Intrusion Detection System for AODV Protocol in MANET

Ms. S.R. Shirke
M.Tech.-II, Shivaji University,
Kolhapur, India,

Prof. (Dr.) V. R. Ghorpade
Principal, D.Y.Patil, COE&T,
Kolhapur, India,

Abstract

Mobile ad hoc network (MANET) is collection of wireless mobile nodes where the participating nodes communicate with each other without any pre-established infrastructures such as a centralized access point. They provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as Ad-hoc On-Demand Distance Vector (AODV). AODV protocol is vulnerable to different attacks such as black hole attack and gray hole attack. Therefore, Security is an important for this protocol to provide secure communication between mobile nodes. Encryption and Authentication are the existing intrusion prevention methods. These prevention techniques are used to prevent network from attacker, but it cannot defend against compromised nodes. To obtain an acceptable level of security, prevention method should be coupled with an intrusion detection mechanism as second line of defense.

In this paper, intrusion detection system is proposed to detect malicious nodes inside the network. Black hole attack and gray hole attack have been implemented. Network simulator 2(NS2) is used to conduct simulations and consider scenario for detecting attacks.

Keywords: MANET, AODV, Blackhole attack, Intrusion Detection System,NS2, Security.

1. Introduction

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance that are participating in the network. Nodes are mobile and they have limited resources. Each node acts as a host and a router at the same time. MANET is very useful in other applications such as emergency rescues and disaster recovery situations, where cellular infrastructures are non-existent. Ad-hoc networks have certain characteristics like high degree of mobility, absence of centralized administration, limited resources etc.

MANET nodes perform the routing functions themselves. Due to the limited wireless transmission range, the routing generally consists of multiple hops. Therefore, the nodes depend on one another to forward packets to the destinations. Routing in such networks is particularly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements.

2. Routing Protocols

An ad hoc routing protocol decides the way to route the packets between computing devices. Based on route discovery time, MANET routing protocols fall into three general categories.

2.1. Proactive (table-driven) routing protocols.

This type of protocols maintains fresh list of destinations and their routes by periodically distributing routing tables throughout the network. Example of proactive routing protocol is Destination Sequenced Distance Vector (DSDV).

2.2. Reactive (on-demand) routing protocols.

This type of protocols creates routes only when they are required by the source node. It finds a route on demand by broadcasting Route request packets. Examples of reactive routing protocols are the

dynamic source routing (DSR), ad hoc on-demand distance vector routing (AODV).

2.3. Hybrid routing protocols

This type of protocols combines the advantages of both the proactive and reactive routing protocols. This routing protocol include ZRP

3. Related work

ADOV is a standardized routing protocol designed for MANET [1].AODV is vulnerable to many different types of attacks [2] such as blackhole attack, gray hole attack. Many secure routing protocols have been proposed previously e.g. SAODV for AODV. Some protocol uses cryptographic schemes, such as encryption and authentication. In Secure AODV (SAODV) [3] secure routing protocol using asymmetric cryptography has been proposed, but key computation is too expensive. These preventive mechanisms cannot defend against all possible attacks. Therefore, intrusion detection is necessary as second line of defense.

Zhang and Lee [4], proposed one of the first approach for an integrated IDS architecture. It uses host-based IDSs based on anomaly detection and misuse detection. They introduce the concept of integrating multiple layers of the protocol stack for efficient intrusion detection.

S. Marti [5] proposed the watchdog mechanism to monitor the neighbor nodes and detect misbehavior.

F. Anjum ,S.Sarkar [6], proposed a signature based intrusion detection technique, in which they investigate the ability of different ad-hoc network routing protocols to facilitate detection of intrusions when the attack signatures are completely Known.

Payal N. Raj, Prashant B. Swadas[7] proposed DPRAODV .In this method , the sequence number is checked against the pre estimated threshold value. If sequence number is higher than the threshold value then it is considered as anomaly.

Satoshi Kurosawa, Hidehisa Nakayama , Nei Kato,Abbas Jamalipour, and Yoshiaki Nemoto [8]proposed an anomaly based intrusion detection method. It uses destination sequence number to detect attack. It uses dynamic training method in which the training data is updated at regular time intervals.

Vishnu K, and Amos J .Paul [9], Gray Hole attack is implemented and impact on the performance of network is studied.

