Enhanced Secure Routing Model for MANET

Vinay Kumar Pandey[1] Dr. Harvir Singh[2] Sanjay Kumar[3]

[1]Department of CSE UTU,Dehradun, India,
vkp1979@yahoo.co.in
[2]Department of CSE UTU, Dehradun, India,
dr.harvir@gmail.com
[3]Department of CSE, Benpour Technologies(P)Ltd,
sanju20077@gmail.com

ABSTRACT

Mobile Ad-hoc Network is group of wireless mobile device with restricted broadcast range and no use of base Infrastructure. The secure routing model helps for reduced honest elicitation and free riding problem. The term honest elicitation means it forward high recommendation for malicious node in order to avoid itself. It means the high recommendation for colluding malicious node. When operating in hostile or suspicious setting, MANETs require privacy and communication security in routing protocol. In this paper we present the type of attacks and operation on network layer with routing protocol technique i.e. based on an on-demand location based anonymous MANET routing protocol called SMRT (secure MANET routing technique with trust model) that achieves security and privacy against insider and outsider adversaries.

KEYWORDS

MANET security, secure protocol, mobility, AADS model, SMART.

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self-organizing system of mobile nodes that communicate with each other via wireless mechanism without central administration like access point or base station. The security Issue of Mobile Ad-hoc Network in-group communication is more complicated because the involvement of more sender and receiver. In previous literature the focus of earlier research is on unicast application. The effect of security attack on multicast MANETs are, therefore, still under research process.

In this paper we proposed the enhanced routing protocol that detect different attacks in a network using an advanced attack detection system (AADS) and switches to a particular protocol that can resist various attack for choose the optimal and secure path in network.

Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,
pp. 37–44, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2405

2. ROUTING IN MANET

Routing in mobile ad hoc network faces additional problem and challenges when compared to routing in wired network with fixed infrastructure. There are several protocols such as OSRP, AODV have been developed to cope with limitation imposed by ad hoc network environment. The problem of routing face some factors i.e. low bandwidth, dynamic topology, high power consumption and high error rates. Most of the protocols follow two design approaches to adopt the characteristics of ad hoc networks, namely the source-initiated on demand and table-driven approaches.

3. TYPES OF ATTACKS IN MANET

There is two types of attacks in Mobile ad hoc network, namely External attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from shared nodes, which are the part of network.

Based on threat analysis several specific attacks that can target the operation of routing protocol in ad hoc network.

A. Message Reply:

After the attacker intercepted message, it will store the message and re-transmit the message to produce the unauthorized effect because the message is transmitted in the air and easily can be intercepted.

B. Denial of Service:

Denial of Service attacks means the complete disruption of the routing function. Specific instances of denial of service attack include the sleep deprivation torture and routing table overflow. In sleep deprivation torture means the consumption of batteries of a specific node by keeping it engaged in routing decision. Another term routing table overflow attack aim is malicious node advertises route that go to non-existent node to authorized nodes available in the network. The attacker tries to create enough routes for disruption the routing. The proactive routing algorithms are more effective to table overflow attack because proactive algorithms is use for discover routing information before it is actually needed.

C. Black hole attack:

The black hole attack means the node exploits the mobile ad hoc routing protocol and attacker consumes intercepted packets without any forwarding. However the attacker runs the risk with neighboring node and modified packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of wrongdoing.

D. Reply attack:

This type of attack explain an attacker inject network routing traffic that has been captured previously. This attack create problem on the freshness of routes.

4. MOBILE ADHOC ROUTING PROTOCOL

There are different type of protocols have been developed to defend against various attacks on Mobile ad hoc network. In this we have mainly discuss two protocol i.e. secure link state protocol and On-demand secure routing protocol to provide safeguard against all the attacks discus in section III.

