Review paper: Existing Security Mechanisms in MANET

Mahendra Pratap Singh
School of ICT
Gautam Buddha University
Greater Noida, India
mpsgbu@gmail.com

Manisha Manjul
School of ICT
Gautam Buddha University
Greater Noida, India
manisham@gbu.ac.in

Abstract: **Wireless mobile ad-hoc network is a group of mobile nodes connected with each other in a scattered manner. There is no fixed topology used to connect mobile nodes. In mobile ad-hoc networks the topology changes rapidly, due to movement of mobile nodes. Some protocols are invented for routing in mobile ad-hoc network e.g. AODV, DSDV, SAODV, DSR, ARAN etc. Mobile ad-hoc networks challenges various kinds of security problems, caused by their nature of cooperative and open systems and by limited availability of resources, due to its dynamic topology fundamental cooperation, lack of association, resource constrained and physical vulnerability of node, in mobile ad-hoc networks two types of attacks can be possible, routing attacks and data forwarding attack. In mobile ad-hoc network secure communication is more challenging task. In this paper we describe existing security mechanisms in MANET and discuss how they fulfill the security goals of authentication, availability, confidentiality, integrity and non-repudiation.**

***Index terms*- Routing protocols, Ad-hoc, MANET, Security**

I. INTRODUCTION

A mobile ad-hoc network is infrastructure less or autonomous system of wireless mobile nodes that can be dynamically change the topology of their connection, means that a network without the fixed routing infrastructure like fixed routers and routing backbones. Unlike traditional wireless networks, they don't have base stations to maintain the activity of mobile hosts. In MANET each node works as a router when transmitting packets from one node to another node. Because of the movement of nodes several routing protocols for mobile ad-hoc networks have been developed. Several of them are Ad-hoc On Demand Vector (AODV) Routing protocol, Dynamic Source Routing (DSR) protocol, Distance sequenced distance vector (DSDV) routing protocol Cluster Based Routing Protocol, Global State Routing Protocol, etc. The applications of an ad-hoc networks comes in personal area networking, meeting rooms and conferences, battlefield operations, disaster relief and rescue operations etc. Several aspects of ad-hoc networks have remarkable security problems. Routing is one such aspect.

A mobile ad-hoc network uses multi-hop communication, it means when two nodes which are not in the communication range of each other, but still can send and receive data between each other with the help of intermediate nodes which should act as routers. This meaning gives another name to mobile ad-hoc network as "multi-hop wireless network".

A mobile Ad-hoc network, what should be covered in the security criteria when we want to inspect the security state of the mobile Ad-hoc network. In the following, briefly introduce the widely-used criteria to evaluate if the mobile Ad-hoc network is secure.

II. SECURITY ISSUES OF EXISTING ROUTING PROTOCOLS

In mobile ad-hoc network apply many types of routing protocol like AODV, DSDV, DSR, OLSR etc., and these are required different types of Security. Security issues are associated with the existing routing protocols. In MANET there is no clear secure boundary, because of the nature of MANET freedom to join, leave and move inside the network which can be compared with the clear line of defense in the traditional wired network. . In this review paper we are discuss some security issues in MANET which is given below.

a) Availability: It is maintain the ability of the node and provide all the design services regardless of the security state of it. In MANET few nodes are selfish and make some of the network services unavailable so that authorized person has not obtain the services from the network such type attack are known as denial of service. Denial of service attack mainly happens in the routing protocol and key management service.

b) Integrity: It is guarantees the identity of the messages when the messages are transmitted from source to destination. Integrity can be categorized mainly in two ways:

- Malicious altering

ISBN: 9788175157538

- Accidental altering

In malicious altering a message can be removed, replayed or revised by an adversary with malicious goal. In the accidental altering the message content is changed or lost due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure.

c) Confidentiality: It is define that certain information is only accessible to those who have been authorized to access. In another words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

d) Authentication: It is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If authentication mechanism is not applied between the source and destination then adversary could impersonate a benign node and access the confidential resources or generated some fake messages so that network operation is disturb.

a) Non-repudiation: It is confirms that the sender and the receiver of a message cannot disagree that they have ever sent or received such a message. At that moment if a node sends a message to the destination and destination node disagree to receive the message or vice versa.

