Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.338 – 345

RESEARCH ARTICLE

Mitigation of Blackhole for AODV (Ad hoc On Demand Distance Vector)

Ms. Bhumi Jani[1], Prof. Hitesh Patel[2]
[1]Information Technology & Gujarat Technology University, India
[2]Information Technology & Gujarat Technology University, India

[1] bhumimina@gmail.com; [2] hiteshldit@gmail.com

Abstract— A Mobile ad-hoc network is a temporary network set up by mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, mobile adhoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. There are lots of detection and defence mechanisms to eliminate the intruder that carry out the black hole attack. We simulated the black hole attack in various mobile ad-hoc network scenarios and have tried to find a response system in simulations.

Key Terms: - MANET; AODV; SAODV; IDS; SAODVABH

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without any fix common infrastructure in place like wireless access point or radio based station. MANET has dynamic topology where devices or nodes in the network can change their position or disappear from the network rapidly. One of the challenges faced by nodes in a MANET is limited resources such as battery lifetime and also the security of its routing protocol. Since MANET is formed in an ad hoc manner, cooperation amongst the nodes to establish the network path is needed. The network for nodes which are not within communication range will be established through a multi-hop link which requires every node to act as a router as well as a normal host. In router mode the node has to discover the route and deliver the data with the help of the routing protocol. In this paper we focus on Ad hoc On demand Distance Vector (AODV) protocol [1] which is one of the reactive ad hoc routing protocols in MANET. AODV has capability to adapt smoothly in a dynamic network environment like MANET because of its low control message overhead. However, it has a drawback i.e. the protocol was designed without any security consideration hence making it vulnerable to security attacks [2]. The condition becomes more serious as MANET uses ether to propagate the message and on the same time the communication channel is always open to various attacks. Black hole is one of many attacks that take place in MANET and it is one of the most common attacks made against the AODV routing protocol.

The black hole attack will disrupt the network and affect the whole network performance. The malicious node in a black hole will pretend to have the shortest and freshest route to the destination node by manipulating the control message to attract other nodes to send their data through its node. AODV works base on destination sequence number and hop count attribute to determine the freshness and shortest path of the route. However these two attributes are not sufficient to reduce the effect of black hole attack in the network. The existing

method of routing update in AODV gives opportunity for attackers to manipulate these attributes. By manipulating those attributes. The attacker can deny Route Reply (RREP) messages from benign nodes to update the routing table.

In our review of previous works, most methods added new control message to the existing protocol scheme to overcome this problem. This approach is considered costly because it introduces overhead to the AODV process during the route discovery phase. Due to that, we devise a new method called SAODVABH (Secure AODV Against Black Hole) which has less overhead in the mitigation process to overcome the effect of the black hole attacks. It works without changing the existing protocol scheme. This method improves the routing update process as well as analysing the receive reply control messages (RREP) to isolate black hole malicious nodes. This method assumes the destination node is reachable by route request and normal black hole characteristic is high destination sequence number carried in route reply. This paper is organized as follows. Section II provides an overview of the AODV route discovery process and a description of a black hole attack. Section III discusses about related works. Section IV presents the SAODVABH, a proposed method to mitigate the black hole attack. Section V discusses about simulation result and lastly, plans for the future work is concluded in Section VI.

II. AODV ROUTING PROTOCOL

AODV is a reactive routing protocol; that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, the nodes do not have to discover and maintain a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes [1]. AODV has borrowed the concept of destination sequence number from DSDV, to maintain the most recent routing information between nodes.

Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. Each neighboring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbours after increasing the hop count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup [3].

The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. If the intermediate node has a route entry for the desired destination, it determines whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQs sequence number for the destination is greater than the recorded by the intermediate node. Instead, the intermediate node rebroadcasts the RREQ packet. If a node receives more than one RREPs, it updates its routing information and propagates the RREP only if RREP contains either a greater destination sequence number than the previous RREP, or same destination sequence number with a smaller hop count. It restrains all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then later updates its routing information of better route to the destination node. Each route table entry contains the following information:

- Destination node
- Next hop
- number of hops
- Destination sequence number
- Active neighbors for the route
- Expiration timer for the route table entry

The route discovery process is reinitiated to establish a new route to the destination node, if the source node moves in an active session. As the link is broken and node receives a notification and Route Error (RERR) control packet is being sent to all the nodes that use this broken link for further communication. And then, the source node restarts the discovery process. As the routing protocols typically assume that all nodes are cooperative in the coordination process, malicious attackers can easily disrupt network operations by violating protocol specification. This paper discusses about blackhole attack and provides routing security in AODV by purging the threat of blackhole attacks.

