

- Privacy: There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations cannot be linked [7].
- Performance: Security and privacy goals must be achieved without undue sacrifices in performance (i.e., without requiring excessive computations and/ or high delay) [7].
- Security: The network must be resistant to passive and active attacks stemming from both outsiders and malicious e.g. compromised insiders [7].

Details of ALARM

Following are the two operations of ALARM protocol

1. Initialization (Offline)

A. The group manager (GM) initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members. During this phase, each member (node) creates a unique private key that is not revealed to anyone. This key is needed to produce valid group signatures. It also creates a corresponding public key (PK member), that is revealed only to the GM. In addition, each member learns the common group public key (PKGM) that is subsequently used to verify group signatures. In case of a dispute and for offline forensics, GM is responsible for opening any contested group signatures and determining actual signers.

B. Depending on the specific group signature scheme, GM might also handle future joins for new members as well as revocation of existing members. Revocation might not be feasible or desired, since it would require propagating in real time update revocation information to all legitimate nodes. Dynamic membership is necessary.

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-TMPs and SK-TMPs, respectively [7].

Each node broadcasts a Location Announcement Message (LAM), containing its location (GPS coordinates), time-stamp, temporary public key (PK-TMPs), and a group signature computed over these fields [7].

Upon receipt of a new LAM, a node first checks that it has not received the same LAM before; it then verifies the time-stamp and group signature. If both are valid, the node rebroadcasts the LAM to its neighbors. The location is included in the pseudonym in order to minimize required state and assist in the forwarding process. Here the current location concatenated with the group signature in the last Location Announcement Message (TmpID = {Location||GSig}). Including location in the pseudonym speeds up the forwarding process and requires fewer look-ups [7].

Whenever the communication is needed, it checks to see if any node currently exists at (or near) that location. This message is encrypted with a session key using a symmetric cipher. 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 recovers the session key and uses it to decrypt the rest. ALARM is not restricted to any specific public key technique [7]. One obvious choice is Diffie-Hellman half-key. Forwarding: Message forwarding is independent of topology dissemination. The actual path can be computed using the shortest path algorithm or any other location-aided routing algorithm, such as [7]. It generates a session key (Ks) and encrypts data with that key using a symmetric cipher for example AES.

4. PROPOSED TECHNIQUE

The ALARM protocol is used to provide mutual authentication between the mobile nodes. In this paper, we are proposing a new enhancement in the ALARM protocol .One assumption of ALARM protocol is that clocks of the mobile nodes are weakly synchronized .When clocks of the mobile nodes are weakly synchronized reply attack will be possible. To prevent reply attack in mobile ad hoc network strong clock synchronization between the mobile nodes must there .In our work, we are using NTP (network time protocol) to provide strong clock synchronization between the mobile nodes.

5. CONCLUSION AND FUTURE WORK

In this paper, we conclude that mutual authentication is required to prevent various inside and outside attacks. We review the ALARM protocol for mutual authentication. In our work, we

propose new technique to provide strong clock synchronization between the mobile nodes. Our new proposed technique will be based on the NTP protocol. In Future, we implement new proposed technique and compare the results with the previous techniques.

REFERENCES

[1] Jian-zhu Lu and Jipeng Zhou, "On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 3 Issue 2, 71-74, Jun 2013.

[2] Tien-Ho Chen and Wei-Kuan Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", ETRI Journal, Volume 32, Number 5, October 2010.

[3] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada, "On Alarm Protocol in Wireless Sensor Networks", IEEE Conference-Wcnc 2012.

[4] Seung Yi, Robin Kravets. “Key Management for Heterogeneous Ad Hoc Wireless Networks”

[5] System Steven M. Bellovin and Michael Merritt .”Limitations of the Kerberos Authentication”.

[6] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets", IEEE ICNP 2007, pp. 304–313, Oct 2007.

[7] [7] S.Karthiga and V.B.Rosy christiana, "Privacy in suspicious mobile ad hoc network by using Alarm", International Conference on Computing and Control Engineering (ICCCE 2012), April, 2012.