ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, No 5, May 2013

A Study of Secure Routing in Mobile Ad-hoc Networks

Desai Piyusha P.

***Abstract*— These days Wireless Communication is one of the popular areas of research. Mobile ad-hoc networks (MANET) operate in the absence of any supporting infrastructure. The absence of fixed infrastructure in MANET makes it difficult to utilize the existing techniques for network services, and poses number of various challenges in the area. The discovery and maintenance of secure route is the most difficult challenge. Security is one of the important issues in MANET. The assumption of a trusted environment is not one that can be realistically expected; hence, several efforts have been made toward the design of a secure and robust routing protocol for ad hoc networks. This paper includes study and overview of some existing secure routing protocols in MANET.**

***Index Terms*— AODV, DSDV, MANET, SRP,TORA.**

I. Introduction

MANET is the collection of wireless mobile nodes forming a temporary or short lived network without any base station. The term routing is very important for a network. Routing is a process of finding an efficient, reliable and secure path from a source node to a destination node via intermediate nodes in a network. Routing in MANET is a challenge due to dynamic topology in network as mobile nodes can move in any direction in the MANET. Instant network setup is the main feature of MANET. MANET is useful in places that have no communications infrastructure or when that infrastructure is severely damaged. A small network for sharing resources can be setup by mobile nodes (laptop, personal digital assistant, smart phones).

MANETs employ wireless communication, where each node participates as a source, destination, or intermediate router. Ad hoc environments are attractive for military applications and disaster response situations where fixed networking infrastructures may not be available once damaged beyond use. Protocol security is vital to proper operation. We consider a protocol secure if it is accurate and reliable, even when faced with malicious attackers.

In order for a MANET routing protocol to operate properly, we must trust intermediate nodes that make up a routing path will operate according to the protocol rules. If a malicious host can inject itself into the routing path, proper routing protocol operation is dependent on the attacker's intentions. Trusting intermediate nodes to follow protocol rules is a significant issue in MANET implementations since these networks are highly dynamic; nodes may continuously join or leave the network and network connectivity changes with mobility. Unfortunately, security is often an afterthought in MANET protocol development. Security is commonly ignored or designed in after the fact as vulnerabilities or attacks are discovered. Moreover, the protocol's upfront security goals are commonly not addressed. Undefined security goals complicate the security analysis task. It is generally considered infeasible to analyze a protocol to determine if it is vulnerable against unknown attacks.

There are several well known protocols in the literature that have been specifically developed to cape with the limitations imposed by ad hoc networking environments. Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, named the table-driven and the source-initiated on demand [5] approaches.

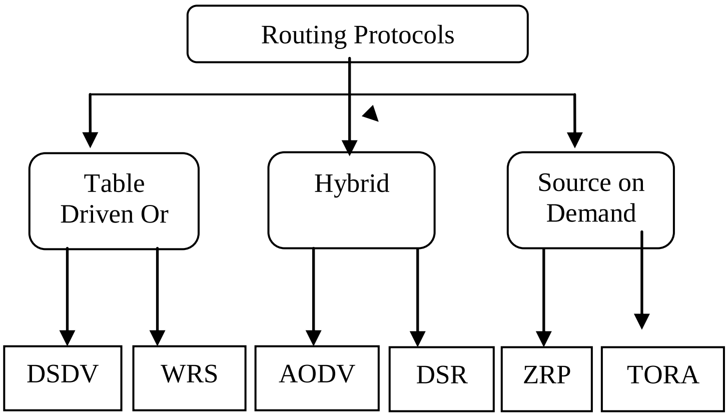

Fig. 1.1 Classification of Routing Protocals

II. SECURITY GOALS

For secure routing between two nodes, following security goals should be satisfied.

(1) Confidentiality: Data in transit to be kept secret from eavesdroppers.

.

Desai Piyusha P., M.E. Student, Computer engineering, LDRP_ITR,Gandhinagar ,Gujarat Techinical University,.Surat,,Gujarat ,India.

(2) Integrity: Data can not be modified without authorization. Wireless networks inherently unreliable, so an adversary can tamper with messages.

(3) Authentication: Communicating nodes need to verify each others' identities. When node A sends data to node B, how node B verify that data is send by mode A and not any other node in the network.

(4) Availability: The service should be available all the time.

