IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
ISSN (Online): 2231-5268
www.ijcsms.com

A LITERARY REVIEW OF MANET SECURITY PROTOCOLS

Krishan Kumar[1], Yogesh Kumar[2], Gaurav Pruthi[3]

[1]Sr. Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat)
krishankumar2005@gmail.com

[2]Sr. Lecturer in CSE Deptt., BPR College of Engg. Gohana (Sonipat)
yogs_crsce@yahoo.com

[3]Assistant Prof in CSE Deptt, Gurgoan College of Engg., Gurgoan
pruthi.gaurav@gmail.com

Abstract

Ad hoc networks offer various applications which are very much essential in wireless networks. But the vital problem concerning their security aspects is the major issue which must be solved. A mobile adhoc network is a collection of nodes that are connected through a wireless medium forming rapidly changing topologies. The dynamic and cooperative nature of ad hoc networks present challenges in securing these networks. Attacks on ad hoc network routing protocols is the main problem which affects the network performance and reliability. Here a brief introduction is made of the most popular protocols that follow the table-driven approach and the source initiated on-demand approach.

KEYWORDS: *Wireless Network, Ad hoc Network, Security, Secure Routing Protocols.*

1.0 Introduction

Mobile ad hoc networks consist of nodes that communicate through the use of wireless mediums and form dynamic topologies. They lack in any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks, is the basic characteristic of these networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform towards routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority, since one does not exist.

Unfortunately most of the widely used ad hoc routing protocols have less security considerations and trust all the participants to correctly forward routing and data traffic. This assumption can prove to be disastrous for an ad hoc network that relies on intermediate nodes for packet forwarding.

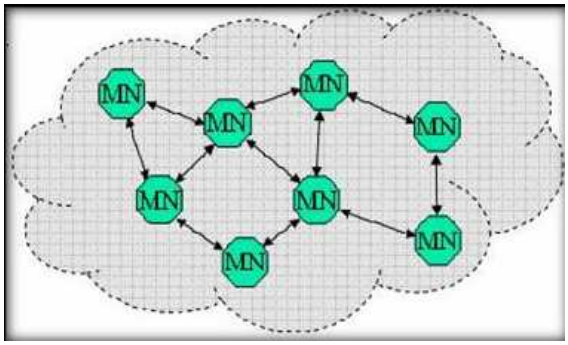

Fig MANET

This paper emphasizes the on demand secure routing with a peep into the working of existing secure routing protocols and also enlightens the characteristics off each one. Rest of the paper is organized as: section 2 is security challenges in MANET, section 3 gives security goals, Section 4 describes survey of protocols and conclusion is in section 5.

2.0 SECURITY CHALLENGES IN AD HOC NETWORK

Routing in mobile ad hoc networks is gripped with additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. There are several well known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth and high error rates [2].

Most of the existing routing protocols follow two different design approaches to confront the inherent

characteristics of ad hoc networks, namely the *table-driven* and the *on-demand* approaches[15].

Some popular protocols in these categories are DBF, WRP, DSDV, OLSRP and AODV, DSR, DDR and TORA in their respective categories.

Roaming freely in a hostile environment with relatively poor physical protection nodes have non-negligible probability of being compromised. Hence, we need to re-consider malicious attacks not only from external but also those from within the network from compromised nodes. Security can be breached through the following ways [12]:

Vulnerability of Channels: Messages can be eavesdropped as in any wireless network, and fake messages can be injected into the network without the difficulty of having physical access to network components.

Vulnerability of nodes: Since the network nodes usually do not reside in physically protected places, such as locked rooms, they are more prone to being captured and falling under the control of an attacker.

Absence of Infrastructure: Ad hoc networks are supposed to operate independently of any fixed infrastructure. The classical security solutions based on certification authorities and on-line servers are rendered inapplicable in the absence of Infrastructure.

Dynamically Changing Topology: The permanent changes of topology require sophisticated routing protocols, in mobile ad hoc networks the security of which is an additional challenge. A peculiar difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the dynamic and not static and should be scalable.

3.0 SECURITY GOALS

There are some goals that need to be achieved in case of secured routing some of these are:

· **Availability:** Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

Integrity: Message being transmitted is never corrupted.

Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Non-repudiation: Ensures that the origin of a message cannot deny having sent the message.

