Int. Journal of Applied Sciences and Engineering Research, Vol. 3, Issue 6, 2014 www.ijaser.com
 editorial@ijaser.com
Research article ISSN 2277 – 9442

A literature survey of secure routing protocols for MANET

Dinesh[1], Ajay Kumar[2], Jatinder Singh[3]
[1] Assistant Professor, Department of Computer Applications, Sri Sai Iqbal College of Mgmt. & Information Tech. Badhani ,(Punjab),India
[2] Associate Professor, Department of ECE, Beant College of Engg. & Tech., Gurdaspur. (Punjab) India
[3] Principal, KC College of Engg. & IT, Nawashar, (Punjab), India
DOI: 10.6088/ijaser.030600003

Abstract: Mobile Ad hoc Networks (MANETs) suppose no established infrastructure setup is available for routing packets from one node to other node in a network and they rely on intermediate nodes. Nodes in MANET are having a risk of various attacks such as eavesdropping attack, battery draining attack etc. The common target of these attacks is data bandwidth, battery power, routing protocols. This paper gives an overview of secure routing protocols by presenting their important functions, security against various attacks, merits and demerits.

Keywords: ARAN, ARIADNE, SRP, SEAD

1. Introduction

Due to the advancement of radio technologies Bluetooth , IEEE 802.11, Hiperlan , a new concept has been found, known as Mobile Ad-Hoc Networks. In this network, Different Mobile users which arrive within the range of radio link will set up the network for communication. The nodes within radio range can communicate with each other direct wireless links. Therefore, A Mobile Ad-hoc NETwork (MANET) is of a collection of mobile nodes that do networking functions such as packet forwarding, routing and service discovery without a fixed infrastructure. Nodes in MANET depend on each other in routing a packet to its destination because of limited range of each node's wireless range.

A MANET is system of wireless nodes that communicate over wireless links which are having limited bandwidth. Each wireless node can work as a sender, receiver, and router. When a node acts as a sender, it can send message to any destination node with some route. When it acts as a receiver, node can receive messages from any other node in the network. When the node will work as a router, it can send the packet to destination or the next router in the route. MANET has many advantages over traditional wireless networks such as speed of deployment, easy deployment, less dependence on fixed infrastructure. Therefore, there is an emerging wireless networking field for future mobile communications. In moving towards MANET technology, the task of finding good solutions for the challenges such as security, routing, quality of service will play a crucial role for the success of Mobile Ad-hoc Network Technology.

Security is an important and essential component for network functions such as packet forwarding and routing. In this paper, an attempt is done to show various issues for a secure MANET. This paper is organized as follows. Section 1.2 presents various issues regarding security in ad-hoc networks. Section 2 gives us comparison different secure ad-hoc routing protocols.

*Corresponding author (e-mail:dinesha@gmail.com)

Received on June 2014; Published on August 2014

2. Security issues

Mobile ad-hoc wireless does not have any established network and all the services of network are created and configured on the fly. Therefore, due to lack of predefined infrastructure support and wireless attacks, security in ad-hoc network is a weakness. Getting a secured ad -hoc network is challenging due to following reasons.

1. Vulnerable wireless link Active as well as passive link attacks possible in ad-hoc network such as impersonation attack, eavesdropping attack, spoofing attack, and IP spoofing attack.
2. Roaming in dangerous environment any misbehaving node can misguide all other nodes from providing any service.
3. Dynamic topology a network topology in ad-hoc network is very dynamic because mobility of nodes is very random in ad-hoc network. Therefore, there is a requirement that secure solutions should be dynamic.

Following are the main issues in providing secure MANET.

2.1 Identification issue

Nodes in ad-hoc network who have access to radio link can set up ad-hoc network very easily. But for the secure communication among different nodes in ad-hoc network, there is need of secure communication link

1. Before setting up secure communication link, node should be capable to identify other node. It is also necessary that node needs to provide his identity as well as his credentials to the node.
2. The delivered credentials and identity need to be authenticated so that identity and associated credentials cannot be questioned by receiving node, Compromised by receiving nodes.