A. Secure Link State Protocol:

SLSP is a powerful and efficient protocol for solving the problem of routing function. It provides proactive routing for mobile ad hoc network. Secure link state protocol can be employed as standalone solution for proactive link state routing and combined with a reactive ad hoc routing protocol creating a hybrid model. Secure link state protocol is the combination of three component namely neighbor discovery, public key distribution and link state updates. Public key distribution technique used by nodes for broadcast the packets within zone. Link state information is broadcast periodically using node lookup protocol; it includes the MAC of sending node. The NLP inform the secure link state protocol if suspicious discrepancies are observed, such as two IP address having the same MAC trying to claim the medium access control of current node. Link state packets identified by the IP address of source node and use the 32 bit sequence number for updates with hash chain technique in the SAODV.The authentication of hash chain itself performed through anchor that contain digitally signed part of an link state update message. The receiver nodes verify signature using encryption technique they have previously cached using public key distribution phase of the protocol. Secure link state protocol maintain a priority ranking of neighbor nodes based on the rate of control traffic. SLSP provide secure neighbor discovery process and using Node lookup protocols for detect discrepancies IP and MAC address. Secure link state protocol offer protection against malicious node. This protocol resists attacks like denial of service and replay attack but some problem occur to resist the black hole attack.

B. On-demand Secure Routing Protocol:

An on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes. A common technique used in routing protocols for ad hoc wireless networks is to establish the routing paths on demand, as opposed to continually maintain a complete routing table.

The OSRP protocol is categories into three phases, namely route discovery with fault avoidance, byzantine fault detection and link weight management.

The first phase is route discovery is responsible for create a route between source node and destination node. The source node sign with its private key a route request message that is broadcasted to all neighbor nodes. This phase finds a least weight path from the source to the destination reason of using flooding; faulty link weight list and routing table overflow attack.

The second phase is Byzantine fault detection. This phase discovers faulty links on the path from the source to the destination. The adaptive probing technique identifies a faulty link after log n faults have occurred, where n is the length of the path. Data packets originating from source contain the nodes list called probe nodes, which send the acknowledgement for received packet.

If the reply is not received by source node a fault is registered on the path. Therefore a malicious node is not able to drop packets without dropping the list of the probe nodes. The fault detection algorithm is able to locate a faulty link after log n faults have been detected using binary search technique. This phase takes as input the full path and outputs a faulty link.

The final phase of the protocol is link weight management. This phase maintains a weight list of links discovered by the fault detection algorithm. The weight list is used by the route discovery phase to avoid faulty paths. The main aim of the protocol is to gives a strong on-demand routing service that is resilient to complex failure. The working of the protocol needs the existence of public key infrastructure in the mobile ad hoc network for certification of authentication of the participating nodes .the protocol manage to discover a fault free path if one exist with colluding malicious node in network.

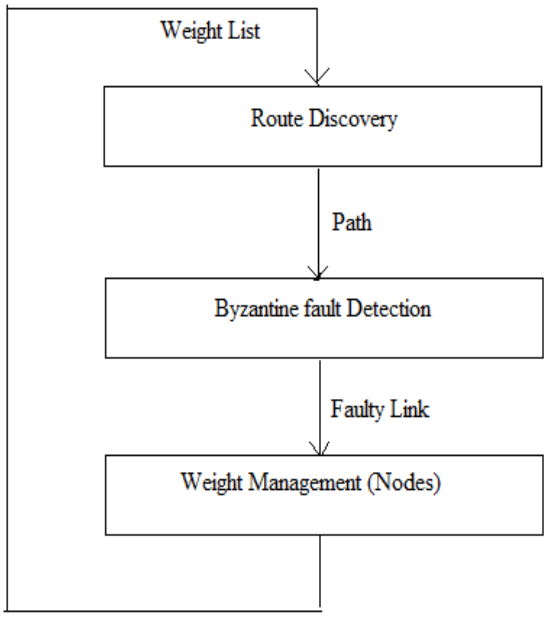

Figure1. The protocol operates in sequence and next protocol receives the output of previous.

So a limitation rests in the inability of the protocol to prevent wormhole attacks. If the wormhole link demonstrates byzantine behavior then the protocol will detect and avoid it. This protocol is can manage replay, routing table positioning and denial of services attacks but both protocol studied in [A, B] fail to defend against the black hole attack.

5. ADVANCE SECURE ROUTING MODEL FOR MANET

Basically, there are two components used in this model which must be implemented at every node because the entire participating node in mobile ad hoc network must have the resources needed for the working of Secure Link State Protocol (SLSP) and On-demand secure routing protocol (OSRP). The main components are:

C. Advance Attack Detection System:

This system is capable of detecting various attacks in mobile ad hoc network. In this paper, we have concentrated on detection of following attacks:

- Routing table overflow: This type of attack occurs in route maintenance phase where other attacks like black hole and sleep deprivation torture occurs in route discovery phase. After establishing an optimum path between source and destination the data packet pass through the network. The nodes used in the optimum path are known as probe nodes. When it receives the data packet, the probe sends the acknowledgement to the source and entry is maintained in a routing table.