III. RELATED WORKS

Piyush [4] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the

network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

Chen [5] presented a solution consisting of two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. According to their solution, each node involved in a session must create a proof that it has received the message; when source node suspects some misbehaviour, Checkup algorithm checks intermediate nodes and according to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm. This solution may generate high traffic and computational cost of detection algorithm may be very high due to the basic limitations of gossip protocol and aggregate signatures.

A mechanism is proposed by Sukla [6] in which before sending any block, source sends a prelude message to destination to make it aware about communication; neighbours monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of acceptable range, the process of detecting and removing all malicious nodes is initiated by collecting response from monitoring nodes and the network. The mechanism has routing overhead increased due to additional routing packets.

For detecting packet forwarding misbehaviour, Oscar [7] proposed an algorithm that uses the principle of flow conservation and accusation of nodes that are constantly misbehaving. Selecting correct threshold of misbehaviour allows distinguishing well-behaved and misbehaved nodes. However, the average throughput cannot reach that of a network where there is no misbehaving node present because the algorithm requires definite time to gather the required data to identify and to accuse misbehaving nodes. Therefore, misbehaving nodes can drop packets before being accused and isolated from the network during the preliminary phase.

A trust-based approach is proposed by Arshad [8] that uses passive acknowledgement as it is simplest; it uses promiscuous mode to observe the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for. Thus, a node can make sure those packets it has sent to the neighboring node for forwarding are indeed forwarded. Routing choices are made based on two parameters: trust and hop-count; therefore, the selected next hop gives the shortest trusted path. Though, monitoring overall traffic would have been a better choice instead of monitoring one nodes request.

Ming-Yang [9] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate nodes are prohibited to reply to RREQs, if an intermediate node is not the destination and never broadcasts RREQ for a specific route, but forward a RREP for the route, then its suspicious value will be increased in the nearby nodes suspicious node table. When the suspicious value of a node goes beyond threshold, a Block message is broadcasted by the node to all other nodes in the network to isolate the suspicious node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

An approach is discussed by Latha [10] in which the requesting node waits for a specific time for replies from neighbours that include the next hop details. After the specific time, Collect Route Reply Table is verified to know whether there is any repeated next-hop-node or not. Existence of repeated next-hop-node in the reply paths indicates the truthful paths or limited chance of malicious paths. Though, the process of finding repeated next hop node increases overhead.

Payal [11] suggested a protocol DPRAODV that finds a threshold value and compares that with difference of sequence number of reply packet and that of route table entry. If it is higher than the threshold value, the node sending reply is added to a list of blacklisted nodes. Also an ALARM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. The protocol has higher routing overhead due to addition of the ALARM packets.

An algorithm is proposed by Deng [12] in which when a source node receives a route reply packet, it cross checks with the previous node on the route to the destination to verify that the node sending reply packet indeed has a route to the destination as well as to the intermediate node. If it does not have, the node that sent the reply packet is judged as malicious node. The mechanism, though, increases endtoend delay and due to the addition of FurtherRequest and FurtherReply packets in the algorithm, routing overhead also gets increased.

IV. **SAODVABH: THE PROPOSED MITIGATION METHOD**

The SAODVABH is designed to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep table to store incoming RREP packet parameter mali list to keep the detected malicious nodes identity and parameter rt upd to control the process of updating the routing table. The pseudo code of modified recvReply() function is shown in Listing 1.

Unlike the conventional AODV protocol, SAODVABH will secure the routing update by imposing an additional condition controlled by parameter rt upd. This parameter only receives either true or false value. By

default, the value is set to true which means the routing table is allowed to be updated regardless of what value the existing two conditions have e.g. the destination sequence number in the RREP message is less than the one in the routing table.

Explanations on how the SAODVABH works is described as follow, When route request (RREQ) message is sent out by the source node S to find a fresh route to the destination node D, all nodes that have fresh enough route information will response to the request including the destination node D. RREP messages received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M. Since the value of parameter rt_upd is true, node S accepts the next RREP messages from node A to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. As a result, the current route entry in routing table will be overwritten by the later RREP coming from node A. SAODVABH method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. Based on possibility of later RREP is came from the actual destination node D, the rt upd parameter value is then set to false when reply from destination node is received. Any RREP message that comes after when rt upd is false will be ignored until the process of detecting malicious node complete

Listing 1. SAODVABH : Proposed Algorithm

```
RecvReply(Packet P) {
Save P.src | P and P.dst_seqno to
rrep_tab
if(rt_upd = false) {
Detect malicious node and save in
mali_list
Flush rrep_tab
Set rt_upd to true
}
if(P.dst no entry in Routing Table RT) {
Add entry of P.dst to RT
}
Select dst_seqno from RT
if(rt_upd= true) or (P.dst_seqno
>RT.dst_seqno or P.dst_seqno =
RT.dst_seqno and P.hopes <RT.hops) {
if (P is from request destination node)
Set rt_upd to false
Update RT entry with P
Send data packets to the
route in RT
} else if (routing is UP for P) {
Forward packet P
else discards P
}
...
}
```

V. SIMULATION AND RESULT

A. Simulation Environment

For simulation, we have used Ns 2.34 network simulator. Mobility scenarios are generated by using a Random waypoint model by varying 50 to 150 nodes moving in a terrain area of 1000m x 1000m. Each node independently repeats this behaviour and mobility is varied by making each node stationary for a period of pause time. The simulation parameters are summarized in Table I.

