J. Modern Technology & Engineering
Vol.2, No.1, 2017, pp.66-75

A HYBRID METHOD FOR DETECTION AND REMOVAL BLACK HOLE ATTACKS IN MOBILE AD-HOC NETWORKS

Shahram Behzad[1*], Fatholla Dadgar[2]

[1]Department of Computer Engineering, Germi Branch Islamic Azad University
Germi, Iran
[2]Baku State University, Baku, Azerbaijan

Abstract. A wireless ad hoc networks (MANETs) consists of a group of mobile nodes which are connected by wireless links. The peculiar characteristics of MANET like open medium, high dynamic. It operates without the use of existing infrastructure. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. A particular type of attack called 'Black Hole' attack compromises the security of the AODV protocol. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. In this paper, a hybrid approach is proposed to detect black hole nodes in the wireless ad-hoc networks. The proposed method find out the safe route between sending node and receiving node by hybrid method. The simulations show that the proposed approach is efficient than original AODV when the black hole attack is present with high packet delivery and less packet drop.

Keywords: *component, wireless ad-hoc network, black hole attack, AODV, detection, routing.*

Corresponding Author: *Shahram Behzad, Department of Computer Engineering, Germi Branch Islamic Azad University, Germi, Iran, e-mail: sh.behzad173@gmail.com*

Manuscript received: *7 December 2016*

1. Introduction

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantage is their limited bandwidth, memory, processing capabilities and open medium [1]. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad Hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-Hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile [2] nodes. Routing is the heart of the network. The main goal of the routing protocol is to establish and maintain the route thus avoiding stale routes and delay due to link breaks and failures. The attacks in mobile ad hoc networks are classified into two types. They are active attacks and passive attacks. Mobile ad-hoc networks are highly vulnerable to active attacks. These include modification of data, deleting the content, dropping the packets, replication of the data. Some of the attacks that can be easily performed over mobile ad-hoc

networks are black hole attack, wormhole attack, rushing attack, spoofing, routing table overflow. Among the above-mentioned attacks, black hole attack shows great impact on the performance of the network. The following problems may occur in the AODV protocol. The misbehaving nodes may perform harmful operations by not following the protocol. Figure (1) shows that a black hole attacks wireless Ad-Hoc network.

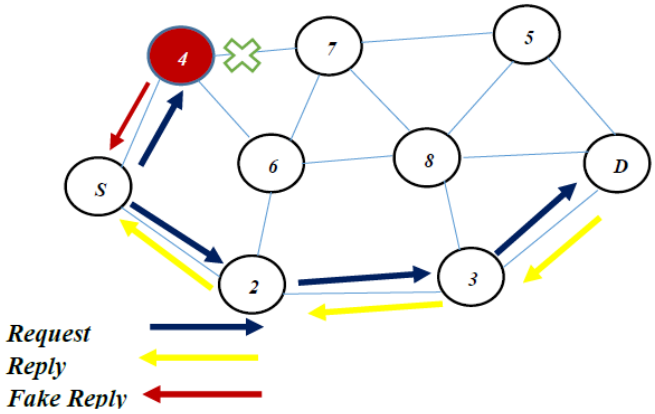

Fig 1. An example of black hole attacks in *wireless Ad-hoc Network*

So, this type of attack should be detected and removed from the network efficiently thereby establishing safe routes. The black hole attacks show great impact on the on demand distance vector routing protocol (AODV). This paper aims to detect black hole attacks in AODV routing protocol.

The paper is structured as follows. Section 2 routing protocol in AODV is considered, in section 3 the Related Works is analysed, in Section 4 the method is proposed. In section 5 simulation and analysis are given. Finally, concluding remarks are given in section 6.

2. Description of AODV (Routing Protocol)

The Ad-Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [3, 4]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination

Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in Fig. 2. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks.