III. ROUTING PROTOCOLS IN MANET

In mobile ad-hoc networks have different type of routing protocols according to the user services and it is provide a secure routing path between source to destination such type of routing protocol discussed below.

A. AODV

The Ad Hoc on Demand Distance Vector Routing Protocol (AODV) is a source initiated, on demand driven, routing protocol [1]. AODV is a demand based routing protocol, when a source node wants to communicate with a specific destination node then route is only traced between them. The route remains established as long as it is needed for further communication. AODV have also another feature to describe the sequence number of a destination for every route entry. This number is included in the RREQ (Route Request) of any node that desires to send data. These numbers are used to ensure the freshness of routing information. For instance, a requesting node always chooses the route with the greatest sequence number to communicate with its destination node. Once a fresh path is found, a RREP (Route Reply) is sent back to the requesting node. AODV also has the necessary mechanism to inform network nodes of any possible link break that might have occurred in the network [2].

B. DSDV PROTOCOL

The DSDV (destination-sequenced distance vector) protocol [3] uses the Bellman-Ford algorithm to calculate paths. Using the cost metric to calculate the hop count, this is the number of intermediate nodes which takes for the packet to reach its destination. DSDV is table-driven proactive protocol, thus all the nodes in the existing network maintain routing table entries by it and not just the neighbors of a node. DSDV use periodic and trigger update mechanism to change propagation. Result of this updates, there is a chance of having routing loops within the network. To remove routing loops from the networks, each update from the node is tagged with a sequence number. Selection of each sequence number is independently chosen by the every node, each node chosen sequence number independently and a periodic update each time. When node update normal sequence number then it is an even number, since each time a periodic update is made the node increments its sequence number by 2 and adds its update to the routing message it transmits. Any node cannot change the sequence number of another node. If node update expired route to its neighbor then it increments the sequence number of the disconnected node by 1. The nodes receiving this update will then look at the sequence number and if it is odd and remove the old entry from the routing table. DSDV uses setting time to get wet due to the route fluctuations in the mobility of the nodes in MANETs.

C. DSR

The DSR protocol is a reactive protocol which requires each packet to carry the full address of every hop in the route, from source to the destination. it means in a large network the protocol will not effectual, in large network due to the increases diameter of network the packet overhead is also increases according to the size of network. Therefore packet overhead may consume more band width of the network, if network is highly dynamic and large it causes that the routing information of every node carried in the packet it create overhead in the packet, so the bandwidth consumed in large network more than the bandwidth consumed in small network. However, this protocol has more advantages over AODV routing protocol, in a small to moderately size networks (Approx. few hundred nodes), DSR performs better than AODV. The advantage of DSR

ISBN: 9788175157538

over AODV is that nodes can store multiple routes in their route cache, which means that the source node can check its route cache for a valid route before initiating route discovery packet, and if a route found valid then there is no need for route discovery. It is very beneficial in network with low mobility. Because of the low mobility of the nodes the routes stored in the route cache will be valid longer. Another advantage of DSR is that it does not require any hello message exchanges or periodic beaconing, therefore nodes can go into sleep mode to conserve their power. This also saves a considerable amount of bandwidth in the network.

D. OLSR

OLSR [4] is a object link state routing protocol, and it is a traditional link state algorithm which create point-to-point routing protocol between two neighbors node. It is minimize each control message and number of broadcasting nodes during the update of routing table when employing multipoint replaying (MPR) strategy. When the topology update it selected every neighbor node to retransmit the packets. This set of nodes is called the multipoint relays of that node. Any node which is not in the set can read and process each packet but do not retransmit. In this routing protocol each node periodically broadcast a list of its one hop neighbors using a hello message. In that case each node selects a subset of one hop neighbors, which covers all of its two hop neighbors. For example, in Fig. 1, node A can select nodes B, C, K and N to be the MPR node s. Since these nodes cover all the nodes, which are two hops away. Each node determines an optimal route (in terms of hops) to every known destination using its topology information (from the topology table and neighboring table), and stores this information in a routing table.

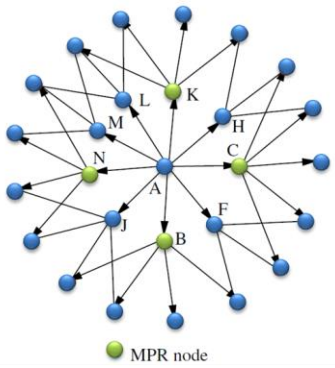

Fig.1 Multipoint relays

Therefore, routes to every destination are immediately available when data transmission begins.

