An Analysis of Issues in Security and Routing Protocol in MANET

K. Vanitha
Research Scholar,AP/CSE,Al-Ameen Engineering College,Erode,India

Dr. A. M. J. Md. Zubair Rahman
Professor/CSE,Al-Ameen Engineering College,Erode,India

K. Anitha
Lecturer/CSE,CSI College of Engineering,Ooty,The Nilgiris,India

Abstract

The Mobile Adhoc Network (MANET) consists of several wireless mobile nodes and due to its mobility their network topology changed dynamically. So the network does not have any fixed infrastructure. In this paper discussed about the various problem and security attacks in each layer in the MANET and also about what are the security services in mobile adhoc network. Routing in adhoc network is main issues because of node mobility and limited resource. Here we discussed two types of routing protocol In this paper also reviewed about the working principles of on demand routing protocol AODV and DSR.Finally compare both the protocol. This will provide guidance for the security related research works in this area.

KEYWORD

MANET, Security Services, Security Attacks, Secure Routing protocol, AODV, DSR

1. Introduction

Nowadays, Wireless communication is implemented by independent mobile users. The mobile nodes can directly communicate with other nodes when they are within the same radio range otherwise it must communicate through the intermediate nodes. The Mobile adhoc network (MANET) consists of several wireless mobile nodes and due to its mobility their network topology is changing dynamically. So the network does not have any fixed infrastructure. A MANET is also called as an autonomous system of mobile nodes.

The Mobile Adhoc Network has the following features:

- Wireless links between nodes are unreliable due to limited energy.
- Constant changing topology due to its mobility.
- Lack of security due to its dynamic change topology.

Because of these features the Mobile adhoc networks not secure. Nodes have changed their position rapidly the wireless link will break. In MANET each node will act as a host as well as a router. All the nodes should be cooperative in order to exchange of information would be successful. This process is called as routing. It has several applications in the commercial sector for rescue operations and disaster relief efforts. MANETs also yields a solution to the military battlefield field in order to detect enemies' movement as well as for exchanging information among military headquarters and so on. Routing in adhoc network is main issues because of node mobility and limited resource. There are several routing protocols are designed for security and energy management such as AODV, DSR, OLSR,TORA, ZRP .In MANET the absence of central infrastructure and shared medium access several security attacks are possible in MANET.

The adhoc network should meet the following security requirements for data transmission.

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-Repudiation

Confidentiality, the transmitted data should known only by intended receiver; *Integrity*, the received data should be an original data (i.e.) No modification of the data during transmission process; *Availability*, the resources and network service must be available at any time and the connection must be stable to correct failures; *Authentication*, The data must be sent and received by the legitimate node for that all nodes must have its own signature; *Non Repudiation*, there should not deny in the sender of the message after sending and the receiver of the message after receiving.

Figure 1:.Mobile Adhoc Network

The MANET faces several problems in each layer as shown in the Table 1.

Table 1. Problem in Each layer in MANET

LAYERS	PROBLEM
Physical layer	Channel Access, power control, Multiuser detection
Network Layer	Routing Addressing Location Management
Transport Layer	TCP Quality of service
Application Layer	Location dependent application Service Discovery Security

2. Attacks in Mobile Ad Hoc-Network

2.1Attack Types

There are two types of attacks 1. Passive attack 2. Active attack.

Passive Attack is not modifying the original data; it is difficult to identify such an attack on the network.

Active Attack is changed or destroys the data while transmitting.

The node which performs an attack on the foreign network called *external* attack. The node which performs an attack within the adhoc network called *internal* attack.

2.2 Attacks in Each Layer on protocol Stack

The table shows the possible attacks in each layer in the adhoc network.

Table 2.Security Attacks in Each Layer in MANET

LAYERS	ATTACKS
Application Layer	Repudiation, Data corruption
Transport Layer	SYN jamming, Session hijacking
Network Layer	Black Hole , Worm hole, Jamming
Data Link Layer	Traffic Analysis, Monitoring
Physical Layer	Jamming, Interception, Eavesdropping
Multilayer attacks	Denial of Service, Impersonation, Replay, Man-in-the-Middle attack

2.3 Routing Attack

There are several attacks which disturb the operation of network in the routing protocol.

