ISSN: 2321-7782 (Online)

Volume 3, Issue 3, March 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Ensemble Approach of Intrusion Detection and Packet Structure to Achieve Efficient and Secure On Demand Routing Protocol

Rahul Tiwari[1]
Department of Computer Science and Engineering,
LNCT, RGPV University
Bhopal, INDIA

Sunil Phulre[2]
Asst.Prof. Department of Computer Science and Engineering
LNCT, RGPV University
Bhopal, INDIA

Dr.Vineet Richhariya[3]
Prof. Department of Computer Science and Engineering
LNCT, RGPV University
Bhopal, INDIA

Abstract: Networks are used in various fields. Network's popularity has motivated the development of mobile ad-hoc networks (MANETs). A mobile Ad-hoc network is a kind of decentralized wireless system which creates a fast changing network. Due to the dynamic nature and changing topology, MANET is a growing dynamic network, also called mobile mesh network. Mobile ad-hoc network has various kinds of security concern problems, which are caused by their nature of collaborative and open systems and by limited availability of assets. Any central coordinator's absence makes the routing a complex one compared to traditional networks. There are various Routing protocols in Mobile Ad-hoc network but the ad hoc on demand distance vector (AODV) is most popular widely used as it has many attributes. The performance will downgrade when particular host or nodes fails as it sends message regarding this to particular source. This paper observes the performance of AODV Reactive routing protocol and Analyzes different attacks that can be possible on AODV. The paper also explained two layer schemes with security which includes intrusion detection algorithm which further aimed at improving normal AODV's performance along with encryption of the packet into another format. Thus, this proposed approach improved by using NS2 simulator, a event-driven simulator which helps to improve various factors like performance factor and security factor.

Keywords: Intrusion; Detection; Blackhole; DoS;MANET.

I. Introduction

A Mobile Ad Hoc Network (MANET) is a decentralized infrstructureless network in which nodes cooperate to forward data frm a source to a destination. Each node in a MANET acts both as a router and as a host.

Several routing protocols have been designed for MANETs [1] to optimize network routing performance over the past years. The major issues involved in designing a routing protocol for MANET are nodes mobility, bandwidth constrained and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology.

MANET routing protocols can be classified as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. While in reactive (on-demand) routing protocols, routes are created whenever a source requires sending data to a destination node which means that these protocols are initiated by a source on demand. In this paper, we concentrate on the AODV protocol [2]. AODV is a reactive protocol, chosen by the IETF for standardization, which has been extensively studied. Conventional MANET routing protocols assume that all nodes cooperate without maliciously disrupting the operation of the protocol and do not provide defense against malicious attackers. However, the existence of malicious nodes cannot be ignored in computer networks, especially in MANETs because of the wireless nature of the network. MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself [2] due its characteristics. Nodes in MANET have limited computation and power capabilities that make the network more vulnerable to Denial of Service (DoS) attacks. It is difficult to implement cryptography and key management algorithms which need high computations like public key algorithms. Node mobility introduces also a difficulty of distinguishing between stale routes and fake routes. A malicious node can attack the network layer in MANET either by not forwarding packets or by changing some parameters of routing messages such as sequence number and IP addresses, sending fake messages several times and sending fake routing information to disrupt routing operations. There are a large number of existing attacks against MANET [3] and solutions to these attacks. Simulation and study of such attacks [3] [4] has become necessary in order to provide defence mechanisms against these types of attacks.

The rest of the paper is organized as follows. In section II, an overview of the AODV routing protocol is presented and the impact of some attacks on MANET is discussed. In section III, the simulation parameters and results are given. In section IV concluding remarks are introduced.

II. AD- HOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV)

Ad hoc on demand vector (AODV) [5] has two operating modes, i.e., route discovery and route maintenance. This section discusses both operating modes.

a. Route discovery mode

Figure 1 illustrates a route discovery process at which the source node A needs to obtain a routing-path towards the destination node D. As shown in the figure, a source node broadcasts a route request (RREQ) message to all neighbours since the node does not have a route-path to the destination node D. After receiving the RREQ message, a relay node B will check its routing table to determine if the node has a routepath to the destination node. Because the relay node does not have the route-path, the node then rebroadcasts the RREQ message. However, before rebroadcasting the route request message, the node will record the route-path to the last node visited by the RREQ message. All the process will be repeated until the route request message arrives to the destination node. When the RREQ message reaches the destination node, the destination node will unicast a route reply (RREP) message as the response to the RREQ message.