2.2 Privacy issue

The identification issue at the same time leads to privacy issue for MANET. A mobile node uses many different types of identities that varies from link level to user level. Any frequent mobile node does not want to show his identity as well as credentials to other node from privacy point of view in mobile environment. Any compromised identity leads to create privacy threat to user device by the attacker. Unfortunately, there is no location privacy in current mobile networking standards. Therefore, privacy protection is necessary for secure ad-hoc network environment.

3. Secure routing protocols

The following are the various secure routing protocols along with features in terms of their merits and demerits they possess and they are defined in this paper along with their features. All protocols are based upon routing protocols such as DSR, DSDV etc.

3.1 ARAN

3.1.1 Introduction

The ARAN is an on demand secure routing protocol that detects against the malicious actions taken by the third parties in an ad-hoc network. ARAN gives security services like authentication, non repudiation and message integrity as part of minimum security policy. ARAN requires the need of trusted certificate server (T) before joining the ad-hoc network. In ARAN, each node has to request a certificate from the trusted certificate server T. The certificate possesses the IP address of the node, time stamp when the certificate was made, its public key, a time when the certificate expires. It is supposed that all the nodes are having fresh certificates from the trusted certificate server and must know public key of certificate server T.

In any secure system based on cryptographic certificates, main issue of revoked certificates should be addressed so that nodes having revoked certificates do not use the network. In this protocol, when a certificate will be cancelled, the trusted certificate server T sends a message which is broadcasted to all the nodes of the ad-hoc network that announces the revocation. Any node getting this message rebroadcasts this message to all its neighbors. Revocation messages should be stored until revoked certificate has been expired normally. Any neighbor of the node having revoked certificate needs to modify routing to avoid transmission through un-trusted node.

3.1.2 Characteristics

1. The ARAN protects against fabrication attacks, modification attacks, and impersonation attacks
2. ARAN is not immune to wormhole attack
3. ARAN uses asymmetric cryptography which is very costly in terms of CPU and energy usage.

3.2 ARIADNE

3.2.1 Introduction

ARIADNE is an on demand secure routing protocol which is based on DSR (Dynamic Source Routing) routing protocol and uses highly efficient symmetric cryptography. ARIADNE guarantees that receiving node of a route discovery process will authenticate the source and source node can authenticate each intermediate node on the way to destination present in RREP message. ARIADNE needs some mechanism for authentic keys required by the protocol. Each node in the ad-hoc network needs a shared key $K_{S,D}$ between the source S and destination D and a TESLA key for each computer in the network.

3.2.2 Characteristics

1. ARIADNE gives us node to node authentication of a routing message using MAC[12] code and shared key between sender and receiver.
2. ARIADNE uses TESLA key for the authentication of RREQ packet.
3. ARIADNE is immune to modification attacks, fabrication attacks, impersonation attacks and wormhole attack.
4. ARIADNE is also immune to cache poisoning attack which could lead to flood of RREQ packets.
5. ARIADNE is immune to wormhole attack using an extension called TESLA with Instant Key disclosure

3.3 SEAD

3.3.1 Introduction

SEAD is a proactive secure routing protocol given by Hu, Perrig and Johnson. This protocol is based on the proactive routing protocol Destination-Sequenced Distance Vector protocol(DSDV)[13]. In this routing protocol each node exchange routing information periodically with all the other nodes in the network so that each node always has a route to all the other nodes in the network. SEAD authenticates sequence number field and metric field of a routing table using the hash chain technique. In this protocol, destination node also authenticates the sender to confirm that routing information comes from correct node. The source of each routing message should be authenticated to prevent impersonation attack.

3.3.2 Characteristics

1. SEAD deals with the attacks that modify routing information broadcasted during update of DSDV-SQ protocol such as to prevent attacks which modify sequence number and metric field in routing table update.
2. ii)SEAD uses efficient one way hash chain technique rather than expensive asymmetric cryptography operations.
3. SEAD supposes some technique for a node to give an authenticed element of hash chain which can authenticate all other elements of chain.
4. SEAD is not immune to wormhole attack.