Denial of Service Attack: The attackers try to exhaust the resource in the Mobile adhoc network as radio jamming and battery exhaustion methods to involve DoS Attack.For example In AODV large number of RREQs i.e message request is sent to the nonexistent destination node which make battery consumption of all the nodes in an entire network.

Black hole attack: In a black hole attack the malicious node makes an advertise itself is that as have the shortest path to the target node by using a routing protocol which causes the malicious node simply drops the packets rather than sending it into the intended receiver.

Wormhole attack: In this attack an attacker records packets in one location in the network and tunnels them to a different location. When routing control messages are tunneled routing can be disrupted. This tunnel between two colluding attackers is referred as a wormhole. This attack is main threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

3. Routing Protocol in MANET

There are two main categories of Routing Protocol in MANET as proactive type and reactive type. Other Category called Hybrid, Which combines both the type.

Proactive (or) Table-Driven protocols: This type of protocol keeps up to date information between every pair of nodes in order to maintain consistency by propagating and route updates at fixed intervals. Such as OLSR, DSDV

Reactive (or) On-Demand Protocols: Based on the demand these protocols establish routes to the destination. Such as AODV, DSR, TORA

Hybrid Protocols: This protocol combines both proactive and reactive protocol features such as ZRP

In this paper we briefly explain on demand routing protocol AODV and DSR.

4. Adhoc On-Demand Distance Vector (AODV) [3], [4]

The variation in Distance-Vector (DSDV) routing protocol is AODV protocol and it is jointly based on both DSDV and DSR. AODV main objective is to minimize the requirement of system-wide broadcasts to its extreme and not maintain routes from every node to every other node in the network instead they are discovered as when needed and that are maintained only as long as they are required. (I.e.) establishes a route to a destination only on demand. AODV is capable for both unicast and multicast routing. The following steps are used by AODV for route establishment

- Discover the path
- Acknowledge the source
- Generate the error when there is no path or any link breakage

A. Discover the path:

AODV initiates a route discovery process using the Route Request (RREQ) and Route Reply (RREP) packets. The RREQ packet is created by source nodes containing its IP address, its current sequence number, the destination IP address, the destination’s last sequence number and broadcast ID.

Each time the broadcast ID is incremented when the source node initiates RREQ. The sequence numbers are used to determine the timeliness of each data packet. The unique identifier is generated for each request by combining both broadcast ID & the IP address. So RREQ can uniquely identify each request.

The requests are sent using the RREQ message and the creation of a route is sent back using RREP message. The source node broadcasts the RREQ packet to its neighbors and then sets a timer to wait for a reply. The node sets up the reverse route entry for the source node in its route table while processing RREQ. These entries will to know how to forward a RREP to the source. The objective of using a lifetime is associated with the reverse route entry is in order to delete the route information if this entry is not used within this lifetime. During the transmission the RREQ is lost means the source node is allowed to broadcast again using route discovery mechanism. The entries in the route table are checked to ensure whether there is a current route to that destination node or not before sending the data packet from source to a destination node. If it is there, the data packet is forwarded to the appropriate next hop toward the destination. If it is not there, the route discovery process is again initiated.

In this method, The Time to Live (TTL) values sets by the source node (TTL) for RREQ to an initial start value. The next RREQ is broadcasted with a TTL value increased by an increment value. If there is no reply within the discovery period, the process of incrementing the TTL value continues till a threshold value is reached, after which the RREQ is broadcasted across the entire network.

B. *Acknowledge the source:*

It creates the RREP when the destination node with a route to the destination receives the RREQ and unicast the same towards the source node using the node from which it received the RREQ as the next hop.

When RREP is routed back along the reverse path and received by an intermediate node, it sets up a forward path entry to the destination based on its routing table. When the RREP reaches the source node, it means that a route from source to the destination has been established and the source node can begin the data transmission.

C. *Generate the error message for route maintenance:*

Once the route discovered between a source node and destination node it is maintained as long as needed by the source node, because there is movement of nodes in a mobile ad hoc network.