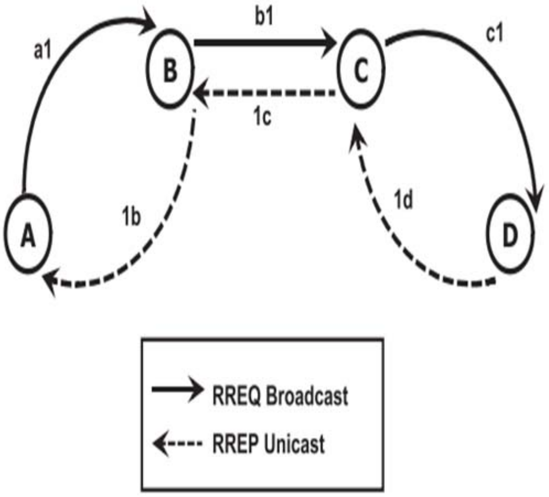
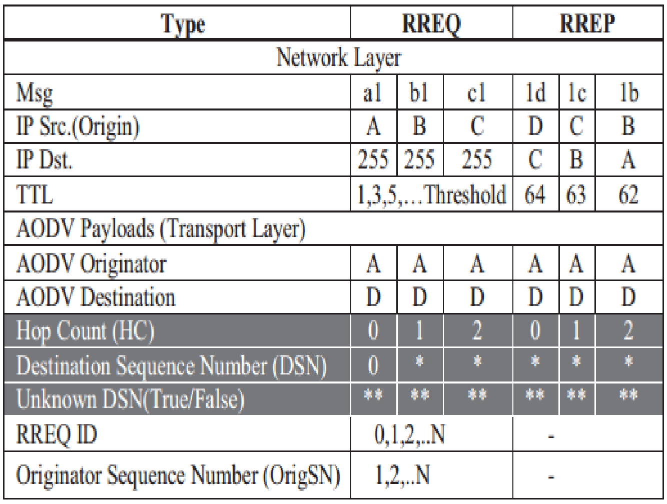


Fig. 1. AODV Route Discovery

ABLE I. shows the details of RREQ and RREP messages delivered by all nodes for discovering the route-path to the destination node. In the table, a1, b1, and c1 denotes route request messages; meanwhile 1d, and 1b symbolizes route reply messages. Each routing message has several fields to keep the routing data, for example, 'IP Src' for holding IP address of the source node, and 'OrigSN' for storing destination sequence number (DSN) of the originator node. In addition, the shaded rows in the table, i.e., HC, DSN, and Unknown DSN fields, store mutable data of the routing messages. These fields will be updated by the local node visited by the routing messages. As a result, the DSN data (‘*’) will change follow the DSN owned by the local node.

b. Route Maintenance

In routing, route maintenance will be used for adapting the network topology changes. For the purpose of route maintenance, all nodes in AODV must continuously listen to the communication channels for detecting link failure. Incoming of RREQ and RREP messages every n seconds to a node indicates that the route paths exist and no link fails between the node and the sender of messages. However, the unavailability of the messages for certain period indicates the link problems. If the node detects a link failure, it can send a hello message to check the failure. Furthermore, the succeeding of link failure detection insists that all nodes answer each of the incoming messages.



Type	RREQ			RREP		
Network Layer						
Msg	a1	b1	c1	1d	1c	1b
IP Src.(Origin)	A	B	C	D	C	B
IP Dst.	255	255	255	C	B	A
TTL	1,3,5,…Threshold			64	63	62
AODV Payloads (Transport Layer)						
AODV Originator	A	A	A	A	A	A
AODV Destination	D	D	D	D	D	D
Hop Count (HC)	0	1	2	0	1	2
Destination Sequence Number (DSN)	0	*	*	*	*	*
Unknown DSN(True/False)	**	**	**	**	**	**
RREQ ID	0,1,2,..N			-		
Originator Sequence Number (OrigSN)	1,2,..N			-		

When a node detects the link failure, the node can generate a route error (RERR) message. The following is the requirements to generate the message:

a. if it detects a link break for the next hop of an active route in its routing table while transmitting data

b. if it gets a data message destined to a node for which it does not have an active route

c. if it receives an RERR from a neighbor for one or more active routes.

