International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
1793-8201

Implementation of Routing Security Aspects in AODV

Suman Deswal and Sukhbir Singh

***Abstract*—security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wireline networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. It is vital to protect the network from different kinds of security threats. This paper proposes a security solution for manets using a pre-existing routing protocol, ad hoc on-demand vector routing (aodv), using password security for each routing node and timeliness to update routing table. Aodv and saodv(secure aodv) are simulated and the performance of both the protocols are evaluated for varying number of nodes and malicious nodes. The performance of saodv was stable whereas that of aodv was found to be degrading sharply with intrusion of some malicious nodes in the network.**

Index Terms—AODV, MANETs, routing, security

I. Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes that can instantly establish a network, whenever they coexist in the same neighbourhood without the need of any fixed infrastructure or centralized administration. The role of routing protocols in an ad hoc network is to allow the source to find routes to destination with the cooperation of other nodes. Due to the arbitrary movement of the nodes, the network topology changes rapidly and randomly. Hence the routing protocol must also be able to react to these changes and must enable the nodes to identify new routes to maintain connectivity. The problem of security in MANETs[2][3] represents a serious challenge. This is primarily due to the high dynamic nature of the ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory and battery power (energy) of each individual node in the network. Rapid and frequent routing protocol interaction between nodes is required.

Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resources leading to many new opportunities for possible Denial-of-Service (DoS) attacks through the routing protocol. One of the most efficient routing protocols into which security measures can be included is Ad hoc On-demand Distance Vector Routing (AODV)[1]. It is observed that complete belief of the network on nodes can lead to many routing attacks. To avoid this, security measures are added to AODV to make it Secure AODV (hence forth called SAODV). In SAODV, each node checks the security of its neighbors before forwarding route requests. It won't forward route request packets to insecure neighbors (or malicious nodes). This measure, clearly, ensures that malicious nodes will not participate in the data transfer from the source to the destination.

II. Literature Survey

Security and secure routing in MANETs has been of interest for quite long time in the research community. In this section we will give a short overview of existing work and entry points to the literature. Many different types of attacks have been proposed so far. A selection of them are the wormhole attack, the blackhole attack[2], and the grayhole attack[10]. [11] describes various passive attacks in MANETs. In most publications on security issues, these or other attacks are presented and discussed. Many different secure routing approaches[7][8][9] have been proposed so far. Secure efficient Adhoc Distance Vector[10],a routing protocol based on the design of Destination Sequenced Distance Vector routing protocol provides a robust protocol against attackers trying to create incorrect routing state in the other node. An I-SEAD protocol[9] prevents an attacker from tampering the next hop or the destination field in the route update. A very complete and extensive overview on ad hoc routing challenges, mechanisms and protocols has been presented by Hu and Perrig in [4]. A detailed section on securing the AODV protocol is given in this publication. The first approach of securing the AODV protocol has been made by Zapata with his SAODV [5]. In a second publication [6] the protocol is presented in greater detail. Further, related issues like key management are presented briefly. In [15], a layered architecture for security has been designed which provides for modularity, simplicity, flexibility and standardization of protocols. The 5 layers-End to end security layer, network security layer, routing security layer, communication security layer and trust infrastructure layer have been described. [16] discusses a resiliency oriented security solution for various security threats. It not only minimizes the effect of malicious attacks but also cope with network faults like node misconfiguration, extreme network overload, operational

Suman Deswal is with the Department of Computer Science & Engineering, DCRUST, Murthal, Haryana, India. e-mail(suman_gulia2000@yahoo.co.in)
Sukhbir Singh is with the Department of Computer Science & Engineering, NCCE, Israna, Haryana, India. e-mail(id:boora_s@yahoo.com).

failures. [17] provides a protocol for implementing security in AODV protocol which provides protection of route discovery and transfer of data. The scheme presented in [17] is based on point to point and end to end encryption using symmetric key based mechanism. The various active and passive attacks are avoided by efficient key verification mechanism and a multilayered enciphering scheme.

III. OVERVIEW OF AODV

In this section, we provide an overview of AODV.