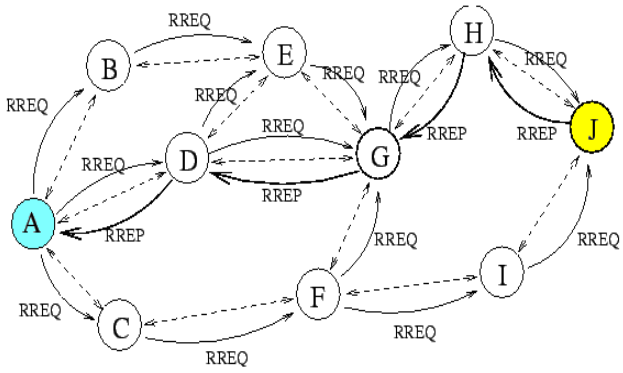

Fig 2. Propagation of RREQ & RREP from A to J.

3. Related work

In this section, we presented a survey of some of the approaches to solve the problem of routing misbehavior in ad hoc networks.

B. Han, and M. Shin [4] proposed a method that requires intermediate nodes to launch path confirmation request to its next hop node to target node. The next hop node verifies its cache for target node. When the next hop node has a route to the target node, it launches route confirmation reply to source node. The source node judges the path in RREP by matching it with the path in RREP route confirmation reply. This operation is carried along with the routing protocol. This increases the routing overhead, which results in performance degradation of MANET, which is a bandwidth, constrained.

The SECTOR protocol [5] presents a countermeasure against wormhole attacks by allowing nodes to prove their encounters with other nodes. However, several hypotheses are needed for this protocol to work correctly. Among these are the necessity for coarse synchronization, the ability of nodes to measure their local

timing with nanosecond precision, the pre-establishment of security associations between each pair of nodes, and the presence of a central authority that controls the network membership. So-called disjoint-path-based approaches have been adopted recently. In [7] a statistical approach based on multipath routing is proposed. This approach uses the relative frequency of each link when discovering routes within the network. The main idea beneath this approach resides in the fact that the relative frequency of a link, which is part of a wormhole tunnel, is much higher than other normal links.

[8] proposed a solution to defending against the cooperative black hole attacks. But in, no simulations or performance evaluations have been done. Ramaswamy et al. [9] studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black hole nodes. In this paper, we evaluate the performance of the proposed scheme in defending against the collaborative black hole attack. In [10] is proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further.

Lu et al [11] proposed a system SAODV for black hole attack. It also address some security weakness of AODV. Deswal and Singh proposed a system that is advance form of SAODV. It uses password for each routing nodes and routing tables. In [10] proposed a algorithm to identify multiple black hole nodes. It introduces data routing information table. This table maintain the entry of each node. It is first to gives the solution of cooperative black hole attack.

Sharma et al [11] solution is the selection of the secure route by the source that is based on the shared hopes among the paths. In the proposed solution, if there is no such path then source will have to send the RREQ message again till the route having shared hopes is not identified. In this solution, no communication can be performed till source finds this path for communication. This solution has a problem of delay.

Tamilselvan et al [12] proposed solution of wait and check strategy for preventing multiple malicious nodes. The authors proposed that source chooses a secure path by repeated next hope node using “wait and check” strategy after collecting route reply (RREPs) message from neighbor nodes. Source node assumes route to be safe and secure if it finds any repeated nodes in the receiving replies. If source does not find any repeated node, it chooses a path randomly for data packets transmission. The wait strategy causes additional processing delay and receiving replies from different nodes create additional delay.

4. Proposed method

AODV routing protocol follows the basic, When RREQ process is sent, the node waits for RREP and once the RREPs come from the nodes, it responses to the

first arrived RREP. The node sends packets with this RREP, which in turn leads to ignoring other REEPs. Such a process leads to ignoring the security or in security of the route, which in turn enhance the chance of malicious nodes (black hole nodes) existence eliminating the transmitted packets. In this paper, a hybrid approach is proposed to detect black hole nodes in the wireless ad-hoc networks. Method based on table and hop count, once a large number of RREPs are received in a successive period from a node, the packets are not transmitted with this RREP. Rather, information of the given node is recorded in a table and, to evaluate the immunity of the route, the hop counts transmitted by RREP are analyzed. Black hole attacks eliminated from operation cycle.