A new Routing Agent is added in ns-2 to include the blackhole attack. In order to implement blackhole attack, the malicious node generates a random number between 1 and 5, adds the number to the sequence number in RREQ and then generates the sequence number in RREP. In our simulation, the communication is started between source nodes to the destination node in presence of the malicious node. The node number of source node, destination node and malicious node are 3, 4 and 1 respectively.

B. Simulation Evaluation Methodology

The simulation is done to analyze the performance of the networks various parameters. The metrics used to evaluate the performance are given below:

Table 1
NETWORK SCENARIO USING AODV

Simulation Parameters	Values
NS Version	Stable Release 2.34
Interface Queue Type	Queue/DropTail/PriQueue
Interface Queue Length	50 packets/interface queue
Prapogation Model	Propagation/TwoRayGround
Topology	1000m X 1000m
No of nodes	50
Traffic Type	UDP
Data Type	CBR
Data Packet Size	512 bytes
Scenario	Random Motion models generated using ”setdest”
Simulation	Time 25sec
Node speed	50 m/s
No of sources	3
No of Destinations	4

- Packet Delivery Ratio: The ratio of the data delivered to the destination to the data sent out by the source.
- Average End-to-end delay: The difference in the time it takes for a sent packet to reach the destination. It includes all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc.
- Throughput: No. of Packets send by network v/s No. Of packets generated by source.

C. Simulation Analysis and Results

Various network contexts are considered to measure the performance of a protocol. These contexts are created by varying the following parameters in the simulation.

- Network size: variation in the number of mobile nodes.
- Traffic load: variation in the number of sources
- Mobility: variation in the maximum speed

D. Simulation of SAODVABH

1. *Throughput of SAODVABH:* Figure 1, shows the throughput of SAODVABH. From the graph we can say that with the intruder we can get good throughput. It is nearer to AODV Throughput.
2. *Delay of SAODVABH:* From the graph shown in Figure 2, delay of network is very less, and we met the result of AODV.
3. *Load of SAODVABH:* Graph shown in Figure 3, shows the total load of system, in terms of All Generated Packets, All Sent Packets, All received Packets, All Forwarded Packets and Also All Dropped Packets per Second.

E. Results

To check for various results I applied different Perl, awk scripts and Trace Graph 2.02 Utitlities for various results like for calculating throughputs, packet delivery ratio, End2End Simulation Delay and load etc.

By applying different scripts to measure normalized routing load, throughput, packet delivery ratio and different parameters like number of sent and received packet on trace file for AODV without and with intruder and DSR algorithm for 50 nodes. I get following results.

By summarizing this result for 50 nodes with AODV without intruder, DSR, AODV with intruder and SAODVABH it is shown Table II