If the source node moves during an active session, it again reinitiates route discovery mechanism to establish a new route to destination.

If the destination node or some intermediate node moves, then node generates Route Error (RERR) message to the affected active upstream neighbor nodes. Subsequently, these nodes propagate the RERR their ancestor nodes. This process continues until the source node is reached. When RERR is received by the source node, it can either stop sending the data or re initiate the route discovery mechanism by sending a new RREQ message if the route is still required. The figure 2 shows an example of AODV protocol.

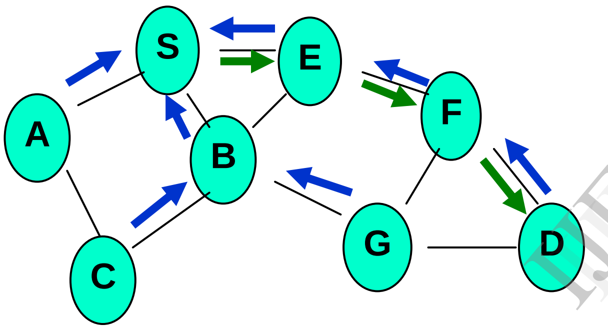

Figure 2.Example of AODV

4.1 Benefits of AODV

- AODV does not put any additional overheads on data packets as it does not make use of source routing.
- It supports both unicast and multicast packet transmissions even for nodes in constant movement.
- It only favors the least congested route not the shortest route.
- It responds very quickly to the topological changes that affects the active routes.

4.2 Limitations of AODV

- The valid route is expired and the determination of a reasonable expiry time is difficult. Since the nodes are mobile and their sending rates may differ widely and can change dynamically from node to node.
- As the size of the network grows, various performance metrics begin decreasing.
- It requires that the nodes in the broadcast medium can detect each others' broadcasts.
- Based on the assumption that all nodes must cooperate and without their cooperation no route can be established, the AODV is vulnerable to various kinds of attacks as it.

5. Dynamic Source Routing (DSR) [6, 7]

Dynamic Source Routing (DSR) is based on the source-based routing in the Adhoc routing protocol. This protocol is source-initiated instead of hop-by-hop. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes.DSR protocol is self organizing and configuring protocol so does not need any existing network infrastructure. It is composed of two essential parts: 1. Route discovery 2. Route Maintenance. To store recent discovered paths, every node maintains a cache in this protocol.

A. Route Discovery:

In DSR before a node needs to send a packet to any node, it first checks its entry in the cache. If it is there in that, then it uses that path to transmit the packet and also attach its source address on the packet. If it is not there in the cache or the entry in the cache is expired because of long time idle, the sender broadcasts a route request packet to all of its neighbors asking for a path to the destination. The sender will be waiting till the route is discovered. The sender can perform other tasks such as forwarding other packets during waiting time. As the route request packet arrives to any of the nodes, they check from their neighbor or from their caches whether the destination asked is known or unknown. If route information is known, they send back a route reply packet to the destination otherwise they broadcast the same route request packet. When the route is discovered, the required packets will be transmitted by the sender on the discovered route. Also an entry in the cache will be inserted for the future use.

B. Route Maintenance:

The node will maintain the age information of the entry so as to know whether the cache is fresh or not. When a data packet is received by any intermediate node, it first checks whether that intermediate node is mentioned destination node. If the intermediate node is the destination node, then the packet is received otherwise that node will be forwarded using the path attached to the data packet. Any link might fail anytime on Adhoc network. Therefore, route maintenance process will regularly monitor and will also notify the nodes if there is any failure in the path. Subsequently, the nodes will change the entries of their route cache. The Figure 3 shows an example of DSR protocol.