The proposed method follows which is if a specific node at a particular time path the response message comes too much threshold, (5 times the response threshold more than path have considered). These nodes stored the information in Table 1 suspect paths and we are awaiting a reply from the other nodes. if this node again too much threshold to path messages we saw we received and the lowest step is The node identified as the black hole node and information nodes to all neighbors to broadcast. But if is a node that does not reply for any request, path and number of hop count are a good to the destination node, Information along with step number is stored in Table Reply safe paths to and use from the this route as a safe path. In fact, we have two separate tables, one for other is suspect nodes for node intact from these two tables, paths suspicious malicious node are separated from the safe path.

Table 1. Reply malicious node

Reply path	Reply repetition	Time
RREP (1)	8	2 Second
RREP (2)	7	1 Second
RREP (3)	9	3 Second
RREP (4)	10	2 Second

Table 2. Reply Safe nodes

Reply path	Reply repetition	Hop count
RREP (1)	1	5
RREP (2)	3	7
RREP (3)	2	4
RREP (4)	1	3

After the table Replies obtained. Based on this table, we chose the best route in terms of being safe. And packets from the route to the destination the desired node will be selected. As shown in Fig. 3

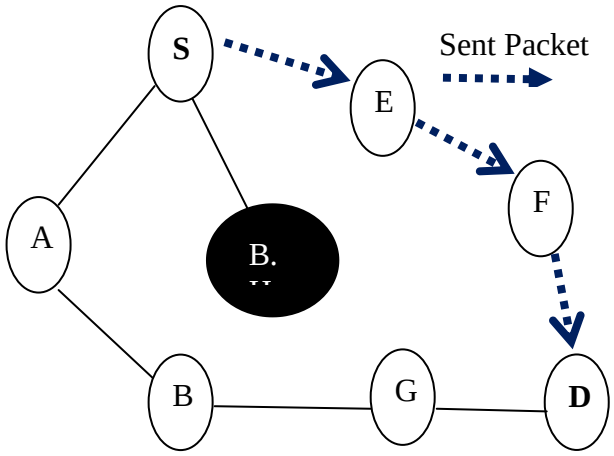

Fig 3. Sent data packets

5. The simulation parameters

This section includes simulation and evaluation of Accurate Black hole attack. we used a wireless network with 802.11 standards, which is a 500 * 500 - simulation environment. According to, we employed 802.11 protocols for the network layer, with node transmission range of 250m, link bandwidth of 11 Mpbs, package size of 512 bytes and simulation time of 200s. We evaluated the DSR efficiency by storing (keeping) the network pace; stop time and size change (the number of mobile nodes 50). Table 3. shows a summary of the parameters that have been used in this simulation.

Table 3. Simulation parametrs

Parameter	**Value**
Simulation	Ns-2.34
Simulation Time	100,120,140,160
Number Of Node	60
Routing Protocol	DSR
Mac Layer Protocol	IEEE 802.11
Traffic Model	CBR

Transmission Range	250M
Area	500 m *500 m
Packet Size	512 Byte
Packet rate	2 packets / sec
Number of Blak hole Node	10 Node

A. Packet delivery ratio(%)

The ratio of the feedback packets delivered to the destinations to individuals generated through CBR sources. It specifies the packet loss rate, which limits the ideal throughput for the network. This usually occurs from a router becoming compromised from a number of different causes. Because packets are routinely dropped from a network

$$PDR = \frac{Packet\ Recived}{Total\ Packet\ transmitted} * 100, \quad (1)$$

where PDR is the package delivery rate, Total Packet transmitted is the number of sent packages, and Packet Received denotes the number of received packages.

B. Packet droop

In wireless mobile Ad-Hoc network , a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. Because packets are routinely dropped from a lossy network.

C. Throughput

It measures the total rate of data sent over the network, including the rate of data sent from cluster head to the sink and the rate of data sent from the nodes to their cluster head

$$T = \frac{\sum_{i=1}^{n} T_i^r}{\sum_{i=1}^{n} T_i^s} * 100, \quad (2)$$

where T_i is the average receiving throughput for the i^{th} application, T_i s is the average sending throughput for the i^{th} application, and n is the number of applications.

