Security in Proactive Mobile Ad Hoc Network Routing Protocols

Mrs. Dhanashree Toradmalle
Assistant Professor,
Shah and Anchor Kutcchhi Engineering College.
Mumbai, India.
Email:sakec.dhanashreet@gmail.com

Mayur Shedage
Student at Shah and Anchor Kutcchhi Engineering College.
Mumbai, India.
Email:shedage.mayur@gmail.com

Nitesh Dogra
Student at Shah and Anchor Kutcchhi Engineering College.
Mumbai, India.
Email:max.james2583@gmail.com

Sanket Gawde
Student at Shah and Anchor Kutcchhi Engineering College.
Mumbai, India.
Email:sanket.sg29@gmail.com

Kumudhan Cherarajan
Student at Shah and Anchor Kutcchhi Engineering College.
Mumbai, India.
Email:kumudhanrajan18@gmail.com

Abstract— A mobile ad hoc network (MANET) is a repetitively self-configuring, mobile wireless node. Routing can takes place proactively (table-driven), reactively (on demand) or in a hybrid manner. This paper, attempts to contribute a discussion on various security issues and various security aspects related to overcome these security issues found in Proactive Mobile Ad Hoc Network routing protocols. This paper also presents a comparison between two proactive routing protocols on various security parameters.

Keywords- *Ad hoc, MANET, proactive, Authenticity, Authorization*

*****

I. INTRODUCTION *TO MANET*

MANET is a group of wireless computing devices like laptop, mobile phone, Personal Digital Assistant (PDA), or similar devices which can communicate directly with one another without a central coordinator(Base Station). A MANET is an autonomous system of mobile routers and associated hosts connected by wireless links.

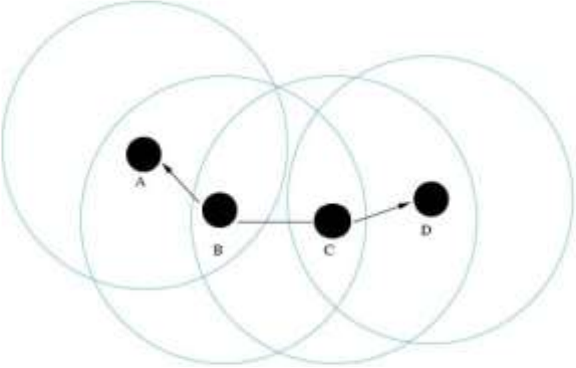

Figure 1 : A Sample Ad hoc Structure

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment. MANETs consist of a one-to-one, independent network.It does not require a fixed network infrastructure due to its wireless nature. They may contain one or more different transceivers between nodes. The growth of laptops and /Wi-Fi wireless networking have made MANETs a popular research topic. MANET has its own routing protocols which can be compromised with route exchange which are frequent, dynamic network structure, bandwidth limitations and multi-hop routing.[1] MANET has three major protocols:

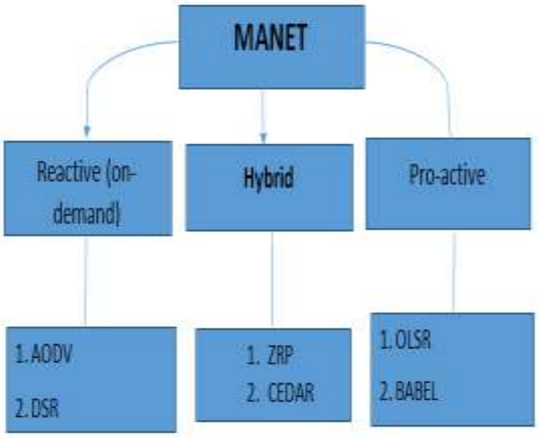

Figure 2: MANET Routing Protocol

II. SECURITY ISSUES IN MANET

The security issues illustrate the vulnerabilities found in Mobile ad hoc networks which degrade the security aspects in MANET. These described security issues needs to be carefully handled in order to make ad hoc network secure.

A. Lack of Secure Boundaries:

This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.[2] In the mobile ad hoc network, there is no need for other node to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with the nodes in its range and hence can join the network automatically. As a result, the MANET does not provide the so-called secure boundary.[2] to protect the network from some potentially dangerous network accesses.

B. *Threats from Compromised nodes Inside the Network*

There are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions[2]. This vulnerability comes from the compromised nodes inside the network. Because of the moving characteristic of the ad hoc network nodes, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Byzantine failures is a good example encountered in the routing protocol for the mobile ad hoc network.[2][3][4] We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among these compromised nodes when they perform malicious behaviors. Hence this failure is very harmful to the mobile ad hoc network.

C. *Lack of Centralized Management Facility*

The absence of centrally managed facility makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic . It is common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently[2]. Lack of centralized management machinery will degrade the feature of trust management for the nodes in the ad hoc network [2].

D. *Networks vulnerable to attacks*

Mobile ad hoc Networks are also prone to some known security attacks which are stated below:

- Denial of Service (DoS)
  Denial of service aims to acquire the availability of certain node or services. In the traditional wired network, the DoS attacks is caused by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable[3][4].
- Impersonation
  Impersonation attack can pose a great challenge to the security of mobile ad hoc network. If there is not a proper authentication mechanism among the nodes, the attacker can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.[3]
- Eavesdropping
  Eavesdropping is another kind of attack that happens in the mobile ad hoc networks. Eavesdropping is practised to obtain some confidential information that should be kept secret during the communication. Because such data are very important to the security state of the nodes, they should be prevented from unauthorized access.[3]
- Attacks against Routing
  In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet delivery[4] . The main aim of attacks on routing protocols is to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations.[4][5]

III. HOW TO SECURE MANET

Following are the various security aspects which acts as a solution to the above discussed issues in Mobile ad hoc network routing protocols:

A. *Availability*

The term Availability means that a node should maintain its ability to provide all the services regardless of the security state of it. This security criterion is faced mainly during the rejection-of-service attacks, in which all the nodes in the network cannot be available the attack target and thus some greedy nodes make some of the network services, such as the routing protocol or other key management service.[3]

B. *Integrity*

Integrity defines the identity of the messages when they are forwarded. Integrity can be compromised mainly in two ways:

Spiteful altering
Accidental altering

A message can be removed by a third party with spiteful goal, which is called as spiteful altering[2] and if the content of the message is changed due to some benign failures, which may be sending errors in communication such as hard disk failure, then it is called as accidental altering.

