Analysis of Network Layer Attacks on Secure Routing Protocol in MANET

Rashmi Jatain
B.Tech, M.Tech , CSE

Abstract— An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Due to the nature of ad hoc networks, secure routing is an important area of research in developing secured routing protocols. Although researchers have proposed several secure routing protocols, their resistance towards various types of attacks and efficiency are primary points of concern in implementing these protocols. Some of the available secure routing protocols and most common network layer attacks against mobile ad hoc networks are evaluated. Secure routing protocols are analysed against the most commonly identified network layer attacks such as: denial-ofservice attack, tunneling, spoofing, blackhole attack and wormhole attack and their comparative analysis is also done
Keywords— MANET, Secure Routing Protocols, Network Layer Attacks and Analysis.

Introduction- 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-organised networks. Ad hoc networks are simple peer-to peer networks, self-organised and with no fixed infrastructure. Ad-hoc network is a concept in computer communication which means that user wants to communicate with each other to form a temporary network, without use of centralized administration. Each node in the network acts both as host and router and must therefore willing to forward packet for other node.[1] A Mobile Adhoc Network (MANET) is a temporary wireless network composed of mobile nodes without any permanent infrastructure. Each node not only operates as an end system, it also acts as a router to forward packets on behalf of other nodes [1]. One of the best features of MANET is its flexibility and can configure itself in the fly and thus very suitable for the emergency situation. Most common issues related to nodes in MANETs are limited resources such as battery backup, limited range etc., dynamic topology i.e number of nodes keeps on changing on the fly and address assignment as allocating address to different nodes successfully. Wireless channels are also facing some issues such as Relatively High Error Rate, High variability in the quality, Low bandwidth, Broadcast Nature and Security Aspects [2]. 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 [3][4]. To address these concerns, several secure routing protocols have been developed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), Secure Routing Protocol (SRP), Security-Aware Routing Protocol (SAR) [5][6][7]. The goal of this paper is analyse secure routing protocols in MANET against network layer attack patterns in ad hoc environment based on the literature study[8][9][10] . From literature is concluded that none of secure routing protocol is secure enough against various attacks. The secure-protocol development has become the most challenging task in securing ad hoc networks. Most of these existing protocols have been developed based on specific security scenarios. So the main purpose of this research is to understand more deeply and analyse MANETs secure routing protocols with network layer attacks [11][12][13. This section contains basic about MANETs, related issues, section 2 contains details about various network layer attacks, section 3 has discussed secure routing protocols, section 4 contains analysis of secure routing protocols with network layer attacks, and section 5 contains comparative analysis of secure routing layer protocols followed by conclusion and references.

1. Network Layer Attacks -

In ad hoc networks, attacks can be classified into active and 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. An active attacker injects packets into the network, eavesdrops and also tries to compromise the network with denial of service. 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 [14][15][16]. Most common network layer attacks identified in ad hoc network environment are as Denial-of-service with modified source route, Tunnelling, Spoofing, Black hole attack, Wormhole attack and Routing table overflow attack [17][18][19].

Denial-of-service with modified source route: A denial of service attack in general could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could break down highlevel services. In the routing mechanism a source node sends route request messages to all neighbours to find a route to the destination node. In the denialof-service case a malicious node in between can successful send an erroneous route message to the source route to disrupt the services [11][17].

Tunnelling: Ad hoc networks have an implicit assumption that any node can be located adjacent to any other node. A tunnelling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The vulnerability is that two such nodes may collaborate to falsely represent the length of available paths by encapsulating and tunnelling the routing message between them**.**

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**.**

Blackhole: 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 [2].

Wormhole: 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].

Routing tables overflow attacks: Routing tables overflow attack attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. The proactive algorithms are more vulnerable to table overflow attacks than reactive algorithms because they attempt to discover routing information with time intervals [5].

2. Secure Routing Protocols in MANETs

There are several secure routing protocols proposed basing on the working principles of the earlier ad hoc protocols [2][7][10].

SEAD: (Secure efficient ad hoc distance vector routing protocol)

SEAD is designed based on the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was proposed by Yih-Chun Hu, David B. Johnson and Adrian Perrig, [3]. SEAD incorporates One- Way Hash function [4] to authenticate in the routing update mechanism to enhance the routing security.

ARIADNE:

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig [3], based on the Dynamic Source Routing protocol (DSR). [4][5][7]. Ariadne uses the basic routing mechanism of DSR and uses TESLA [6] broadcasting authentication protocol. Ariadne provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the pair of communicating nodes.

SRP: Secure Routing Protocol

SRP was proposed by Papadimitratos and Hass [8]. SRP is implemented over DSR [4], [5], with an underlying Security Association (SA) between the source and destination nodes. The trust relation is maintained with a public key infrastructure and a shared key K(sd), was maintained between the source and destination nodes using the security association.

ARAN:Authenticated routing for Ad hoc Network

Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M.BeldingRoyer developed Authenticated routing for Ad hoc Network [9] based on AODV [4][5][11] using Certificates with a Central Certification Authority. ARAN is based on Cryptographic Certificates and relies on a central trusted Certification Server (T).

SAODV: Secure Ad hoc On-Demand Distance Vector Routing

SAODV is a secure routing protocol developed based on AODV. SAODV was developed by Manel Guerrero Zapata, N. Asokan [13]. SAODV in its implementation assume that there is already a central key management system through which every node can obtain public keys. Digital signatures are used to authenticate the fields of the message and hash chains to secure the hop count information.