Fig.4 shows attackers different time 100 to 160 against packet droop rate. Packet droop rate of the proposed method and AODV under attack less. When the number of attacks, the packet droop rate in proposed method and AODV under attack much more. But the changes in the proposed method is less.

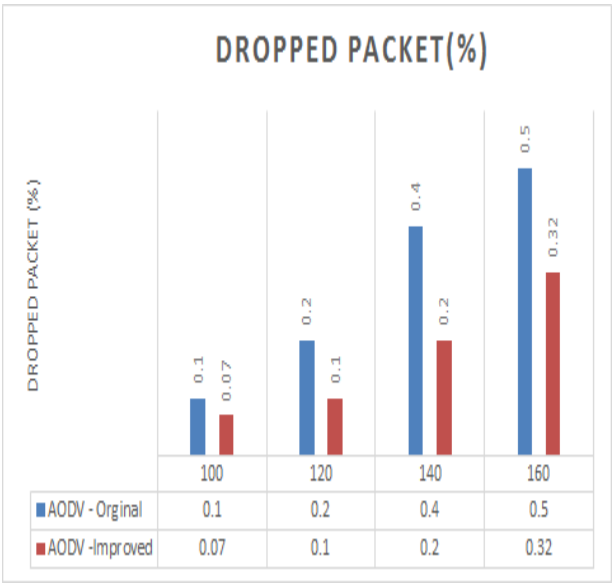

Fig 4. Packet Droop Vs Time

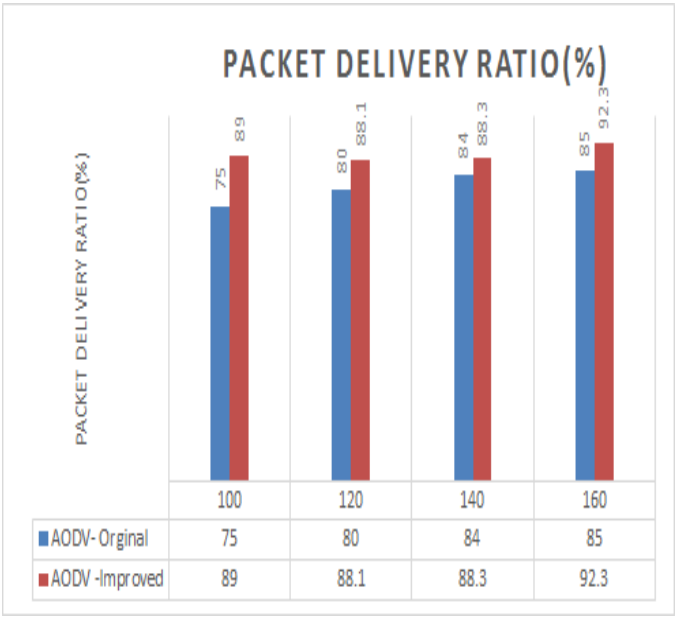

Fig 5. Packet delivery ratio Vs Time

Fig. 5 shows the packet delivery ratio of proposed method at the different time Than the AODVunder attack is better, the package delivery rate at the time of 150 to 300 , is better .When the number of attacks is higher, the packet delivery dsr rate is much lower than proposed method. But the changes in the proposed method is better.