Figure 2 shows the process taken by nodes when a broken link detected. As shown in the figure, node 6 has detected a link failure while transmitting the data to node 9. Node 6 could not receive any response from node 9 after a certain period of time. Node 6 then generated an RERR message, and propagated the message back towards node 2. When node 4 receives the RERR from node 6, it compares and removes any entry in its routing table that has the RERR destination. The RERR itself is then sent either through broadcast or unicast message transmission

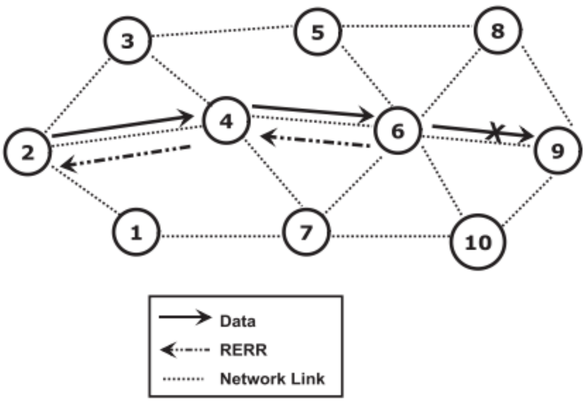


Fig. 2. Route Error Detection

c. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations

III. AODV Protocol And Security Flaws

Ad Hoc On-Demand Vector Routing (AODV) [6] is a reactive routing protocol. It uses destination sequence numbers to ensure the freshness of routes and guarantee loop freedom. To fid a path to a destination, a node broadcasts a route request (RREQ) packet to its neighbors using a new sequence number. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ unless it has a fresher one. When the intended destination or an intermediate node that has a fresh route to the destination receives the RREQ, it unicasts a reply by sending a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. Then the source node starts sending data packets to the destination node through the neighboring node that fist responded with an RREP. When an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate a route error (RERR) packet to each of its active upstream neighbors. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deal with data transmission. This scenario decreases the memory overhead, minimizes the use of network resources, and runs well in high mobility situation

The behavior of a malicious node is to disrupt the operation of the AODV routing protocol [6]. The malicious node can spoof source or destination IP address, modify RREQ or RREP packets and/or generate fake RREP or RERR packets. Some of the attacks such as blackhole and grayhole attack are discovered by the source node in connection-oriented protocols such as TCP because the lack of acknowledgments. The source node understands that there is a link error because the destination node does not send ACK packets. If the source 290 node sends out UDP data packets the problem is not detected because UDP is a connectionless protocol.

d. Flooding Attack on AODV

In a flooding attack [7], a malicious node takes advantage of the route discovery process of the AODV routing protocol. The malicious node aims to flood the network with a large number of RREQs to non-existent destinations in the network which takes a lot of the network resources. Since the destination does not exist in the network, a RREP packet cannot be generated by any node in the network and all the nodes keep on flooding the RREQ packet. When a large number of fake RREQ packets are broadcast into the network, new routes can no longer be added and the network is unable to transmit data packets. Thus, it leads to congestion in the network and overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a DoS attack. Moreover, unnecessary forwarding of these fake RREQ packets has serious effects in MANET as a result of limited computational and power resources of nodes.

However, the AODV protocol can mitigate against this attack by reducing the maximum number of RREQs that a node allowed to send per second.

e. Selfi Attack on AODV

In MANETs the nodes cooperate to forward data and routing packets from one node to another node. A selfish node is the node that saves its resources; such as battery, by not cooperating in the network operations. A selfish node affects the network performance as it does not correctly process routing or data packets based on the routing protocol. The selfish node behavior is known as a selective existence attack [7]. Selective existence is kind of a passive attack as the node neither participates in the network operation nor changes the content of packets.

The selfish node does not even send any HELLO messages and drops all data and control packets even if these packets are sent to it. When a selfish node needs to send data to another node, it starts working as normal AODV operation. After it fishes sending its data, the node returns to its silent mode and the selfish behavior by dropping all data and routing packets directed through it. Neighbor nodes detect the absence of the selfish node after an interval of silence, and will assume that the node has left their neighborhood. So, they invalidate their own route entries to this node and selfish node becomes invisible to the network.

f. Grayhole Attack on AODV

In a grayhole attack [8], a malicious node behaves normally as a truthful node during the route discovery process by replying with true RREP messages to the nodes that started RREQ messages. After the source node starts sending data through the malicious node, the malicious node starts dropping these data packets to launch a (DoS) denial of service attack. So, the malicious node forwards routing packets and drops data packets. This selective dropping makes grayhole attacks much more difficult to detect than blackhole attacks. Grayhole attack is also known as node misbehaving attack [8] as the malicious node misleads the network by agreeing to forward the packets in the network.

g. Blackhole Attack on AODV

In a blackhole attack [8], a malicious node absorbs the network traff and drops all packets. To carry out a blackhole attack, a malicious node waits for incoming RREQ packets from other nodes. When the malicious node receives an RREQ message, without checking its routing table, it inuniately sends a false RREP with a high sequence number and zero hop count to spoof its neighbours that it has the best route to the destination. Thus, the malicious node reply will be received by the source node before any reply from other nodes. When a source node receives multiple RREP, it chooses the RREP with the largest destination sequence number and the smallest hop count. Then the source node ignores other RREP packets and begins sending data packets over the malicious node. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the destination node. The malicious node attacks all RREQ packets in this way and takes over all routes. Therefore all packets are sent to a point where they are not forwarding anywhere. If the malicious node generates false RREP messages that appear to come from another victim node, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