- Black hole attack: The black hole attack occurs in route discovery phase. If the source node needs to send application layer data to the destination node in mobile ad hoc network using AODV, when there is not a route to the destination node in the routing table of the source node. So routing discovery process start firstly, the source node send a routing request packet (RREQ) to it next hop then the intermediate or destination node send routing response packet (RREP) to the source node. When it receives the RREP, the source node sends the application layer data to the destination node. If the node that was supposed to forward packet fails to do so within the certain timeout period, the black hole attack occurs.

- Replay attack: When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack. It means the attacker inject into network routing traffic and target the freshness of routes.

D. Switching System:

The advanced attack detection system detect the particular attack which is not resist by the underlying protocol, this switches another protocol to carry the further transmission. There are two possible cases of switching:

- Case 1: If the underling protocol is secure link state protocol before attack detection and black hole attack is detected. The advance attack detection system switches to OSRP Protocol.

- Case2: If the underlying protocol is OSRP before attack detection and denial of services or Replay attack is detected. The advance attack detection system switches to secure link state protocol.

So, by using the AADS model, user able to detect and resist all the above attacks [discussed in section III]. The schematic view of the proposed is given below.

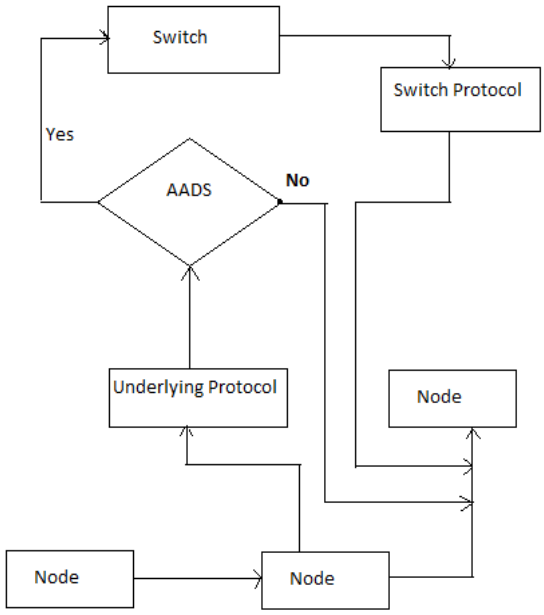

Figure2. Advance Secure Routing Model

E. SMRT Protocol Operation:

This section describes the secure MANET routing technique with trust model (SMRT) operation. SMRT is an anonymous location centric on-demand routing protocol that is work in underlying protocol with AADS. The basic operation of SMRT is similar to AODV. SMRT allows a source to specify a destination area and simultaneously discover multiple destination nodes in it. However, to keep the description simple, we assume that only one node exists within each destination area. There are some notations used in the operation of SMRT protocol is given below.

RREQ	**Route Request**
RREP	**Route Reply**
DST-AREA	**Destination area (or location)**
PK_X, SK_X	**Public, private key of X**
TS_X	**Time-stamp of X**
DST_{Loc}	**Exact location of a destination node**

Table 1.Notation Used

We assume that only one node exists within each destination area. The source broadcasts a route request (RREQ), which contains the destination location, in the form of coordinates and a radius – DST-AREA. The source starts by searching in an area with a smaller radius and if no reply is received within a specific time window, it increases the radius of the area and sends another RREQ. In any of these cases the RREP is logged as a failing one and the source waits to receive another RREP for this RREQ. Upon receiving a RREQ, each node first checks if *TSSRC* is valid. If not, the RREQ is dropped. Next, the node checks whether it has previously processed the same RREQ. The SMRT Data Message Format is mentioned below.