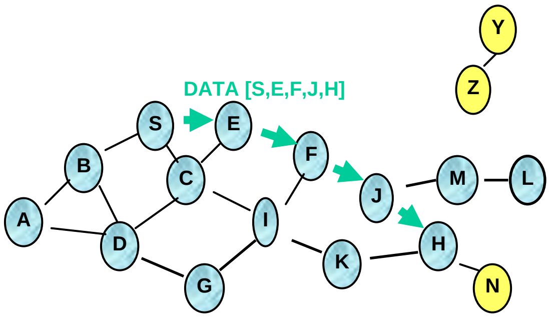

Figure 3: Example of DSR

5.1 Benefits of DSR

- Create routes only when they are needed.
- DSR protocol is that there is no need to maintain a routing table so as to route a given data packet as the entire route is contained in the packet header.

5.2 Limitations of DSR

- The limitations of DSR protocol is that this is not scalable to large networks and even requires significantly more processing resources than most other protocols.
- In order to obtain the routing information, each node must spend a lot of time to process any control data it receives, even if it is not the intended recipient.

6. Comparisons of DSR and AODV Protocol

Dynamic source routing (DSR)

- Source broadcasts RREQ through the network.
- Intermediate nodes add its address to RREQ and continue broadcasting until RREP received.
- Full path selected by source and place into each packet sent.

Ad hoc on-demand distance vector (AODV)

- Hop-by-hop routing.
- Source sends RREQ to neighbors.
- Each neighbor does so until reach the .destination.
- The reverse path is used to send RREP by the destination node.
- Source doesn't put whole path but only next hop address in outgoing packets

7. Conclusion

In this survey paper, we try to look over the security issues in the mobile ad hoc networks, which may be a main trouble in the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kinds of security risks. Then we talk about the main attack types that threaten the current mobile ad hoc networks. First we briefly introduce the essential characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connected with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. There are also increasing security threats to the mobile adhoc network, which need to gain enough attention. Finally we describe adhoc on-demand routing protocol AODV and DSR and their comparison. This gives guidance to the security related research works in this area.

8. References

[1] S. Murthy and J. J. Gracia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and ApplicationsJournal, Special Issue on Routing in Mobile Communication Networks, vol. 1, no. 2, Oct. 1996, pp. 183–97.

[2] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,”Proc. IEEE Network Protocols, 2002, Nov. 12–515, 2002, pp. 78–87.

[3] C. Perkins, E. B. Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft”, RFC 3561, IETF Network WorkingGroup, July 2003.

[4] C. E. Perkins and E. M. Royer, “Ad-Hoc On Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA,1999, pp. 90-100.

[5] P. Papadimitratos and Z. J. Haas, “Secure Routing: Secure Data Transmission in Mobile Ad Hoc Networks,” Proc. ACM Wksp. Wireless Security 2003, Sept. 2003, pp. 41–50.

[6] D. B. Johnson, D. A. Maltz, Y.C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[7] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer Publ., 1996, pp. 152-81.

[8] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,”

[9] Y. Xiao, X. Shen, and D.-Z. Du (Eds.)”Wireless/Mobile Network Security” pp, @ 2006 Springer.

[10] Nishu Garg and R.P.Mahapatra, “MANET Security Issues,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[11] H. Deng, W. Li, and D. Agrawal, Routing Security in Wireless Ad Hoc Networks.*IEEE Communications Magazine*, vol. 40, no. 10, 2002.

[12] I. Aad, J. Hubaux, and E. W. Knightly, Denial of Service Resilience in Ad Hoc Networks, *In Proc. of 10th Ann. Int’l Conf. Mobile Computing and Networking* (MobiCom 2004), pp. 202 - 215, ACM Press, 2004.

[13] P. Ning and K. Sun, How to Misuse AODV: A Case Study of Inside Attacks against Mobile Ad-Hoc Routing Protocols, *Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy*, WestPoint, NY, 2003.

[14] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. *Proc. of MobiCom 2002*, Atlanta, 2002.

[15] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, pp. 38-47, 2004.

[16] C. Perkins, *Ad Hoc Networks*, Addison-Wesley, 2001.

[17] R. Oppliger, *Internet and Intranet Security*, Artech House, 1998.

[18] B.Wu, J.Wu, E. Fernandez, S. Magliveras, and M. Ilyas, Secure and Efficient Key Management in Mobile Ad Hoc Networks. *Proc. of 19th IEEE International Parallel & Distributed Processing Symposium*, Denver, 2005.