International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 2, February 2013 **ISSN 2319 - 4847**

A Study of Secure Routing protocols

Amandeep Kaur[1], Hardeep Singh[2]

[1]M-Tech(CSE), , Research Scholar, Lovely Professional University Phagwara(Pb.) India.
[2]Assistant Professor, Lovely Professional University Phagwara (Pb.) India.

ABSTRACT

Mobile Ad hoc networks have no fixed infrastructure available for routing packets in an end to end network and instead rely on intermediary peers. There are various types of attacks which an effect the MANETs. Routing Protocols, data, bandwidth and battery power are the common target of these attacks. This paper gives an overview of various secure routing protocols by presenting their characteristics and functionality along with their respective merits and drawbacks. A comparison of these protocols is also presented based upon certain security parameters.
Keywords: Routing protocols, Security, MANET, attacks.

1. INTRODUCTION

Wireless Network is growing new technology in this modern era that will allow users to access services and information electronically, irrespective of their geographic positions. Wireless Networks are basically divided into two broad categories-Infrastructure Networks and Infrastructure less (ad hoc) networks. Infrastructure network has fixed and wired gateways. Whereas in the case of wireless network, there is no need of any type of wire. In Infrastructure Networks a mobile host interacts with a bridge in the network called base station within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range in one base station, it connects with new base station and start communicating through it. This situation is called Handoff. Next recent advancement Bluetooth introduced a fresh type of wireless system which is frequently known as mobile Ad hoc networks.MANET is self configuring network of mobile routers and associated hosts connected by wireless links. Participating nodes acts as routers which are free to move randomly and manage themselves arbitrarily & thus the wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger internet. Hence the topology of the network is much more dynamic and the changes are often unpredictable oppose to the internet which is a wired network.
This paper is organized as follows: section 2 presents different types of security goals achieved in Ad hoc networks. In the section 3 we are presenting that what are the security attacks and describe the various types of security attacks. In section 4 we discuss the types of routing protocols and analyze some secure routing protocols. At last we will compare the secure routing protocols based upon some parameters and conclude our study and future work.

2. SECURITY GOALS OF AD HOC NETWORKS

Some well-known Ad Hoc network applications are:

Collaborative Work: For some business environments, the need for collaborative computing might be more important outside office environments than inside. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.
Crisis-Management Applications: By using Ad Hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.
Personal Area Networking and Bluetooth: A personal area Network (PAN) is a short-range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

There are five major security goals that are needed to maintain a reliable and secure Ad hoc network environment. There are mainly as following:
Confidentiality of Data- keeps data secret (usually accomplished by encryption).
Integrity of Data- prevents data from being altered (usually accomplished by encryption).
Availability of Data- data should be available on request.
Authenticationof Data- verification that the data or request came from a specific, valid sender.

3. SECURITY ATTACKS

Adhoc networks are more easily attacked than a wired network. The attacks prevalent on Ad hoc routing protocols can be broadly classified into passive and active attacks. There are two classifications of attacks in MANETs.

- Active attack: in order to perform some harmful operations the misbehaving node has to bear some energy costs is known as active attacks.
- Passive Attacks: Passive attack is mainly about lack of cooperation with the purpose of energy saving. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

Here we describe the different types of attacks against different layers:
Classification of different types of attacks on different layers of the protocol stack:

Table1: Different attacks against different layers.

Layers	**Attacks**
Application layer	Repudiation, Data correction
Transport layer	Session hi-jacking, SYN flooding
Network layer	Wormhole, Black hole, Byzantine, Flooding, Resource Consumption, Location disclosure Attack.
Data link layer	Traffic analysis, monitoring disruption MAC, WEP weakness.
Physical layer	Jamming, interception, eavesdropping.
Multi-layer attacks	DoS, impersonation,replay,man-in-middle attack.

- **Attacks based on the modification:**This is the more simple way to disturb the operation of the Ad hoc network. This kind of attacks is based on the modification of the metric value for a route or altering the messages passes through that route. There are three ways in which this can be achieved: Redirection by changing the route sequence number, Redirection by altering the Hop Count, Denial of service by altering routing information.
- **Impersonation attacks:** More generally this is known as spoofing. In this the malicious nodes hides its IP and MAC addresses and uses that of another node. Since current routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing.
- **Attacks by fabrication of information:** There are basically three subcategories of fabrication of information attacks- Falsification of route error messages, Corrupting routing state, and Routing table overflow attack. In any of three cases detection is very difficult.

4. ROUTING PROTOCOLS IN MANETS

Ad Hoc routing protocols can be broadly classified as being Proactive (Table-Driven), Reactive (On- Demand) and Hybrid routing protocols.

In a **Proactive routing protocol**, all the routes to each destination are kept in an up-to-date table. Changes in the network topology are continually updated as they occur.

In the **Reactive routing protocol**, a connection between two nodes is only created when it is asked for by a source. When a route is found, it is kept by a route maintenance procedure until the destination no longer exists or is indeed.

In the **Hybrid routing protocol**, combination of proactive and reactive protocol.

Here we are presenting the comparison of reactive and proactive protocols:

Table 2: Comparison between Proactive and Reactive routing protocols.

Routing Protocols	**Proactive**	**Reactive**
Advantages	A Route can be selected immediately without any delay.	Lower bandwidth is used maintaining Routing tables. More energy efficient. Effective route maintenance
Disadvantages	Produce more control traffic. Takes a lot more bandwidth. Produces network congestion.	Have higher latencies when it comes to route discovery.

4.1 SECURE ROUTING PROTOCOL:

Here we discuss some secure routing protocols based upon some parameters like:

Packet delivery fraction: the ratio of the number of data packets delivered to the destinations. It describes the loss rate that will be seen by the transport protocols, which in turn affect the maximum throughput that the network can support.it is, describe as follows:

$$\sum \text{Number of packets receive} / \sum \text{Number of packets send}$$

Average end to end delay: it is the delay experienced by the packet from the time when it was sent by a source till the time it reached to the destination. This includes all the possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times.