Ad hoc On demand Distance Vector Routing (AODV) [1] protocol is proved to be an efficient routing protocol for implementation in Ad hoc networks. It is a Source-Initiated On-Demand or Reactive Routing Protocol. When a source node desires to send a message to a certain destination node to which it does not have a valid route, it initiates a route discovery process. The source node broadcasts an RREQ (Route REQuest) message to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a route to the destination in its routing table is reached. During the process of forwarding the RREQ, an intermediate node record in its routing table (i.e., precursor list) the address of the neighbour from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Additional copies of the same RREQ received later are discarded. Once the RREQ reaches the destination or an intermediate node with a route, the respective node responds by unicasting an RREP (Route REPly) message back to the neighbor from which it first received the RREQ, which relays the RREP backward via the precursor nodes to the source node. Routes are maintained as follows: HELLO beacons are sent periodically via broadcast to the neighboring nodes. When a source node moves, it has to re-initiate the route discovery protocol to find a new route to the destination. On the other hand, when an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate an RERR (Route ERRor) message to each of its active upstream neighbors. These nodes in turn propagate the RERR packet to their upstream neighbors, and so on until the source node is reached. The source node may then choose to re-initiate the route discovery for that destination if a route is still desired. Every routing table entry at every node must include the latest information available about the sequence number for the IP address of the destination node for which the route table entry is maintained. This sequence number is called the 'destination sequence number'. It is updated whenever a node receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination. AODV depends on each node in the network to own and maintain its destination sequence number to guarantee the loop-freedom of all the routes towards that node. A destination node increments its own sequence number under two circumstances:

- immediately before a node originates a route discovery; it must increment its own sequence number. This prevents problems with deleted reverse routes to the originator of a RREQ.
- immediately before a destination node originates a RREP in response to a RREQ, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.

IV. SECURITY ISSUES IN MANETS

We analyze the security issues concerning MANETs. A node is malicious if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. The attack on MANET can be classified as the active and passive attacks:

*Passive attacks***:** A passive routing attack does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to the routing traffic. Hence such attacks are difficult to detect.

Active attacks An active attack attempts to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data steam or modifying packets transition through the network. Active attack are of two types: external and internal. An external attack is one caused by nodes that do not belong to the network. An internal attack is one from compromised or hijacked nodes that belong to the network. As malicious nodes already belong to the network as authorized parties, and hence are protected with network security mechanisms and services, therefore, internal attacks are more severe.

Blackhole: An attacker can project itself as having shortest route to a destination [2], whose data packets it wants to intercept, thereby causing the source to send data packets via this node. A malicious node receiving the RREQ may claim to have route to the desired destination by sending RREP back to the originator. If the source receives this RREP first then it sends all data packets via this malicious node and thereby leaving the fate of those data packets on the malicious node. The malicious node now discards or consumes all the data packets, leading to the complete loss of all data packets.

*Grayhole***:** An attacker forwards all RREQs and RREPs but forwards only a few data packets[10], dropping all other data packets. Clearly it points out a lapse in the routing protocol. This type of attack is known as grayhole problem. By nature, it belongs to the set of internal active attacks.

Wormhole: Wormhole[10] is a collection of two or more malicious nodes belonging to the ad hoc network that are connected by a private network connection. Suppose two nodes A and B make a wormhole. Then A forwards all packets that it receives to B through the worm hole to be forwarded by B normally, similarly, B forwards all packets to A, that it receives, through the wormhole. It clearly disrupts routing by short circuiting the normal flow of routing packets.

Denial of service (DoS): The DoS[2] attack results when the network bandwidth is hijacked by a malicious node. It can be done in several ways. One way is to flood any centralized resource so that the network crashes or no longer operates correctly. For example, a malicious node by generating frequent route requests can make the network resources

unavailable to other nodes.

Routing table overflow: A malicious node, by generating route requests to several non-existent destinations, causes other nodes to create several entries in their routing table[13], one for each desired (non-existent) destination to keep the address of the sender in the precursor field so that it can transmit RREP or RERR back to the originator, and leads to the overflow of their routing table. When the routing table of a node overflows, then it doesn't entertain any further route requests (including those for existent destinations from non-malicious nodes). As a result the route discovery process gets adversely affected.

Energy consummation: Energy is a critical parameter in MANETs. Battery-powered nodes try to conserve energy by transmitting only when absolutely necessary. An attacker, by sending route requests (frequent and unnecessary) or forwarding unnecessary packets, makes other nodes consume energy leading to useless consumption of energy[12] .

V. Proposed Secure AODV

SAODV avoids active external attacks by not forwarding route requests to the external nodes. This is done by authenticating all the nodes of the network. In the implementation carried out here the authentication of a node is determined by its password. Here all the nodes of the network are assigned the same password. Hence before forwarding route request to a neighbour, a node first checks the authenticity of the neighbouring node by verifying its password. If it is found legal, then only route request is forwarded. In this way, external nodes are excluded from entry into the network. The problem of route table overflow is solved by updating the tables at regular intervals of 70ms.