(5) Data Freshness: It suggests that the data is recent, and it ensures that no old messages have been replayed.

(6) Non-repudiation: Sender and receiver cannot deny its role in communication.

(7) Authorization: It ensures that only authorized nodes can be accessed to network services or resources.

Instead of attempting to define common security goals based on the multiple security views, it makes more sense to view overall security in terms that determine if a protocol meets its intended goals, even when faced with malicious intruders.

In order for a routing protocol to be effective it must deliver an optimally correct route by possessing the following properties:

- Accuracy. A routing protocol is accurate if it produces routes that meet its objectives (i.e., the returned routes are valid).
- Reliability. A routing protocol is reliable if its returned routes are always accurate, even if non-malicious failures (e.g., mobility, hardware failure, etc.) occur.

Accuracy and reliability must be maintained at all times for a protocol to maintain its effectiveness.

III. ATTACKS ON MANET ROUTING PROTOCOLs

Attacks on mobile ad hoc networks can be classified into following two categories:

A. *Passive Attacks*

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it.. An attack which is specific to the passive attack is given below:

1) Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission..

B. *Active Attacks*

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

Brief descriptions of active attacks are given below.

1) Network Layer Attacks

The list of different types of attacks are given below:

i) Wormhole Attack

In wormhole attack[1], a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

ii) Black hole Attack

In Black hole attack[1], an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

iii) Resource Consumption Attack

In this attack, an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks.

iv) Routing Attacks

There are several attacks which can be mounted on the routing protocols and may disrupt the proper operation of the network. Such attacks are :

- Routing Table Overflow: In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.
- Packet Replication: In the case of packet replication, an attacker replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

2) Transport Layer Attacks

i) Session Hijacking

Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. All the communications are authenticated only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack.

3) Application Layer Attacks

i) Repudiation: In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

4) Multi-layer Attacks

Here we will discuss security attacks that cannot strictly be associated with any specific layer in the network protocol stack.

i) Denial of Service

In this, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. One way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate.

ii) Impersonation

In this attack, a compromised node may get access to the network management system of the network and may start changing the configuration of the system . A man-in-the-middle attack is an example of impersonation attack. The attacker reads and possibly modifies messages between two end nodes without letting either of them know that they have been attacked.

IV. RELATED WORK

Some of the secure routing protocols are discussed as follow:

A. Destination Sequence Distance Vector[7]

The Destination Sequence Distance Vector (DSDV) comes under proactive or table driven routing protocol and is a well known MANET routing protocol. Here each table must contain the destination node address, the minimum number of hops to that destination, the next hop in the direction of that destination and an entry for sequence numbers for every destination. A higher sequence number denotes a more recent update sent out by the source node.

When a node receives any update information, it checks the sequence number in the packet and if the information in the packet is older than the receiving node has in its routing tables, then the packet is rejected otherwise the information is updated . After this the update packet is forwarded to all other neighboring nodes except the one from which the packet came.

B. Security Aware Ad-hoc Routing [5]

Security-Aware ad hoc Routing (SAR) makes use of security attributes to take the routing decision. In SAR, security metric is embedded into the RREQ packet. Nodes are required to have keys for decryption of data while forwarding or receiving the data. If a path with the required security attributes is found a RREP is sent from an intermediate node or the destination node to the source node. In case of more than one route the shortest route is selected for data forwarding.

C. Secure Ad hoc On-demand Distance Vector Routing [2]

The SAODV (Secure Ad hoc On-demand Distance Vector Routing) protocol [2] is an extension of AODV. Adversary nodes may forge AODV packets, listen to others, reply packets in their own interests, and report errors where there are none. To defend these attacks, it is assumed that each node has a certified public key. Hop-by-hop authentication is used to protect routing messages, and all intermediate nodes need to cryptographically validate the digital signatures appended with a routing message.

D. Secure Routing Protocol (SRP) [3]

Secure Routing Protocol (SRP) is another routing protocol which uses symmetric cryptography. The protocol is based on route querying method. SRP Requires a Security Association (SA) between source and destination node. Key generated by the SA is used to encrypt and decrypt the data by the two nodes.