Non-impersonation: No one else can pretend to be another authorized member to learn any useful information.

Attacks using fabrication: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

3.1 ATTACKS ON AD HOC NETWORK

There are various types of attacks on ad hoc network which can be described as:

• **Location disclosure [14]:** The privacy requirements of an ad hoc network are targeted under location disclosure. In this attacker is able to discover the location of a node, or even the structure of the entire network Through the use of traffic analysis techniques, or with simpler probing and monitoring approaches.

• **Black hole***:* In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fabricated fake replies divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

• **Replay:** Routing traffic that has been captured previously is injected into the network in a replay attack. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

• **Wormhole:** The wormhole attack is one of the most powerful ones since it involves the cooperation between two malicious nodes that participate in the network.

• **Blackmail:** A blackmail attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender.

• **Denial of service:** Denial of service attacks are aimed at the complete disruption of the routing function and therefore the whole operation of the ad hoc network.

• **Routing table poisoning:** Routing protocols are maintained tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes.

4.0 SECURE ROUTING PROTOCOLS

Some of the popular protocols which come under secured ones have been discussed here.

(i) ARAN [17]

Authenticated Routing for Adhoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Adhoc environment. Authentication, message integrity and non-repudiation to an Ad-hoc environment are introduced by ARAN. ARAN is composed of two distinct stages. The first stage is simple and requires little extra work from peers beyond traditional Adhoc protocols. Nodes performing the optional second stage increase the security of their route, but incur additional cost for their ad hoc peers who may not comply.

Characteristics:-

This protocol is capable only for defense against the two attacks namely Replay and Routing table poisoning. The remaining attacks cannot be defended by it.

(ii) SEAD [17]

Our Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network. To support use of SEAD with nodes of limited CPU processing capability and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions

Characteristics:-

SEAD protocol is capable for defense against the three attacks namely Replay, Denial-of-Service and Routing table poisoning. The remaining attacks cannot be defended by it.

(iii) SRP [13]

Secure Routing Protocol (Lightweight Security for DSR), can be use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP doesn't attempt to secure ROUTE ERROR packets but instead delegates the route maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. To ensure Freshness SRP uses a sequence number in the REQUEST but this sequence number can only be checked at the target. SRP requires a security association only between communicating nodes and uses this security association just to authenticate ROUTE REQUESTS and ROUTE REPLYS through the use of message authentication codes. At the target, SRP can detect modification of the ROUTE REQUEST, and at the source, SRP can detect modification of the ROUTE REPLY. Since SRP requires a security association only between communicating nodes, it uses extremely lightweight mechanisms to prevent other attacks.

Characteristics:-

SRP protocol is capable for defense against the three attacks namely Replay, Denial-of-Service and Routing table poisoning. The remaining attacks cannot be defended by it.

(iv) SECURE AODV [13]

The SecAODV implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust. The SecAODV implementation follows Tuominen's design which uses two kernel modules ip6_queue, ip6_nf_aodv, and a user space daemon AODV. A 1024-bit RSA key pair is then generated by the AODV daemon. The securely bound global and site-local IPv6 addresses are generated using the public key of this pair.

Characteristics:-

SAODV protocol is capable for defense against the two attacks namely Replay and Routing table poisoning remaining attacks cannot be defended by it.

(v) BISS [17]

Building Secure Routing out of an Incomplete Set of Security Associations (BISS), Even when prior to the route discovery, only the receiver has security associations established with all the nodes on the chosen route the sender and the receiver can still establish a secure route. Thus, the receiver will authenticate route nodes directly through security associations. The sender, however, will authenticate directly the nodes on the route with which it has security associations, and indirectly (by exchange of certificates) the node with which it does not have security associations. Mechanisms similar to direct route authentication protocols determine the operation of BISS ROUTE REQUEST. When an initiator sends a ROUTE REQUEST, it signs the request with its private key and includes its public

key *PKI* in the request along with a certificate *cl* signed by the central authority binding its id with *PKI.*

Characteristics:-

This protocol is capable for defense against the two attacks namely Replay and Routing table poisoning. The remaining attacks cannot be defended by it.

(vi) SLSP [16]

The Secure Link State Protocol (SLSP)] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within *R* hops, which is termed as their *zone.* Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (*LSU*) packets from malicious alteration, as they propagate across the network.