IV. Related Work

AODV routing protocol performs both unicast and multicast routing. It maintains the route as long as they are needed by the source node. It uses the sequence number field to avoid the looping and to ensure the freshness of the route. As wireless network are prone to path breakage due to the mobility of the nodes, fading environment etc., so it is beneficial to provide some stable routes which can improves the performance of AODV protocol. Many researchers have proposed changes in the AODV protocol for increasing the efficiency, stability and security [1] [7] [8] of the MANETs.

The main problems that should be considered are energy efficiency and security in Adhoc networks. The resources present in MANET are limited, e.g., battery power MANET is very important resource as it has limited life and are not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission. Considering the above problems Gomez et al. proposed the PARO protocol which evaluated the distance between two nodes and after the distance calculation determine the transmission power needed to reduce power consumption. In PARO protocol it is assumed that each node can directly communicate with all the other node in the network (a one-hop network). A sending node uses the maximum power to transmit the first packet to the destination node and receives the ACK packet from destination. Then it determines the distance from itself to destination node and compute the minimum power needed for data transmission. Because the network is fully connected in PARO, broadcasting messages to the source and the destination node result in extra power consumption. Yang et al. have proposed a PAMP (Power aware multipath routing protocol) where routes are created by calculating the remaining power of nodes and recorded in RREQ packets. When destination node receives this RREQ packet it calculates the amount of power needed for data transmission and compares the both. If remaining power is less than the required power then destination node waits for the next RREQ consequently very long delay occurs in the route creation process.

Wang et al. have proposed a power efficient routing and maintenance protocol in MANET which removes some drawbacks of PAMP protocol. This protocol mainly considers the transmission bandwidth between two nodes and creates the routes on the basis of the power available for the data transmission in those routes. Vadival et al. have proposed an energy efficient with secured reliable routing protocol (EESRRP) for MANET. This protocol creates the routes on the basis of some threshold value of the power and packet drop ratio using AODV protocol. A new power aware multicast routing protocol for MANET which similar to the PAMP protocol but has less overheads is proposed by Varaprasad et al. If path breakage occurs in the MANET then lot of energy wasted in the creation of the new routes, due to flooding of RREQ packets. Pan et al. have proposed a local repair mechanism for on-demand routing in MANET. This protocol repairs the route locally whenever route breakage occurs, without notifying the RERR message to the source node and reduces the overheads of route maintenance. But they did not consider the security and the battery power of the nodes. Security in MANET is another big issue in current days. The proper security mechanism for detecting the possible attacks in AODV routing protocol needs to be incorporated for the security. Many type of attacks are possible in MANET and the most frequent one is packet dropping attack. John and Vivekanandan have proposed a framework for secure routing in Mobile and ad-hoc network. This protocol focus on cooperation in packet forwarding. A context-free protocol there is no need to know whether nodes are selfish are not, so this protocol does not need to track node's behavior to build a context consequently avoiding all the troubles caused by context maintenance. Such a context-free solution is very different from traditional context-based ones and must be designed in a totally new way. But in this protocol security mainly d epends on the cooperation of the nodes. A secure energy efficient routing protocol for wireless ad-hoc networks has been proposed by Mahimkar et al. which selects the paths along nodes with a higher reputation number and higher residual battery capacity.

In Mobile and ad-hoc network the power with the node is a scarce resource, which can not be replaced. Also the very applications of MANET for real life scenario makes it prone to attack by the external/internal agencies. Many methods have been proposed to look in to those problems but a lot of overhead is associated with them. Therefore, in this work an energy shaving routing scheme using dynamic route shortening and local route repair mechanism id developed. A security mechanism is also designed by using the trust value of the node to locate the reliable communication path which detect the malicious node in the network.

V. Proposed Work

The proposed protocol uses challenges to establish security in the ad hoc mobile network. Proposed work is divided into two parts.

Part 1: Communication

1. Initial Network
2. Make connection
3. Encrypt Packets
4. Change format of the packets into code1 and code2
5. Start Communication

6. Send Packet of Network

Part 2: Intrusion Detection

1. Check Every node behavior
2. If any node it sending packets to itself then warn the node.
3. If node would not improve it's behavior then block the node.