A SRP Header (Figure 1) is added to the base header. The RREQ packet consists of a *query sequence number (QSEQ)*, *query identifier (QID)*, and the out put of a key hashed function. The key hash function takes IP header, header of the basic routing protocol, and the shared key.

The intermediate nodes broadcast the query to the neighboring nodes and update their routing table. If receiving node has the same QID in their routing table, query is dropped. When the destination is reached, destination node checks for the security metrics by calculating the key hash function ―*message authentication code (MAC)".* After verifying the secret key it generates reply packet for source node consisting of path from source to destination, QID, QSEQ. After receiving the reply packet source node again calculates its MAC. There can be multiple routes from source to destination. Route maintenance in this protocol is also done through route error message.

E. Secure AODV using RSA Signature[6]

An extension of the *Ad Hoc On-demand Distance Vector* (*AODV*) [6] routing protocol has been proposed [7] to protect the routing protocol messages. The *Secure-AODV* scheme assumes that each node has certified public keys of all network nodes, so that intermediate nodes can validate all in-transit routing packets. The basic idea is that the originator of a control message appends an *RSA signature* and the last element of a *hash chain* (i.e., the result of *n* consecutive hash calculations on a random number). As the message traverses the network, intermediate nodes cryptographically validate the signature and the hash value, generate the *k-th* element of the hash chain, with *k* being the number of traversed hops, and place it in the packet. The route replies are provided either by the destination or intermediate nodes having an active route to the sought destination, with the latter mode of operation enabled by a different type of control packets.

The use of public-key cryptography imposes a high processing overhead on the intermediate nodes and can be considered unrealistic for a wide range of network instances.

F. Temporary Ordered Routing Protocol [5]

The Temporally-Ordered Routing Algorithm (TORA) is for routing data Mobile ad-hoc networks. The TORA attempts to achieve a high degree of scalability . In its operation the algorithm attempts to suppress, to the greatest extent possible, the generation of far-reaching control message propagation. The TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type. TORA builds and maintains a Directed Acyclic Graph rooted at a destination. No two nodes may have the same height. Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally-ordered heights at all times, TORA achieves loop-free multipath routing, as information cannot 'flow uphill' and so cross back on itself.

The key design concept of TORA is localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain the routing information about adjacent (one hop) nodes. The protocol performs three basic functions:

□ Route creation

□ Route maintenance

□ Route erasure

V. CONCLUSION

This paper is an effort to concentrate on the overview study of all routing protocols supporting security requirements along with an overview of the various security goals and major possible security attacks on routing process in mobile ad hoc network. It has been further concluded that due to the dynamically Changing topology and infrastructure less, decentralized Characteristics, security and power awareness is hard to achieve in mobile ad hoc networks.

REFERENCES

[1] Raj Tirthraj,Verma A K, " Survey and Analysis of secure routing protocols for MANETs," in the proceeding of National Conference on cutting Edge Computer and Electronics Technology (CECT 2009), Pantnager, February14-16,pages501-06.

[2] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, Internet Draft: draft-guerrero-manetsaodv-00.txt, 2002.

[3] P. Papadimitratos, Z.J. Haas, P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratossecure-routing-protocol-00.txt 2008-12-11.

[4] A K Verma, mayank Dave and R C Joshi, "Classification of Routing Protocols in MANET", at National Symposium on Emerging Trends in Networking & Mobile Communication (NSNM-2003),pp. 132-139, Sept 5-6, 2003. (dsdv aodv).

[5] Yu-Chee Tseng, Wen-Hua Liao, Shih-Lin Wu, "Mobile Ad Hoc Networks and Routing Protocols", Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic´ Copyright ©2002 John Wiley & Sons, Inc. ISBNs: 0-471- 41902-8 (Paper); 0-471- 22456-1 (Electronic).

[6] Manel Guerrero Zapata , and N. Asokan. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, vol. 3, no. 6, July 2002, pp. 106-107.

[7] Perkins Charles E., Bhagwat Pravin: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, London England UK, SIGCOMM 94-8/94.

Piyusha Desai is a M.E. student in the Dept. of Computer Engineering, LDRP_ITR, Gujarat Techinical University, Gujarat,India. She received his B.E. degree in Computer Engineering from Veer Narmad South Gujarat University, India in 2010. Her research interests include Mobile Ad-Hoc Networks,Routing protocols in Manet.