4. AODV routing protocol

As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. When a route to the new destination is needed, the node uses *route request* (RREQ) messages; it flooded RREQ through the network in order to discover the paths required by a source node. An intermediate node that receives a RREQ replies to it using a *route reply* (RREP) message only if it has a route to the destination whose corresponding destination sequence number is greater or equal to the one contained in the RREQ. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination.

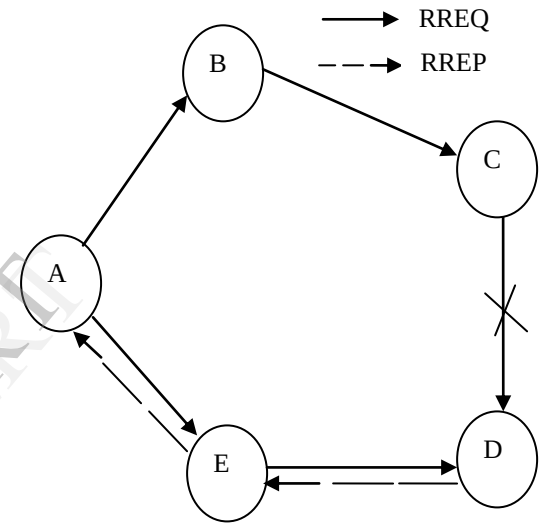

Figure.1 Working of AODV

Operation of the AODV protocol is given in Fig.1**.** Here, node A as the source which wants to communicate with node D, which is the destination. Node A creates and broadcast the RREQ messages to node B and E. Since node B and node E do not have a route to node D, they would again broadcast the RREQ control message to node C and node D, again Node C broadcast the RREQ messages to node D. If an RREQ message with the same RREQ ID is received, node discards the newly received RREQs. Here, Node D receives two RREQ messages, so the node D silently discards the newly received RREQs.

When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards the RREP message is unicasted to the source node. In figure.1, Node D unicast reply to Node A with its new sequence number.

5. Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then drop all the packets.

In Fig. 2, source node A wants to send data packets to a destination node D in the network. Source A initiates the route discovery process. Let Node M is a malicious node which acts as a black hole. The malicious node does not check its routing entries and immediately responds with an RREP message even if it may not have a valid route to the destination, In RREP message hop count value is set to lowest values and the sequence number is set to the highest value. The malicious node reply will be received by the requesting node before the reception of reply from actual node D. So, data communication initiates from A towards M instead of D.

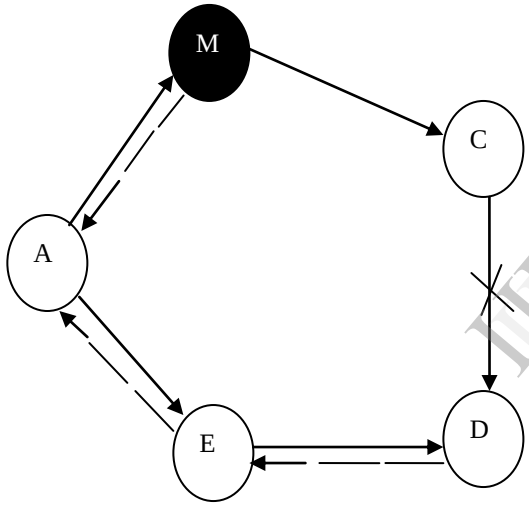

Figure 2. Working of Blackhole Attack

In this way node A will think that this is the active route and thus active route discovery is complete. Node A will ignore all other replies and will start sending data packets to node M. In this way the source chooses the path provided by the malicious node and the all data packets will be lost. The malicious node M forms a black hole in the network and this attack is called black hole attack.

6. Gray Hole Attack

In gray hole attack, attacker node can drop some selected packets according to some criteria or randomly. The difference of Black Hole Attack compared to Gray Hole Attack is that malicious nodes never send true control messages initially. In Fig. 2.M is malicious node, here if M is under gray hole attack then M node not forward all packets and drops some of the packets randomly.

7. Proposed approach

We implement both gray hole attack and black hole attack. The packet delivery ratio of the network is calculated in both scenarios .i.e. with and without the presence of malicious nodes. In malicious scenario packet delivery ratio is very less. An algorithm should be implemented to identify such malicious nodes.

Simulations results are in two format i.e. NAM and trace file. After simulation of both scenario, there are two trace results one for normal scenario and another for malicious scenario. After studying the trace results we propose a new detection algorithm that uses these two trace files to detect malicious node.