SAODV solves the problem of blackhole by disabling the intermediate nodes to send route replies and there by allowing the generation of route reply only by the destination node. After receiving route reply from an intermediate node, the originator sends an enquiry to check whether a route from that intermediate node to the destination node exists or not. If it exists, the originator trusts the intermediate node and sends out the data packets via this intermediate node. If not, the originator simply discards the reply message from the intermediate node, sends out alarm message to the network, isolates that intermediate node from the network and starts a new route discovery process. No malicious node can read the data in the data packet due to the encryption of the message. Every node checks password before forwarding the RREQ. All nodes on the route from source to destination are secure and fulfill security requirements of the sender.

VI. Simulations and Results

A simulation testbed for mobile ad hoc network is developed to evaluate the performance of the AODV and SAODV routing protocol. Both the protocols were simulated over this testbed and its performance was studied for various environments. The testbed should have the following properties:

Closed area: It should simulate the environment of a closed area in which nodes move.

Nodes: The nodes should be mobile. Their speed and directions should be controllable so that they can be moved according to the mobility model we wish to use.

Mobility model: The mobility model used here is the 'random waypoint model'. According to this, initially all the nodes are distributed uniformly. Then each one of them chooses a random destination and starts moving in the direction of that destination. After reaching that destination, it remains stationary for some period of time (called pause time) and then again chooses a new destination and starts moving towards it. This cycle continues until the total run time, which is again a controllable parameter.

Graphics support: It should show all the movements and communications of nodes.

The testbed developed in the above mentioned way is used to run AODV on it. The values of some parameters considered during the study are noted below.

Area	1500*300 meter^2
One time quantum	50 msecs
Speed of the nodes	20 meters/second
Run time for the simulation	200 seconds
Direct Transmission Range of the nodes	250 meters
Channel capacity	1.6 Mbps

Where channel capacity is the maximum number of data packets transmitted through the channel per second.

Using the above constant parameters, the simulation is carried out for 200 seconds for each set of variable input parameters. All the results are averaged over hundred runs, for each combination of these input parameters.

A. No. of data packets Vs No. of nodes in the network

It may be seen from Fig. 1 that AODV and SAODV have almost similar performance when the number of malicious nodes in the network is zero. It is proved [5] that for a system employing low security level, when there are no malicious nodes, SAODV takes about 1% extra time in transmitting the data packets when compared to AODV.

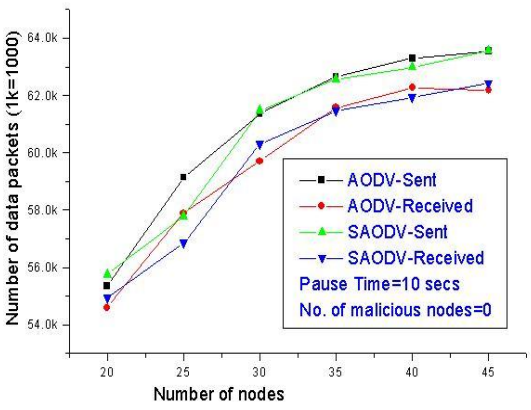

Fig.1 No. of data packets Vs No. of nodes in the network

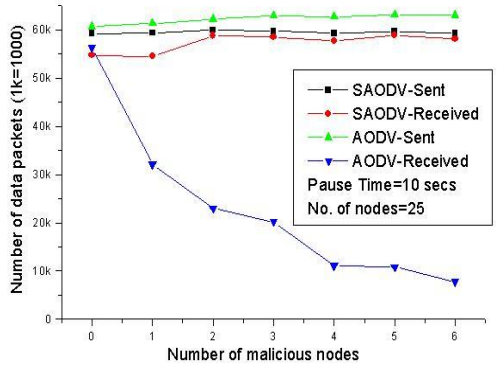

Fig.2 No. of data packets Vs No. of malicious nodes

Hence the number of data packets sent by SAODV, falls short when compared to those by AODV, by about 1%. This performance shown in the graph confirms this result.

B. *No. of data packets Vs No. of malicious nodes*

It may be seen from Fig. 2 that with the increase in the number of malicious nodes, the number of data packets sent by AODV increases marginally, where as those by SAODV remains almost constant. It indicates that malicious nodes have no effect on the number of data packets send by SAODV. While the data packets received in case of AODV falls drastically with increase in the number of malicious nodes, those packets received in case of SAODV increases initially and then remains constant. It clearly indicates that AODV is badly affected by malicious nodes.