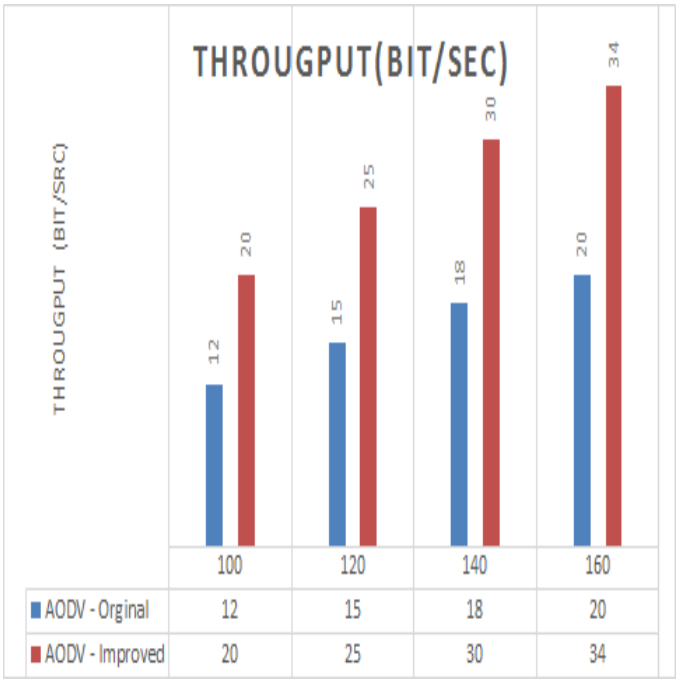

Fig 6. Throughput Vs Time

Fig. 6 show that the For 100 to 140 time, it is obvious that the throughput for Propose method is high compared to that of AODV under attack. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. The overall low throughput of AODV under attack is due to route reply. The black hole node immediately sends its RREP and the data is sent to the black hole node which cast off all the data. The network throughput is much lower.

3. Conclusion

In this paper, we studied the issue of black hole attacks in MANET routing. In addition, proposed a feasible solution for it on the improvement AODV protocol to avoid the black hole attack, and prevented the network form further malicious behavior. In this paper, we proposed an improvement DSR based secure routing protocol, named AODV (improvement AODV). The improvement AODV discover and removed and defense architecture in MANETs by using the hybrid method (RREP Time and hop count) and, Neighborhood Information test. Proposed method of Association original AODV protocol increases the routing security and encourages the nodes to cooperate in the ad-hoc structure. It identifies the black hole nodes and isolates them from the active data forwarding and routing. To be able to indicate the efficiency of proposed method using the NS-2 simulator, the proposed system is compared with (AODV under attack). The outcome of the simulation in packet delivery rate, packet drop rate and throughput indicated that the proposed method provides a better result when comparing to the (AODV under attack) method.

References

1. Capkun S., Buttyan L., Hubaux J.-P., (2003) SECTOR: Secure Tracking of Node Encounters in Multihop Wireless Networks, Proc. ACM Wksp., Sec. of Ad-Hoc and Sensor Networks, Fairfax, VA, Oct.
2. Deshmukh S.R., Chatur P.N., (2016) Secure routing to avoid black hole affected routes in MANET, Colossal Data Analysis and Networking (CDAN), Symposium on. IEEE, 1-4.
3. Dhama S., Sharma S., Saini M., (2016) Black hole attack detection and prevention mechanism for mobile ad-hoc networks, Computing for Sustainable Global Development (INDIACom), 2016, 3rd International Conference on IEEE, 2993-2996.
4. Lee S., Han B., Shin M., (2002) Robust routing in wireless ad hoc networks, In: ICPP Workshops, p. 73.
5. Lee S-J., Gerla M., (2000) AODV-BR: Backup routing in Ad-Hoc networks, Wireless Communications and Networking Conference, *WCNC*, 2000, IEEE, 3.
6. Lu S., Li L., Lam K-Y, Jia L., (2009) SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack, Proc. of Intl. Conference on Computational Intelligence and Security, Beijing, China, 421-425.
7. Perkins C, Belding-Royer E., S. Das, (2003) Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561.
8. Qian L., Song N., Li X., (2005) Detecting and locating wormhole attacks in wireless Ad-Hoc networks through statistical analysis of multi-path, *Proc. IEEE WCNC*, New Orleans, LA, Mar.
9. Ramaswamy S., Fu H., Nygard K.E., (2005) Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks, International Conference on Wireless Networks, Las Vegas, Nevada.
10. Ramaswamy S., Fu H., Sreekantaradhya M., Dixon J., Nygard K., (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, 2003 International Conference on Wireless Networks, Las Vegas, Nevada, USA.
11. Sharma N., Sharma A., (2012) The Black-hole node attack in MANET, Second International Conference on Advanced Computing & Communication Technologies, 546-550.
12. Tamilselvan L., Sankaranarayanan V., (2007) Prevention of Black Hole Attack in MANET, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Aug 27-30, p.21.