3.4 SRP

3.4.1 Introduction

The Secure Routing Protocol (SRP) was a protocol compatible with many reactive routing protocols. SRP was immune to attacks that disrupt the route discovery process. SRP allows the source of a route discovery to discard bogus replies. SRP depends upon the Security Association (SA) between Source (S) and destination node (D). SA can be made by using hybrid key distribution which was based on the public keys of Source node (S) and Destination node (D). S and D can use a secret symmetric key ($K_{S, D}$) using the public keys of one another.

3.4.2 Characteristics

1. SRP is immune with malicious nodes that can modify, fabricate, and replay routing packets.
2. SRP is immune to IP spoofing attack because neighbor discovery mechanism will bind the medium access control and IP addresses of nodes.
3. With the DSR(Dynamic Source Routing). SRP uses a six word header Containing unique identifiers that tag MAC code and discovery process.
4. SRP suffers from route cache poisoning attack.
5. SRP suffers from validation mechanism for route maintenance messages.
6. SRP is not immune to wormhole attack.

4. Conclusions

Due to available computing hardware and wireless networking, we are capable of using the Mobile Ad-hoc Network Technology. Therefore, there is need to design and develop routing protocols which can support performance with security. The accurate execution of these secure routing protocols is necessary for proper functioning of a MANET. A number of protocols have been proposed for securing MANETs but no comparison of their performance has previously available. In the current work, we have compared various secure routing protocols by showing their characteristics, differences and features. It can be summarized that each protocol has definite merits and demerits, and can be suitable for a specific application environment.

Acknowledgement

I am thankful to Punjab Technical University, Jalandhar which gives me opportunity to do research work as a research scholar.

5. References

1. Chatshik bisdikian, 2001. An Overview of the Bluetooth wireless technology, IEEE Communication Magazine, 39(12), 86-94.
2. Brian P. Crow, Indra Widjaja, Jeong Geum Kim, Prescott T. Sakai, 1997. IEEE 802.11 Wireless Local Area Networks. IEEE Communication Magazine, 35(9), 116-126.
3. Doufexi A., Armour S., Butler M, Nix A., Bull D., 2001. A Study of the Performance of HIPERLAN/2 and IEEE 802.11a Physical Layers. IEEE VTC'01, 668- 672.
4. Perkins C.E, 2000. Ad Hoc Networking, Addison-Welsey Longman.
5. Dahill B, Levine B. N, E. Royer, Shieldsr C, 2002. ARAN : A Secure Routing Protocol for Ad Hoc Networks. UMass Tech Report, 02-32.
6. Hu Y.C, Perrig A. and Johnson D. B, 2002. Ariadne : A Secure On-Demand Routing Protocol for Ad hoc Networks. Proc.ACM Int'l. Conf. Mobile Computing & Networking (Mobicom'02), Atlanta, Georgia, 12-23.
7. Hu Y.C, Perrig A. and Johnson D. B, 2002. SEAD : Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proc. 4th IEEE Workshop On Mobile Computing Systems and Applications, Callicoon, NY , 3-13.
8. Papadimitraos P, Haas Z. J, and Samar P, 2002. The Secure Routing Protocol (SRP) for Ad Hoc Networks. Draft-papadimitratos-secure-routing-protocol 00.txt.
9. Zapata M.G, 2001. Secure ad-hoc on-demand distance vector (SAODV) routing, IETF MANET, internet draft (Work in progress),draft-guerrero-manet-saodv- 00.txt.
10. Yi S, Naldurg P, Kravets R, 2001. Security aware ad-hoc routing for wireless networks. Proc. Of the 2nd ACM international Symposium on Mobile Ad- hoc networking and Computing (Mobi-Hoc'01), 299-302.
11. Papadimitraos P,and Haas Z, 2003. Secure link state routing for mobile ad-hoc networks. Proc. of Symposium on Applications and internet Workshops (SAINT'03), 379-383.
12. Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications. June 2003 http//standards.ieee.org/getieee802/download /802.11-1999.pdf-accessed 10/10/2006.

13. Perkins C., and Bhagwat P, 1994. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. ACM SIGCOMM.