Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks

Ashwani Garg
M Tech, Department of Computer Science & Engineering
N C College of Engineering, Israna, Panipat
Haryana, India

Vikas Beniwal
Assistant Professor, Department of Computer Science & Engineering
N C College of Engineering, Israna, Panipat
Haryana, India

Abstract -- A Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. There are a number of routing protocols developed by researchers. Due to the nature of ad hoc networks, secure routing is an important area of research in developing secure routing protocols. Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary points of concern in implementing these protocols. This paper presents some of the available secure routing protocols and most common attack patterns against ad hoc networks. Routing protocols are subjected to case studies against the most commonly identified attack patterns such as: denial-of-service attack, tunneling, spoofing, black hole attack and wormhole attack etc.

Keywords -- Security attacks, Security Issues, Routing Protocols

I. INTRODUCTION

In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organized networks. Ad hoc networks are simple peer-to-peer networks, self-organized and with no fixed infrastructure. They are used in military oriented tactical operations, for emergency law enforcement, and in rescue missions. Confidentiality, integrity, availability, non-repudiation and authentication are the basic requirements of information security [2]. Ad hoc network's dynamic topology with no centralized administration makes it highly vulnerable for its security-breach, particularly secure routing in ad hoc networks has been a challenging task for researchers. Currently researchers are proposing a variety of secure routing protocols to meet their specified security requirements. In these proposals, different secure protocols fulfill different security requirements and counter against certain attack patterns. Researchers evaluate these protocols in context to how resistant these are, to security attacks and performance appraisal is done through simulation.

II. REVIEW OF ROUTING PROTOCOLS

In MANETs, some form of routing protocol is required in order to dynamically detect the multi-hop paths through which packets can be sent from one node to another [1]. There are basically two categories of routing protocols for MANETs:

1. Table Driven (Proactive): DSDV, GSR, WRP
2. Source Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR

Much of the research has been done focusing on the efficiency of the MANETs. There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirements of these protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP). Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary point of concern in implementing these protocols. Hence, there is a need for review.

III. SECURITY ATTACKS

Mobile ad hoc network can be subject to many types of attacks. In Mobile ad hoc network, attacks can be classified into Passive Attacks and Active Attacks. Brief introduction of both attacks are as follow:

A. Passive Attacks

In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic [11]. The attacker only looks and watches the transmission and does not try to modify or change the data packets. Two types of passive attacks are:

1. Traffic analysis

In this attack, attacker monitors packet transmission to infer important information such as a source, destination and source-destination pair.

2. Eavesdropping

In Eavesdropping, attackers obtain some confidential information e.g. private key, public key, location or even password of the node that should be kept secret during transmission.

B. Active Attacks

In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks. Various types of active attacks are:

1. Sinkhole Attack

A sinkhole node tries to attract the data toward itself from all neighboring nodes. In this attack, a malicious node generates fake routing information and show itself as legal nodes for the route. Sinkhole node attempts to draw all network traffic according to itself, modifies the data packets, decrease the network life time, create complicated network and finally destroy the network.

2. Flooding Attack

In this attack, a malicious node may also inject false packets to consume the available resources onto the network, so that valid user can not able to use the network resources for valid communication [8].The flooding attack is possible in all most all the on demand routing protocols such as SRP, SAODV, ARAN etc.

3. Replay

This attack usually targets the freshness of routes. In this attack an attacker firstly record the message and then resend the old message to the other nodes to make update their routing table to stale routes.

4. Rushing Attack

In Rushing attack, attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node .By this way rushing attack can slow down the performance of network .The rushing attack can act as an effective DoS attack against all currently proposed on demand MANET routing protocol[6][7].

C. Common attacks in MANETs

1. Denial-of-service with modified source route

In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service.

2. Tunneling Attack

In tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes.

3. Wormhole Attack

In Wormhole an attacker records packet at one location in the network, tunnels them to another location, and retransmits them back into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality

4. Black hole Attack

In Black hole attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept and in this way it can compromise the service[4][5].

5. Spoofing Attack

In Spoofing a single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it. Later the information can be used to create DoS attacks.

IV. CASE STUDIES OF ATTACK PATTERNS ON ROUTING PROTOCOLS

A. Secure Efficient Ad hoc Distance Vector (SEAD)

SEAD was developed based on Destination Sequence Distance Vector (DSDV) and incorporates One-Way Hash function [9] to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbor authentication through Hash functions, an attacker can not compromise any node. SEAD is prone through wormhole attack. Even if authentication is provided using hash functions, a wormhole attack is possible through tunneling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination.

Routing table overflow attacks are possible in SEAD, as SEAD is developed based on a table driven approach. A compromised node can advertise routes to nodes which are not in the network and there by fill in the space allocated in the routing table with false node routes. Spoofing attack is possible through compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Black hole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunneling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats.

B. Ariadne

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MACs and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime [10]. Wormhole attacks are possible in Ariadne through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

C. Secure routing protocol (SRP)

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbors and maintain a priority ranking inversely proportional to the query rate. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis is similar to Ariadne as it is based on DSR protocol.

D. Authenticated Routing for Ad hoc Network (ARAN)

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbor node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network.

Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern. Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, black hole attacks are impossible due to node level authentication with signatures.

E. Secure Ad hoc On-Demand Distance Vector Routing (SAODV)

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts [12]. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible replay attacks.

V. CONCLUSIONS

This paper discusses common possible attacks on different protocols being used in MANETs. We have tried to analyze them so as to prevent the attacker to intrude in wireless networks. There are lots of techniques with which, one can easily detect most of the attacks. One can choose them in accordance with the protocol being used in the network. However, no protocol is fully secure from attacks being encountered in the MANETs. Hence, one must choose a combination of techniques intelligently to avoid any attack and make the network fully secure.

REFERENCES

[1] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011

[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).

[3] Hao Yang, Haiyun Luo, Fan Ye, songwu Lu and Lixia Zhang,"Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol. 11,(2004) pp. 38-47.

[4] Hoang Lan Nguyen, Uyen Trang Nguyen " A study of different types of attacks on multicast in mobile ad hoc networks" , Journal of Ad hoc Networks, Vol. 6,(2006),pp. 32-46.

[5] Sudhir Agarwal,Sanjeev Jain, sanjeev Sharma,"A survey of Routing attacks and security Measures in mibile adhoc networks",Journal of computing , Vol 3, Issue 1,(2011), pp. 41-48.

[6] Bing Wu,Jianmin Chen,Jie Wu, Mihaela cardei ,"A survey on Attacks and Countermeasures in Mobile ad hoc networks",Wireless/Mobile network security, Springer,(2006).

[7] Manel Guerrero Zapata, N. Asokan in Nokia research center and was submitted to WiSe'02, September 28, 2002, Atlanta, Georgia, USA".

[8] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).

[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[10] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.

[11]Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang [2005]. "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05).

[12] Anand Patwardhan, Jim Parker and Anupam Joshi**.** "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/ Publications/ nist-umbc-adhocids-ipv6.pdf.

[13] Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[14] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edition). [2004]. Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354) C. Siva Ram Murthy and B.S. Manoj. [2004]. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526).