Number of dropped packets: it is the total number of dropped packets that have been collected during the running of the simulations. To calculate the number of dropped packet is by subtracting the number of received packets to those packets generated by the source/sender.

Routing overheads: routing overhead or routing load is used as the ratio of routing packets to the data packets. As for thecalculation, normalized routing load = routing packet sent/packet received.

Here we are giving some secure routing protocols are as:

SLSP (Secure Link State Protocol): This protocol provides secure proactive topology discovery which is beneficial for network operation. It is known as standalone and self-contained link state discovery protocol. It is responsible for securing the route discovery and distribution of link state information. This protocol is robust against Dos and Byzantine adversaries. But this protocol is still vulnerable to colluding attackers and other attackers[12].

SEAD (Secure Efficient Ado Distance Vector Routing Protocol): It is based on DSDV routing protocol. This protocol is used to guard against Denial of Service by using one way hash functions. It provides limited CPU processing capability. Long lived routing loops can be reduced by using destination sequence numbers. These destination sequence numbers provide replay protection of routing update messages in SEAD[12].

SAODV: It is an enhancement over AODV routing protocol that utilizes security feature like integrity and authentication. It uses digital signature to authenticate non mutable field of messages and hash chains to secure hop count information. IPSec provides secure network transmission in MANET for data messages. And digital signature is used when a RREQ is sent between source nodes to destination node. Primarily, sender node signs the message and intermediate node verifies the signature before generating of reverse route to the host. And destination node signs the RREP to its private key.

CONFIDANT (Cooperation of nodes fairness in dynamic adhoc network): this algorithm is enhancement of DSR routing and based on selection of selfish and unselfish nodes. Trust and routing calculation process is evaluated by experience, observation and behavior of other nodes, present in the network. It identifies routing misbehavior and maintains the provision of correct forwarding and traffic diversion.

DSDV :is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

PrAODV: It is an enhancement of an AODV routing. It uses prediction based routing to reduce route breakages which improves the performance. It maintains two additional parameter in RREP message of AODV such as velocity and

location information. These parameters help to calculate predicted link value by which source node can easily predict lifetime of a node.

CORE: Michiardi and Molvahave introduced this approach. Suggested algorithm relies on DSR routing. It follows reputation mechanism for monitoring of the cooperativeness of nodes. This mechanism uses the nodes' reputation to forward packets through reliable nodes.

SAR: It is an extension of AODV routing protocol. This protocol considers trust level mechanism to take efficient and secure routing decision. In this a node can find a path through nodes with a particular shared key. It shares symmetric encryption key concept among the nodes. SAR increase overhead due to calculation of encryption and decryption process at each node. It can be implemented using any routing protocol.

SPREAD (Security Protocol for Reliable data delivery): It provides data confidentiality security service in routing protocols. It uses secret sharing scheme between neighboring nodes to strengthen data confidentiality. It overcomes the problem of eavesdropping and colluded attacks.

AODV-SEC: It is an improved version of SAODV and extension of AODV routing protocol. It uses PKI as a trust anchor for node identification using X.509 certificates. X.509 version of AODV-SEC does not scale if the traffic load increases. It may be due to the cryptographic mechanisms.[12]

5. CONCLUSION AND FUTURE SCOPE

This paper review the different types of secure routing protocols but there are no performance analysis is presented. In the future we will compare the DSDV and SAODV protocols and by highlighting their features, differences and their characteristics. We can sum up that each protocol has definite advantages and disadvantages and can be appropriate for a particular application environment.

REFERENCES

[1] Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla, Anil Garikapati, "Security in Ad-hoc Networks",*IEEE International Conference on Computational Intelligence and Communication Systems*, 2011.

[2] Sima. "Security Issues in Ad Hoc Networks", *International Journal of Information and Communication Technology Research*, August 2011.

[3] Sonia Boora, Yogesh Kumar, Bhawna Kochar, "A Survey on Security Issues in Mobile Ad-hoc Networks", *IJCSMS International Journal of Computer Science and Management Studies*, Aug 2011.

[4] Eric Lee, "Security in Wireless Ad Hoc Networks" *Science Academy Transactions on Computer and Communication Networks*, March 2011.

[5] Nitish Pathak, Neelam Sharma, "MOBILE AD-HOC NETWORK: OPTIMIZATION OF ROUTING ALGORITHMS FOR MOBILITY MODEL",*International Journal of Reviews in Computing*, April 2012.

[6] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", *IEEE Personal Communications*, 2009.

[7] Karan Singh, R. S. Yadav, Ranvijay, "A REVIEW PAPER ON AD HOC NETWORK SECURITY", *International Journal of Computer Science and Security*,April 2010.

[8]C. Sreedhar, Dr. S. Madhusudhana Verma, Prof. N. Kasiviswanath, "A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols", *(IJCSE) International Journal on Computer Science and Engineering*, 2010.

[9] I Papaj, E. Dobos, A. Cizmár, "Performance analysis of new integration model of security and QoS as a one parameter in MANET', *journal of Electrical and Electronics Engineering*, 2011.

[10] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer", *www.elsevier.com/locate/procedia*, 2010.

[11] J. Papaj, A. Cizmár, E. Dobos, "Implementation of the new integration model of security and QoS for MANET to the OPNET', *Communications in Computer and Information Science*, 2011.

[12] UMANG SINGH, "SECURE ROUTING PROTOC OLS IN MOBILE ADHOC NETWORKS-A SURVEY AND TAXANOMY', *International Journal of Reviews in Computing*, 2011.