IV. SECURE ROUTING PROTOCOLS IN MANET

In mobile ad-hoc networks feasible for many secure routing protocols which are provide security between source and destination. Few secure routing protocols given below:

A. SAODV

SAODV is a secure version of AODV. It uses hash chains for protect the non-mutable fields and digital signature to secure hop count field in both RREQ and RREP messages. Working of a SAODV explains in detail that is when the route discovery process starts from a source node to generate a random seed number and maximum hop count (MHC) and set the value Time To Live (TTL) from the IP header. Source node generate the HMAC and also generate a RREQ packet and broadcast to discover the secure path between source to destination when the destination receives the RREQ packet and the destination node generate RREP packet and send to the source through unicast reply.

B. ARAN

ARAN is an Authenticated Routing protocol for Ad hoc Networks [20] and it is a signature based extension to the AODV routing protocol, to provide secure route discovery. Source node and the intermediate node is sign a entire routing message in ARAN after than receiving a sequence number and signature before appending their signature and forward it to their neighbors. When a source node A needs to seek a route, it generates a RREQ and signs it. An example shows in Fig. 2, When node B (one hope neighbor of node A) receive the message, it uses the pubic key of the certificate server to extract A's public key and verify it with the received signed message. If signature is successfully verified, then the received message is supposed to be authentic and unaltered. Then node B updates the routing table according to the RREQ, and node B signs it and appends its own certificate to the message before rebroadcasting it to its one-hop neighbors. Otherwise, the RREQ is supposed to be unauthentic and will be discarded. Assuming node C is one of B's one-hop neighbors and C receives the RREQ message from B. Similarly, C validates the corresponding signature

ISBN: 9788175157538

with the given certificate. Upon successfully verifying the signature, C then removes B's certificate and signature, updates routing table, signs the entire message originally broadcast by node A, appends its own certificate and rebroadcast it. During the route discovery, each intermediate node repeats these steps. When the destination node receives the RREQ, it creates an RREP and unicasts it back along the reverse path to the source in the same way.

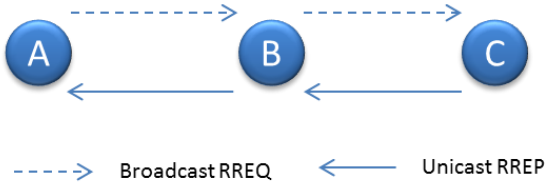

Fig. 2 RREQ & RREP in ARAN

C. ARIADNE

The Ariadne [5] is a secure on-demand routing protocol based on DSR. It provides three ways of authenticating routing messages; using pairwise shared secret keys, using pairwise shared secret keys combined with broadcast authentication or digital signatures. If shared keys or digital signatures are used then the routing message is authenticated by appending a Message Authentication Code (MAC) or digital signature for each intermediate node. The protocol also proposes the use of TESLA broadcast authentication mechanism [10] for intermediate hop authentication and shared secret for endpoint authentication. Reverse hash chains and delay key disclosure generated by TESLA mechanism and provide authentication of routing message. Before the key is disclosed all the neighbors receive the authentication message through loosely synchronize clocks and a delay at least the network round-trip time which provide the guarantee its neighbor. Ariadne provides both integrity and authentication of routing information, however non-repudiation can only be guaranteed when using digital signatures, since MACs are impossible for others to verify.

D. SRP

The Secure Routing Protocol (SRP) [6] is designed as an extension to DSR or the inter zone part of the Zone Routing Protocol (ZRP) [7]. The protocol relies solely on symmetric key cryptography for authenticated route discovery, assuming that shared secret keys have already been established between the source and destination nodes. A Message Authentication Code (MAC) based on the shared key is appended to route requests in order to allow the destination to authenticate the originator. However, intermediate nodes and the recorded route are not authenticated. Additionally, route error messages do not contain any verification and hence can be forged by adversaries. The protocol provides authentication and integrity, but introduces some serious issues for the availability.

E. SLSP

The Secure Link State Protocol [8] is a secure proactive routing protocol employing a similar strategy as SAODV for message authentication. Link State Updates (LSUs) are digitally signed by the originating node, with all mutable fields excluded. The mutable fields are instead governed by a hash chain, which do not allow reduction in the hop count. By specifying a maximum hop count, the protocol can be used as the intra zone part of ZRP [9] only end-nodes are authenticated, such that intermediate nodes may spoof their identity without being revealed.