C. *Packet Delivery Ratio (PDR) Vs No. of malicious nodes*

PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. It is clear from Fig. 3 that PDR of AODV is heavily affected by the malicious nodes where as the PDR of SAODV is immune to it. This graph confirms that while SAODV is secure against blackholes, AODV is not.

VII. CONCLUSIONS

In this paper we presented a selection of analysis results for the secure routing protocol SAODV. The implementation of the protocol has been done using C++ language. It was found that the resulting secure routing protocol, SAODV, can secure the ad hoc network from the routing attacks of black hole, routing table overflow and external and passive attacks and also keeps only the latest and correct information in the routing table. Since this protocol enforces that no intermediate node can originate RREP therefore after receiving route request, only the destination will initiate RREP. No malicious node can read the data in the data packet due to the encryption of the message. Every node checks password before forwarding the RREQ. Hence all nodes on the route from source to destination are secure and fulfill security requirements of the sender. The simulation results prove the feasibility of secure routing protocols. Performance of AODV was found degrading sharply with.

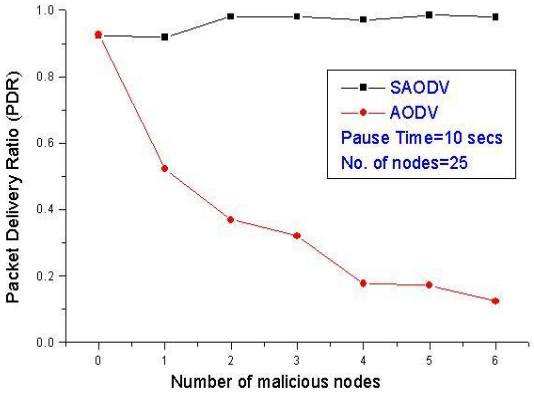

Fig.3 Packet Delivery Ratio (PDR) Vs No. of malicious nodes

REFERENCES

[1] C. E. Perkin, E. M. Royer, "Ad-hoc on demand distance vector(AODV)routing," The Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999.

[2] Hongmei Deng, Wei Li, and Dharma P. Agarwal "Routing security in wireless Ad Hoc networks" IEEE Communications Magazine, October 2002.

[3] Lidong Zhou and Zygmunt J.Haas "Securing Ad Hoc networks" IEEE Network,November/December 1999.

[4] Yih-Chun Hu, David B.Johnson and Adrian Perrig" SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks" IEEE fourth workshop (SMCSA'02) June 2002 Calicoon NewYork.

[5] Seung Yi, Prasad Naldurg, Robin Kravets "A security-aware routing protocol for wireless Ad Hoc networks" http://www-sal.cs.uiuc.edu/~rhk/pubs/ SCI2002.pdf.

[6] B.Lu and U.W.Pooch "Cooperative security-enforcement routing in mobile Ad Hoc networks" IEEE2002

[7] Panagiotis Papadimitratos and Zygmunt J. Haas " Secure routing for mobile Ad hoc networks" Wireless Networks Laboratory, School of Electrical and Computer Engineering, Cornell University,395 and 323 F.T. Rhodes Hall, Ithaca NY 14853

[8] Varaprasad, G.; Venkataram, P. "**The analysis of secure routing in mobile Ad Hoc network"** Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on Volume 4, Issue , 13-15 Dec. 2007 Page(s):393 – 397

[9] Wei-Shen Lai1, Chu-Hsing Lin2, Jung-Chun Liu2, Yen-Lin Huang2, Mei-Chun Chou2 "I-SEAD: A secure routing protocol for mobile Ad Hoc networks"

[10] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless" IEEE fourth workshop (SMCSA'02) June 2002 Calicoon NewYork.

[11] Jiejun Kong, Xiaoyan Hong, Mario Gerla "A new set of passive routing attacks in mobile ad hoc networks" MILCOM'03

[12] J. Cano, Kim Dongkyun, J.J Garcia-Luna-Aceves, P. Manzoni, k. Obraczka ,"Power-aware routing based on the energy drain rate for mobile ad hoc networks" Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on , 2002 Page(s):565-569.

[13] Y. Zhang and W. Lee. Intrusion detection in wireless Ad-Hoc networks. MOBICOM 2000,Boston, MA, USA.

[14] S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations. IETF RFC2501, 1999.

[15] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen "A security architecture for Mobile Ad Hoc networks"

[16] Hao Yang, Haiyun Luo, Fanye, Songwu Lu, and Lixia Zhang "Security in mobile ad hoc networks challenges and solutions"

[17] Asad Amir Pirzada and Chris McDonald "Secure routing with the AODV protocol" 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.