The algorithm is analyzes the data which is collected from both trace file. First trace file is for normal scenario, it is used to define legal behavior. In malicious scenario, some nodes are set as malicious, so in this trace file behavior of those malicious nodes is compared with legal behavior and it is found that this trace file contains specific behavior patterns of blackhole attack for malicious node. This behavior pattern is called signature of attack. This signature of attack is used to detect malicious node.

When user gives any scenario then its trace file is compared with previously created signature of attack. If this signature is matched with some nodes trace results of given scenario then it declares that those specific nodes are malicious.

In this work, main criteria for identification of a malicious node is the creation of signature of attack from malicious scenario, which is compared against a normal scenario, Node which drops packet according to signature is said to be misbehaving node, while remaining nodes are said to be properly behaving.

8. Performance metrics

The performance of the network is evaluated using following performance metrics:

8.1 Packet Delivery Ratio (PDR)

The packet delivery ratio is nothing but the ratio between the total numbers of packets send at the source to the total number of packets receives at the destination. To improve the performance of the network system the packet delivery ratio must be high as possible

8.2 Packet Drop Ratio (PDRR)

It is a measure of the number of packets dropped by the routers. Packet loss can be caused by channel congestion or normal routing. In addition to this, malicious node purposely drops the packet to perform attack.

8.3 Throughput

It is defined as total number of packets received by the destination. It is a measure of effectiveness of a routing protocol. A network throughput is the average rate at which message is successfully delivered between a receiver and its sender.

9. Simulation Environment

In order to analyze the performance of routing protocols in MANETs in the real world, a scenario based simulation analysis is needed since there is a lack of necessary infrastructure for their deployment. In this section, a set of experiments conducted to analyze the performance of the AODV routing protocol is described by using the scenarios for simulations. The results give an idea of how the protocol behaves in the given scenario and helps to identify the metrics for detection of malicious node.

Table 1. Simulation Parameter

Parameter	Value
Simulator	Ns-2(version 2.32)
Simulation time	500 (s)
Number of nodes	20
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)
Topology	750 x750 (m)
Pause Time	2 (s)
Packet Size	512
Number of malicious node	1,2,4,6.

Network scenario is set up a with 20 wireless nodes moving at random, the *pause time* values represent the movement of the objects. Each of the objects can move at a random direction, stop for some time (per the *pause time*), and then change its direction at random and move again. The number of data source and destination nodes is chosen randomly. In simulation, node positions and movements are randomly generated by using setdest utility. We use CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. The connection types are generated by using cbrgen utility. For simulation, Ns2 Network Simulator has been used. The simulation parameter is given in Table 1. .

10. Experimental results

Each scenario has two simulations. First we simulated the AODV with no attacker node and checked the packet delivery ratio. In the absence of attack the delivery ratio obtained is higher. Then we introduced a malicious node in the network and it drops the packet as shown in Fig. 3.

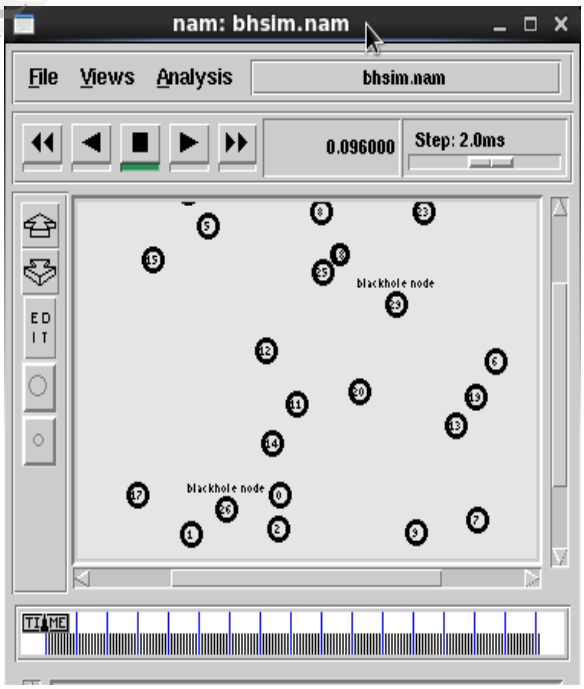

Figure. 3. Malicious scenario

The packet delivery ratio (PDR) is calculated in both simulation. Xgraph given in figure 4 compares the packet delivery ratios in both cases; with and without blackhole attack. The red line represents the PDR of basic AODV routing protocol, the green line represents the PDR of AODV under black hole

attack. Xgraph shows that when the malicious node is present in the network, it reduces the packet delivery to destination.