C. *Authenticity*

Authenticity assures that participants in communication are genuine or not. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is no confirmed mechanism, the competitor could masquerade a liberal node and thus get access to confidential sources, or even generate some fake messages to disturb the network operations.

D. *Authorization*

Authorization defines the permissions the participant has and cannot be prevented, by the licenses authority. Authorization is generally used to assign different access rights to different level of users. For example, we need to confirm that network management function is only accessible by the network management.[2] Therefore there should be an authorization process before the network management accesses the network management functions.

IV. SECURITY PROTOCOLS-A SOLUTION

There are various security protocols used to provide security in mobile ad hoc networks. Some of the protocols are individual security protocol and some acts as an extension or plug-ins along with the MANET Routing algorithms. Some of the featured Mobile ad hoc routing protocols which acts as a solution to the above discussed vulnerabilities found in the MANET Routing protocols are Secure Extension to OLSR protocol(SOLSR) and Authenticated Routing for Ad hoc Networks(ARAN).

A. *Secure Extension to OLSR protocol(SOLSR)*

This mechanism is implemented as an extension to the OLSR protocol. The proposed and implemented mechanism is based on signing each OLSR control packet with a digital signature for authenticating this message[7]. Also, the mechanism provides a timestamp exchange process. The timestamps are used to prevent replay attacks on the routing protocol.

The digital signature is based on symmetric keys. Each node involved in the routing signs the message packet and forwards it. Using this hop-by-hop approach does not provide end-to-end signatures[7], which again means that the digest is not a true signature with respect to the node which originates, but rather a signature from the node which forwards, ensuring that it trusts the source of the message in the previous hop[7]. A node that does not have access to the shared secret key cannot produce a verifiable digest. All receivers running secure OLSR discard messages with non-verifiable digests. SOLSR only provide integrity of the message packets and it does not provide confidentiality.

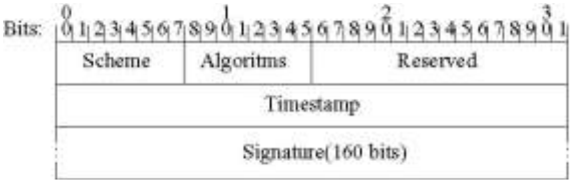

Fig. The basic Signature Message

B. *Authenticated Routing for Ad hoc Networks(ARAN)*

ARAN is based on certificates and successfully defeats all identified attacks. ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication[8]. ARAN is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source[8].

ARAN also prevents Mobile ad hoc networks from different attacks discussed above such as Denial of service(DoS), Attacks through Impersonation etc. Replay attacks are prevented by including a nonce and a timestamp with routing messages[8]. ARAN provides authentication and non-repudiation services using pre-determined cryptographic certificates that guarantees end-to-end authentication

V. COMPARISON TABLE

PARAMETERS	SOLSR	ARAN
Authentication	Does not follow authentication procedure	This provides authentication through certificates
Integrity	Provides integrity	Has built-in integrity support
Confidentiality	Does not support	Provides confidentiality through encryption of message
Prevention of attack	Prevents spoofing attack	Prevention almost all type such as DoS and Impersonation attack

VI. CONCLUSION

In this paper, we have discussed various security issues found in mobile Ad Hoc network and how it can be overcomed. The two security protocols which implement the discussed security aspects play a vital role in Proactive MANET routing protocols. The main security aspects are integrity and confidentiality which can be achieved by implementation of SOLSR and ARAN, as these prevent almost major vulnerabilities in Proactive MANET routing algorithms respectively. The combination of both these security protocols can turn up as a new security criterion which provides both integrity and confidentiality.

REFERENCES

[1] V. Umadevi, Dr. Ramar, Dr.Zaheer , "Security Requirements in Ad hoc Mobile Networks" in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 2, April 2012,Mrs College of Business and Economics, Asmara, State of EritreaJ.

[2] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks - A Survey" Department of Computer Science and Electrical Engineering. University of Maryland, Baltimore County

[3] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah 'SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY'' in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

[4] Sarvesh Tanwar, Prema K.V, ''Threats & Security Issues in Ad hoc network: A Survey Report" in International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[5] Isa Maleki, Ramin Habibpour, Majid Ahadi, Amin Kamalinia ,"SECURITY IN ROUTING PROTOCOLS OF AD-HOC NETWORKS: A REVIEW"in International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.4, August 2013

[6] Shushan Zhao, Akshai Aggarwal, Shuping Liu, Huapeng Wu " A Secure Routing Protocol in Proactive Security Approach for Mobile Ad-hoc Networks" in IEEE.

[7] Andreas Hafslund, Andreas Tønnesen, Roar Bjørgum Rotvik, Jon Andersson and Øivind Kure "Secure Extension to the OLSR protocol'' in OLSR Interop and Workshop, 2004.

[8] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, ElizabethM.Belding-Royer"SecureRoutingProtocolforAdHocNetworks''