Message-Type =DATA (1 byte)
H(RREQ) (32 bytes)
H(RREP) (32 bytes)
TS_{SRC} (4 bytes)
E_{KS}(Data)

Figure3. SMRT Data Message Format

This is done by computing a hash of the new RREQ (*H* (*RREQ*)). Upon receiving a RREP, each node checks whether it has cached the corresponding *H* (*RREQ*). If not, the RREP is dropped since this node was not on the forward route. If *H* (*RREQ*) is already cached, the node checks if the same RREP has been processed. If so, the RREP is dropped. When the RREP is received, the source first check for the correctness of the time-stamp and the exact location of the replying node then verifies the group signature. If invalid, the RREP is discarded and logged as a failure. Figure 3 shows the format of data messages with appropriate field sizes. If the route breaks, a route error (RERR) message similar to that in AODV is generated. For backward compatibility, SMRT messages can be easily sent over IPv6. We can define a new extension header to carry SMRT route identifiers (i.e., < *H* (*RREP*), *H* (*RREQ*) >) and use it to encapsulate data packets. RREQ and RREP encapsulated inside an IPv6 header can be broadcasted based on DST-AREA. Since DST-AREA is only 4 bytes, in can fit into the IPv6 address, or it could be a part of PRISM extension header in RREQ.

6. CHALLENGES OF ROUTING PROTOCOL

The routing protocol secure link state protocol fails to prevent the black hole attack and On-demand secure routing protocol fails to resist denial of service attack but both protocols can resist replay and routing table positioning attacks.

So aims of this paper is proposing a new model “Advance Secure Routing Model for MANET” that joint feature of both protocols to resist all attacks discussed in section III.

7. CONCLUSION AND FUTURE WORK

MANETs present different threats due to difficult properties. These are open up very security risk from conventional wired network, and each of them how security is provided and maintained. Due to mobility and dynamic nature of mobile ad hoc network nodes, link breaks are likely to be common. So the network layer, in which routing take place, is vitally focused on MANET. The

attacks other than these are beyond the scope of this model. In this paper, we have faced various attacks in mobile ad hoc network and working of routing protocols that can resist various attacks using advance secure routing model.

REFERENCES

[1] Li Shi-Chang, Yang Hao-Lan and Zhu Qing-Sheng , "Research on MANET Security Architecture Design", In IEEE Conference on Signal Acquisition and processing, pp. 90-93, June 2010.
[2] Y. Dong, T. W. Chim, V. O. K. Li, S. M. Yiu, and C. K. Hui, "Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1536–1550,2009.
[3] Luo.j. fan, M., YeD.Black Hole Attack Prevention based on authentication mechanism, pp.173-177, IEEE 2008.
[4] Song J-H, Wong VWS, Leung VCM Secure position-based routing protocol for mobile ad hoc networks. Ad Hoc Networks, Volume 5, Issue 1:76–86, 2007
[5] Wang N-C, Huang Y-F, Chen J-C A stable weight-based on demand routing protocol for mobile ad hoc networks. Information Sciences: an International Journal, Volume 177, Issue 24:5522–5537, 2007.
[6] Eisbrener J, Murphy G, Eade D, Pinnow CK, Begum K, Park S, Yoo SM,Youn J-H ,Recycled path routing in mobile ad hoc networks. Computer Communications, Volume 29, Issue 9:1552–1560, 2006.
[7] David Holmer, Baruch Awerbuch and Herbert Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in The 8th ACM International Conference on Mobile Computing and Networking, September 2002.
[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, \Ariadne A secure on-demand routing protocol for ad hoc networks," in The 8th ACM International Conference on Mobile Computing and Networking, September 2002.
[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks", In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), June 2002, pp. 3-13, June 2002.
[10] P. Papadimitratos and Z. Haas, \Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27{31, January 2002.
[11] D. B. Johnson, D. A. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multi-HopWireless Ad Hoc Networks. in Ad Hoc Networking, ch. 5, pp. 139-172. Addison-Wesley, 2001.
[12] C. E. Perkins and E. M. Royer, Ad hoc Networking, ch. Ad hoc On-Demand Distance Vector Routing. Addison-Wesley, 2000.
[13] S. Marti, T. Giuli, K. Lai, and M. Baker, \Mitigating routing misbehavior in mobile ad hoc networks," in The 6th ACM International Conference on Mobile Computing and Networking, August 2000.

AUTHORS

Vinay Kr. Pandey PhD*(CSE), M.Tech(CSE), Professor & HOD in Computer Science & Engineering at shivalik college of engineering and He is pursuing PhD on "Enhanced Security Framework for Mobile Ad Hoc Networks " from UTU, Dehradun & completed M.Tech in CSE from UTU Dehradun. He has also done M.Tech in (IT) from Lucknow. He has more than 10 years of experience in teaching and industry, along with 3yrs experience in research. He has guided students of B.Tech and M.Tech on various projects and new emerging technologies. An area of interests is Wireless Communication.