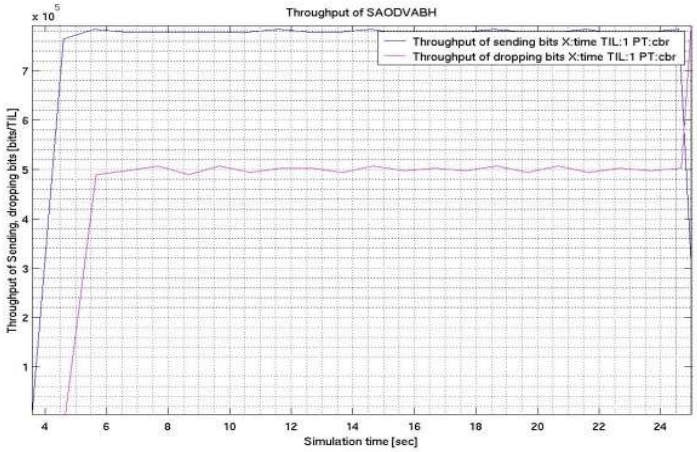

Fig. 1 Throughput of SAODVABH

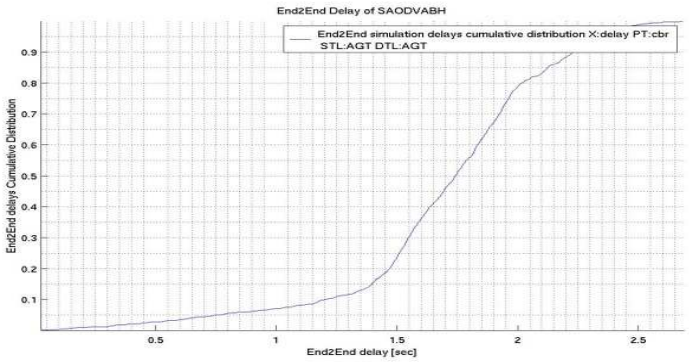

Fig. 2 Delay of SAODVABH

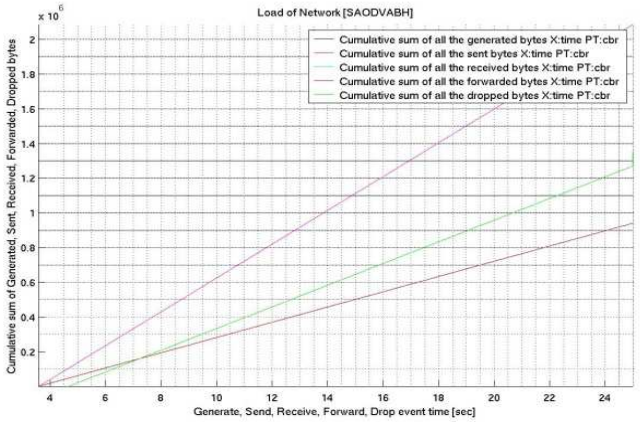

Fig. 3 Load of SAODVABH

Table 2
Result with parameters

Parameters	AODV without intruder	DSR	AODV with intruder	SAODVABH
Average Throughput	336.56	330.48	68.46	336.49
Data Sent	4302	4302	4302	4302
Data Receive	1766	1734	79	1764
Packet Delievery Ratio	41.05	40.31	1.84	41.00
Average End2End Delay	1.699 s	1.733 s	1.242 s	1.703

VI. CONCLUSION AND FUTURE WORKS

In SAODVABH, we have used a very simple and effective way of providing security in AODV against blackhole attack. As from the graphs as well as simulation results we illustrated in results we can easily infer that the performance of the normal AODV drops under the presence of blackhole attack. Our prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending signal to its neighbors. Our solution: SAODVABH increases PDR with minimum increase in Average-End-to-end Delay and normalized Routing Overhead.

There are some drawbacks which should be improved and some of them are given below:

- Find out and block an authenticated user, which start miss behaving inside the network.
- Scalability still remains largely unexplored.
- Energy consumption.
- Lacks of effective analytical tools especially in case of large scale wireless network setting.
- Computation complexity

REFERENCES

[1] E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, ser. WMCSA '99. Washington, DC, USA: IEEE Computer Society, 1999, pp. 90–. [Online]. Available: http://dl.acm.org/citation.cfm?id=520551.837511

[2] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," Wirel. Netw., vol. 11, no. 1-2, pp. 21–38, Jan. 2005. [Online]. Available: http://dx.doi.org/10.1007/s11276-004-4744-y

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Internet Engineering Task Force, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[4] P. Agrawal, R. K. Ghosh, and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks," in Proceedings of the 2nd international conference on Ubiquitous information management and communication, ser. ICUIMC '08. New York, NY, USA: ACM, 2008, pp. 310–314. [Online]. Available: http://doi.acm.org/10.1145/1352793.1352859

[5] C. Wei, L. Xiang, B. Yuebin, and G. Xiaopeng, "A new solution for resisting gray hole attack in mobile ad-hoc networks," in Communications and Networking in China, 2007. CHINACOM '07. Second International Conference on, 2007, pp. 366–370.

[6] H. P. Singh, V. P. Singh, and R. Singh, "Article: Cooperative blackhole/grayhole attack detection and prevention in mobile ad hoc network: A review," International Journal of Computer Applications, vol. 64, no. 3, pp. 16–22, February 2013, published by Foundation of Computer Science, New York, USA.

[7] S. S. G.S. Mamatha, "A robust approach to detect and prevent network layer attacks in manets," International Journal of Computer Science and Security (IJCSS), vol. 4, pp. 275–284, July 2010.

[8] A. Jhumka, N. Griffiths, A. Dawson, and R. Myers, "An outlook on the impact of trust models on routing in mobile ad hoc networks (manets) 1."

[9] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems." 2011, pp. 107–117.

[10] L. Tamilselvan and D. V. Sankaranarayanan, "Prevention of blackhole attack in manet," 2007.

[11] P. N. Raj and P. B. Swadas, "Dpraodv: A dynamic learning system against black hole attack in aodv based manet," International Journal of Computer Science, vol. 2, pp. 54–59, February 2010.
[12] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol. 40, no. 10, pp. 70–75, 2002.