VI. Simulation And Results

The performance of proposed algorithms are implementaed on network simulator (NS-2) and the results are compared with original AODV to check the performance. So by the result comparison we can say the now there are less consumption in the network and now AODV performs better than the original AODV. To reduce the packet dropping attack in the network the security mechanism is implemented to detect the malicious node in the network and hence, reducing the packet dropping attack in the network. It is evident from the results that the proposed algorithms are able to save energy of the nodes in the network as well as able to find the malicious nodes in the network.The simulation parameters used to implement the proposed algorithms have been tabulated in Table 1.

TABLE 2: SIMULATION PARAMETERS USED IN SIMULATION

Simulation Time	**360 seconds**
Protocol	**Normal, Unsecure and Proposed Work**
Area:	**1000 x1000**
Traffic	**TCP/FTP**
Channel	**Wireless**
Operation mode	**802.11**
Mobility	**Random waypoint**
Antenna	**Omni directional**
IFQ	**50**
Nodes	**50**
IFQLEN	**1000**

The following parameters have been used for evaluation of the performance of proposed algorithms: Non-Authentic Packets: It shows the effectiveness of the attackers in network. It's effect is shown in fig 3.

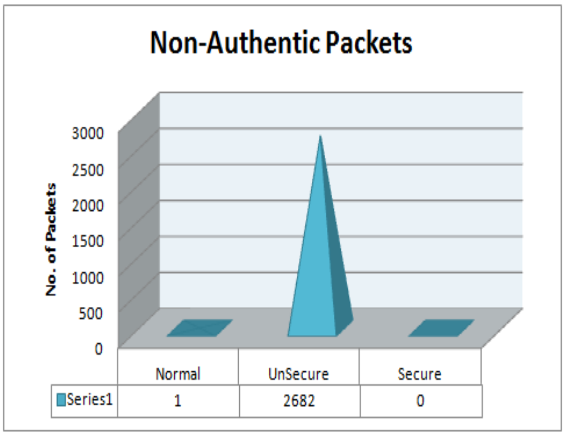


Fig 3: Number of non-authentic packets in network due to attachers node

Number of Attacking Nodes: It shows that how many nodes are still attacking or not getting block it's abnormal behaviour in the network. This effect is shown in fig 4.

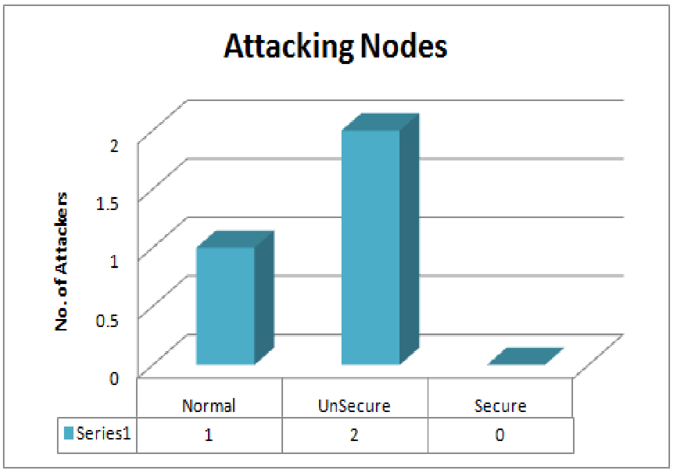


Fig 4: Number of Attaching node effecting the network

VII. CONCLUSION

This paper provides security to network; the malicious nodes are easily identified and isolated. By checking the challenge reply the malicious activities are detected. This reduces the routing through faulty nodes. The comparison shows efficiency among the normal, unsecure and proposed work secure protocols.

References

1. Alex Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)," International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.
2. Preeti Sachan and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011 DOI : 10.5121/ijnsa.2011.3518 229.
3. Jasvinder and Monika Sachdeva, "Effects of Black Hole Attack on an AODV Routing Protocol Through the Using Opnet Simulator," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, issue 8 ,August 2013.
4. Jaspal Kumar, M. Kulkarni and Daya Gupta , " Effect of BlackHole Attack on MANET Routing Protocols," I.J. Computer Network and Information Security , 2013, 5,64-72 Published Online April 2013 in MECS.
5. Rai ner B aumann, " Ad hoc On Demand Distance Vector Routing Protocol,"AODV, Presentation at ETH Zürich April 02.
6. Ms Darshana Patel and Ms Vandana Verma," Security Enhancement of AODV Protocol for Mobile Ad hoc Network," International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 1, January 2013.
7. Komal Joshi and Veena Lomte, "Preventing Flooding Attack in MANET Using Node-to-Node Authentication," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.
8. Onkar V. Chandure and Prof. V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET," Onkar V Chandure et al/(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011, 2607-2613..