Protocol	Authentication	Integrity	Confidentiality	Availability	Non-repudiation	Assumptions
SAODV	Yes[1]	Yes	No	Yes	Yes	Established PKI
SRP	Yes[1]	Yes	No	Yes	No	Established PKI
Ariadne	Yes[1]	Yes	No	Yes	No	Established PKI or shared secret keys
SLSP	Yes[1]	Yes	No	Yes	Yes	Established shared secret key
ARAN	Yes	Yes	No	Yes	Yes	Established PKI

1=Not intermediate nodes

Table1. Comparison of Existing secure MANET protocols

ISBN: 9788175157538

Table1 shows how the different protocols meet the security goals. It is to be notice that if the protocol improves denial of service resistance than the availability property is considered to be satisfied and also it does not imply that will resist all attacks.

V. CONCLUSION

In this review paper we are discussed some types of secure routing protocol which provides security in mobile ad-hoc network by different types of mechanism. Some routing protocols provide better security compare then other routing protocol to discover the neighbor's node and destination without any type of disturbance but our conclusion prefer the few routing protocol like SAODV SLSP and ARAN. Some of these routing protocols provide better security in small network with low mobility. When we compare the different secure routing protocol in mobile ad-hoc network find some work better in low mobility which is less dynamic and few provide the high performance in high mobility with high dynamic condition. But our point of view some researches ongoing to provide secure routing protocol to both high and low mobility with better performance.

REFERENCES

[1] E.M.Royer, C.K.Toh."Ad-hoc On-Demand Distance Vector Routing". University of California, Georgia Institute of Technology Internet Draft: draft-ietf-manetaodv-13.txt 2003.

[2] C.E.Perkins, E.M.Royer. "Ad-hoc On-Demand Distance *Vector Routing"*. Sun Microsystems Labratories, University of California, Internet Draft: draft-ietfmanet-aodv-13.txt 2003.

[3] C.E. Perkins, T.J. Watson, Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers, in: ACM SIGCOMM_94 Conference on Communications Architectures, London, UK, 1994.

[4] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, Optimized link state routing protocol for ad hoc networks, IEEE INMIC, Pakistan, 2001.

[5] D. Johnson, D. Maltz, J. Jetcheva, The dynamic source routing protocol for mobile ad hoc networks, Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, 2002.

[6] A. Iwata, C. Chiang, G. Pei, M. Gerla, T. Chen, Scalable routing strategies for multi-hop ad hoc wireless networks, IEEE Journal on Selected Areas in Communcations 17 (8) (1999) 1369–1379.

[7] B. Bellur, R.G. Ogier, F.L Templin, Topology broadcast based on reverse-path forwarding routing protocol (tbrpf), in: Internet Draft, draft-ietf-manet-tbrpf-06.txt, work in progress, 2003.

[8] P. Papadimitratos and Z. J. Haas. Secure link state routingfor mobile ad hoc networks. In *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, page 379. IEEE Computer Society, 2003.

[9] Z. Haas. A new routing protocol for the reconfigurable wireless networks. In Proceedings of 6th IEEE International Conference on Universal Personal Communications, IEEE ICUPC'97, volume 2, pages 562–566. IEEE, New York, USA, Oct. 1997.

[10] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA broadcast authentication protocol. RSA CryptoBytes, 5:2–13, 2002.

[11] K.K. Kasera, R. Ramanathan, A location management protocol for hierarchically organised multihop mobile wireless networks, in: Proceedings of the IEEE ICUPC_97, San Diego, CA, October 1997, pp. 158–162.

[12] T.-W. Chen, M. Gerla, Global state routing: a new routing scheme for ad-hoc wireless networks, in: Proceedings of the IEEE ICC, 1998.

[13] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, A review of routing protocols for mobile ad-hoc networks, Elsevier ECS, 2004.

[15] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields,and E. Belding-Royer. Authenticated routing for ad-hoc networks. *Selected Areas in Communications, IEEE Journalon*, 23:598–610, 2005.

[16] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *RSA CryptoBytes*, 5:2–13, 2002.

ISBN: 9788175157538