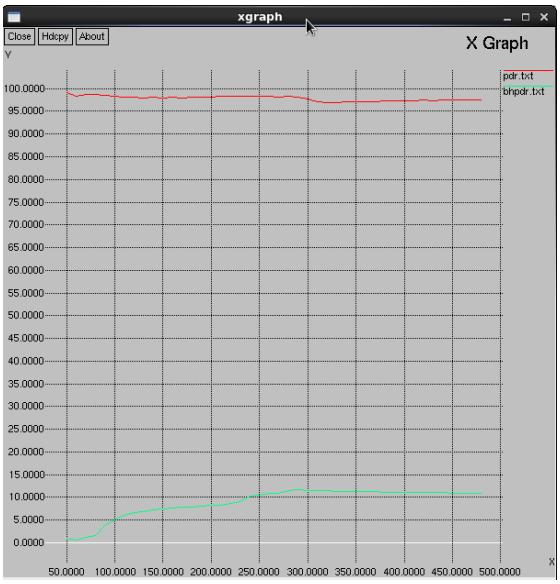

Figure 4.Packet delivery ratio

We get the simulation results from output trace file of the Tcl scripts, which has .tr extension. Trace files include all events in the simulation such as when the packets are sent, which node generated them, which node has received, which type of packet is sent, if it is dropped why it is dropped etc. In our simulations we use new trace file format that is especially used in wireless networks and includes detailed event information. To get the results from the trace files we needed some fields like event (send, receive, drop), trace level, reason of event. To identify the malicious node from the trace file we used AWK utility and cat commands.

An awk program is a sequence of patterns and corresponding actions. When input is read that matches a pattern, the action associated with that pattern is carried out. Input shall be interpreted as a sequence of records. For each pattern matched, the associated action shall be executed. Cat command writes the output into text file.

For creation of signature of attack awk command is used .Trace files fields like event (send, receive, drop), trace level, reason of event is given as input to create signature of attack. If event is packet drop and reason of packet loss is black hole then this pattern is matched with trace file result of given scenario. If both pattern matches then awk command takes action .This action gives list of nodes that drops the packet according to our attack signature. These nodes are called malicious nodes. Then number of packets drop by each malicious node is counted i.e. Drop count and this output is written in text file as shown in Table2.

In Table 2, it is shown that node number 26,27,28,29 are the malicious node and that drops the packets due to attack and it is the aim of proposed Intrusion Detection System.

Table 2. Malicious node

Malicious Node Number	Drop Count
26	1189
27	1057
28	1060
29	3297

11. Conclusion

AODV protocol in MANET is vulnerable to various kinds of attacks due to dynamic topology and lack of centralized access point. Security of AODV is most important issue. Black Hole attack and Gray Hole attack is simulated and it is observed that when the malicious node is present in the network, it reduces the packet delivery to destination.

In this paper, Attack signature is created by comparing normal scenario with malicious scenario. This signature is compared with given scenario to detect malicious nodes. Signature based Intrusion Detection System is used to detect the attacker node. The work can be extended by introducing some methods to secure AODV protocol from other types of attacks such as spoofing, wormhole attacks.

References

(1) E. Perkins, E. M. B. Royer, and S. R.Das, Ad hoc On-Demand Distance Vector AODV) routing, RFC 3561, July 2003

(2) Peng Ning, Kun Sun, "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Adhoc Routing Protocols," in Proceedings of the 4th Annual IEEE Information Assurance Workshop, pages 60-67, West Point, June 2003

(3) M. G. Zapata, Secure Ad Hoc on-demand Distance Vector (SAODV) Routing, IETF Internet Draft,draft-guerrero-manet-saodv-03,Mar. 2005

(4) Y. Zhang and W. Lee. “Intrusion Detection in Wireless Ad Hoc Networks". In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August, 2000

(5) S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265

(6) F.Anjum, D. S. bandhu and S.Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative Study of Various Routing Protocols", 2003.

(7) Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based.

(8) S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackhole attack on AODV based mobile ad-hoc networks by dynamic learning method, *"International Journal of Network Security*, pp. 338–346, 2007.

(9) Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

(10) J. Ros and P. M. Ruiz, Implementing a New Manet Unicast Routing Protocol in NS2", December,2004.

(11) ns-2 : http://www.isi.edu/nsnam/ns/