Characteristics:-

This protocol is capable for defense against the three attacks namely Replay, Denial-of-Service and Routing table poisoning. The remaining attacks cannot be defended by it.

(vii) ARIADNE [17]

A Secure On Demand Routing Protocol for Ad Hoc Networks (ARIADNE) using the TESLA broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication. Adding a MAC (computed with a shared key) to a message can provide secure authentication in point-to-point communication; for broadcast communication, however, multiple receivers need to know the MAC key for verification, which would also allow any receiver to forge packets and impersonate the sender.
Secure broadcast authentication an asymmetric primitive, such that the sender can generate valid authentication information, but the receivers can only verify the authentication information. TESLA differs from traditional asymmetric protocols such as RSA in that TESLA achieves this asymmetry from clock synchronization and delayed key disclosure, rather than from computationally expensive one-way trapdoor functions.

Characteristics:-

This protocol is capable for defense against the three attacks namely Replay, Denial-of-Service and Routing table poisoning. The remaining attacks cannot be defended by it.

(viii) SAR [16]

Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. We assume that the base protocol is an on demand protocol similar to AODV or DSR. In the original protocol, when a node wants to communicate with another node, it broadcasts a Route Request or RREQ packet to its neighbors.

Characteristics:-

This protocol is capable for defense against the two attacks namely Replay and Routing table poisoning. The remaining attacks cannot be defended by it.

5.0 CONCLUSION

An attempt has been made to present an overview of the existing security scenario in the Ad-Hoc network environment. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks.
Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats.

6.0 References:

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad hocNetworks,” Proc. 6th Annual ACM/IEEE Int’l. Conf. Mobile Computing and

Networking (Mobicom'00), Boston, Massachusetts, August 2000, pp. 255-265.

[2] E.M. Royer, and C.-K. Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," IEEE Personal Communications, vol. 2, no. 6, April 1999, pp. 46-55.

[3] S. Ramanathan, and M. Steenstrup, "A Survey of Routing Techniques for Mobile Communications Networks," Mobile Networks And Applications, vol. 2, no. 1, October 1996, pp. 89-104.

[4] T. Clausen, P. Jacquet, and L. Viennot, "Comparative Study of Routing Protocols for Mobile Ad hoc Networks," Med-Hoc-Net'02, Sardegna, Italy, September 2002, 10 pp.

[5] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," Proc. ACM Conf. Communications Architectures and Protocols (SIGCOMM'94), London, UK, August 1994, pp. 234-244.

[6] T. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The Optimized Link State Routing Protocol – Evaluation Through Experiments and Simulation," Proc. 4th Int'l. Symp. Wireless Personal Multimedia Communications, Aalborg, Denmark, September 2001, 6 pp.

[7] C.E Perkins, and E.M. Royer, "Ad hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[8] D.B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[9] F. Anjum, Anup K. Ghosh, nada golmie, paul kolodzy, radha poovendran, rajeev shorey, d.Lee, j-sac, "Security in Wireless Ad hoc Networks", ieee journal on selected areas in communications, vol. 24, no. 2, February 2006.

[10] H.-A. Wen, C.-L. Lin, and T. Hwang, "Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients," Computers and Security, vol. 25, pp. 106-113, 2006.

[11] Yih-chun hu, adrian perrig, "A Survey of Secure Wireless ad hoc routing" IEEE security & privacy May-June 2004

[12] Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93-B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.

[13] A. Kush, P. Gupta, A. Pandey, C. J. Hawang, "Power Aware Virtual Node Routing Scheme in Ad Hoc networks", IASTED International Conference on Wireless Networks and emerging Technologies(WNET 2004) , Banff, Canada , pp. 698-704, July 2004

[14] A.Kush, V.Rishiwal, "A SECURE ROUTING PROTOCOL FOR WIRELESS AD HOC NETWORKS" in the Proceedings of International Cryptology Workshop and Conference 2008 (cryptology2008) held in Malaysia, ICIIS 2008.

[15] A.Kush "Security Aspects in AD hoc Routing", Computer Society of India Communications, Vol no 32 Issue 11, March 09 pp 29-33.

[16] A.Kush "Security and Reputation Schemes in Ad-Hoc Networks Routing" International Journal of Information Technology and Knowledge Management January June 2009, Volume 2, No. 1, pp.185-189.

[17]. A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3 pp 1793-1799, ISSN: 1793-821X