SAR: Security- Aware Routing Protocol

Seung Yi, Prasad Naldurg and Robin Kravets [14] developed SAR. So directly look into the secure mechanism incorporated by SAR over AODV. SAR uses Security as on of the Key Metrics in its route discovery and maintenance.

3. Analysis of Secure Routing Protocols against Network Layer Attacks

SEAD Analysis

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 neighbour 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 tunnelling 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. Blackhole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunnelling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats.

Ariadne Analysis

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. Wormhole attacks are possible in Aridane 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**.**

SRP Analysis

The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbours 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. As SRP and Ariadne are based on DSR protocol, so other features for analysis are similar in both algorithms.

ARAN Analysis

Aran uses public key cryptography and a central certification authority server for node authentication and neighbour node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbour 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. Tunnelling attacks are possible in ARAN. Two compromised neighbour 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, blackhole attacks are impossible due to node level authentication with signatures.

SAODV Analysis

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. Tunnelling 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 reply attacks.

SAR Analysis

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. The security of SAR in terms of trust level and message integrity is evaluated as under: Trust Level: SAR routing mechanism is based on the behaviour associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust- based hierarchy, cryptographic

techniques like: encryption, public key certificates, shared secrets, etc. are employed. Message integrity: The compromised nodes can utilize the information flow in between nodes and reading of packets to launch attacks. It results in corruption of information, confidentiality of the information, and in denial of network services.

4. CONCLUSION

Securing ad hoc environments is a challenging task. The main purpose of this paper work was to acquire in-depth knowledge of ad hoc routing protocols and secures routing protocols. Security analysis of some of the secure routing protocols are done against most commonly identified network layer attack patterns in mobile ad hoc networks. In the secure routing protocols most of the security attacks are possible with a compromised node. From the network layer attacks analysis, it is concludes that table driven protocols are more prone to security attacks than on demand driven protocols. Protocols based on DSR and AODV are more stable to security attacks due to the strong cryptographic implementation. Research in this area of ad hoc secure routing protocols is still very actively and further we can implement secure routing protocols.

REFERENCES

[1] Seema, Yudhvir Singh, Vikash Siwach, ―Quality of Service in MANET‖, International Journal of innovations in Engineering and Technology (IJIET), ISSN: 2319-1058, pp 28-31, (October 2012).

[2] Gopal Singh, Yudhvir Singh, Dheer Dhwaj Barak, ―Analysis of Secure Routing Protocols in Mobile Adhoc Networks‖, International Journal of Science, Engineering and Computer Technology, ISSN – 2231-508X, Vol 2, Issue 1, pp 142-145, (March 2012).

[3] 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), (2002).

[4] Preeti, Yogesh Chaba, Yudhvir Singh, ―Review of Detection and Prevention of DDOS attack in MANET‖, Proc. National Conference on Challenges &Opportunities in Information Technology(COIT – 2008), India, pp. 56-59 (March

[5] Yogesh Chaba, Yudhvir Singh, Manish, ―Performance Evaluation and Analysis of Cluster Based Routing Protocols in MANETs‖ Proc. IEEE/ACEEE ACT 2009, India[Online : IEEE Xplore Digital Library, Digital Object Identifier: 10.1109/ACT.2009.26], pp. 64-66, Available: http://ieeexplore.ieee.org/ (2009)

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

[7] Yogesh Chaba, Yudhvir Singh, Aarti, ―Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs‖ International Journal of IT & Knowledge Management (ISSN: 0973-4414) Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[8] Panagiotis Papadimitratos and Zygmunt J. Haas, ―Security in Mobile Adhoc Networks‖, Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, (January 27-31, 2002).

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

[10] M. Abolhasan, T. Wysocki and E. Dutkiewicz, —A review of routing protocols for mobile ad hoc networks‖, Ad Hoc Networks, pp. 1–22, (2004).

[11] Yogesh Chaba, Yudhvir Singh, Preeti, —Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET‖ International Journal of Networks, Academy Publisher (ISSN: 1796-2056) Issue 4, No. 3, pp. 178-183 (May 2009).

[12] Yudhvir Singh, Yogesh Chaba, —Information Theory Tests based Performance Evaluation of Cryptographic Techniques‖ International Journal of IT & Knowledge Management (ISSN: 0973-4414) Vol. 1, No. 2 pp. 475-483 (July-Dec, 2008).

[13] Manel Guerrero Zapata, N. Asokan, —Secure Ad-ahoc on-demand distance vector‖ WiSe'02, Atlanta, Georgia, USA. Pp 35-45, (September 28, 2002).

[14] Seung Yi, Prasad Naldurg and Robin Kravets, —SAR: Security Aware Routing Protocol‖, Dept. of Computer Science, University of Illinois at UrbanaChampaign.

[15] Basagni, S. Conti, M. Giordano, S. Stojmenovi & Cacute, —Mobile Ad Hoc Networking‖, WileyIEEE Press, pp. 1-33, 275-300, 330-354, (September 2004).

[16] C. Siva Ram Murthy and B.S. Manoj, —Ad Hoc Wireless Networks, Architecture and Protocols‖, Pearson Education, pp. 321-386, 473-526, (2004).

[17] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh, —Attack Prevention Methods for DDoS Attacks in MANETs‖, Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21, (2011).

[18] Renu Dalal, Yudhvir Singh, Manju Khari, —A Review on Key Management Schemes in MANETs‖, International Journal of Distributed and Parallel Systems (IJDPS), ISSN: 0976-9757, Vol.3, No.4, July 2012, pp 165-172, (2012).