Asian Journal of Information Technology 12 (9): 291-296, 2013
ISSN: 1682-3915

A Novel Technique to Analyze and Detect Black Hole Attacks in MANET

G. Usha and S. Bose
Department of DCSE, Anna University, 600025 Chennai, India

Abstract: Mobile ad hoc networks are self configuring, dynamic networks. Because of its dynamism any nodes can join and leave the network at any time. So, these networks are easily attacked when the communication takes place. In this study, first researchers analyzed the behaviour of the attack by using AODV protocol. Researchers used ns-2 to evaluate the proposed mechanism. First, researchers analyzed the network with various network attributes. Second, we detect the attack by using new fast algorithm. The technique is fast because researchers use only single packet to detect the attackers. Third, we compared the research with existing AODV algorithm. The simulation results show that there is significant improvement of the proposed technique in packet delivery ratio rather than existing AODV protocol.

Key words: Ad hoc networks, black hole attacks, Ad hoc On demand Distance Vector protocol (AODV), attackers, network

INTRODUCTION

Mobile Ad hoc Networks (MANET) are self configuring, self deployable and dynamic in nature. There is no centralized infrastructure for MANET. So, each node acts as a router where it receives and forwards packet by itself. The restriction of these networks is one user is able to send/receive message to other user only if both are in particular transmission range. But unlike cellular or wired networks MANET does not require any base station or centralized router. MANET's can be used in various applications such as tsunami, earthquake and military communications and so on. Mobile adhoc networks are more advantageous to portability and mobility but are vulnerable to various types of security attacks.

Though, MANET's have lot of advantages, they suffer for various security problems. Improving MANET security is still a research issue. Because, MANETs suffer for various kinds of attacks. For example, MANET's MAC layer (Yang *et al*., 2004) suffer for jamming attacks, network layer suffers (Burbank *et al*., 2006) for black hole attack, gray hole attack, worm hole attack and so on. Because of its infrastructure, less network MANETs are highly vulnerable. So, providing security to MANET is challenging issue because routing protocols are violated by intruders. Routing protocols (Zhou and Haas, 1999) in MANET are classified as unicast routing protocols, multicast routing protocols, secure routing protocols, network layer routing protocols. Routing protocols play the challenging task such that it should correctly deliver routing messages from source to destination. Every protocol has its own different technique to deliver messages from source to destination. For example, AODV and DSR are existing on-demand routing protocols. But these protocols do not offer any security solution for the communication process. Generally the packet delivery mechanism in MANET is achieved through two operations-routing packets and forwarding packets. So, malicious activity is achieved in both the operations.

In this study, first researchers analyze how a malicious node exploits AODV protocol and yields attacks in routing and forwarding packets. Second, we propose a fast algorithm to detect black hole attacks. Packet delivery ratio increases in the proposed approach. Routing packets is also increased from source to destination. Network overhead is also reduced. The performance of the method is compared with normal AODV. We have evaluated the algorithm with various network attributes and various node densities. We conduct network simulations in network simulator (ns-2) (Issariyakul and Hossain, 2009) to evaluate and understand the proposed algorithm.

LITERATURE REVIEW

Recently many researchers proposed solutions to detect black hole attacks in MANET. Some of the researchers proposed new protocols while the others provide the methods to secure already existing ones.

Corresponding Author: G. Usha, Department of DCSE, Anna University, 600025 Chennai, India

There are various secure routing protocols such as Secure Ad hoc On-demand Distance Vector routing (SAODV) (Lu *et al*., 2009).

Al-Shurman *et al.* (2004) propose two different types of solution to defend against black hole attack. The first method works in redundant route identification technique. In this approach, the researcher assumed that there is more than one path available for a source node to transfer packets. The source node recognizes the safe route by considering the number of hops or nodes which avoids routing through black hole attacks. In the second solution by using the sequence number they identified the attacks. This approach contains additionally two tables which maintain the details about the last packet sequence number and last packet received. By using this information the sender node identifies the malicious node. Tamilselvan and Sankaranarayanan (2007) propose the detection technique by using a timer which is in timer expired table. It collects the request from all the nodes and stores the sequence number which is named as Collect Route Reply Table (CRRT). Based on the time out value it judges the route. Because of timer setting the communication delay increases in the network.

Jaisankar *et al.* (2010) propose a security technique consist of two parts: detection part and reaction part. In detection part each node maintains a Black Identification Table (BIT) which stores information like source id, destination id, Packet Modified Count (PMC), Packet Received Count (PRC), Packet Forwarded Count (PFC). By using the PMC, the BIT table is updated for black hole nodes. The next part is reaction part where the nodes are isolated by maintaining isolation table. The isolation table also stores the ID's of black hole nodes which are broadcasted to all other nodes in the network. A delay is introduced in the network. Mistry *et al.* (2010) propose detection technique maintains additionally three fields. They are Cmg-RREP-Tab, a timer MOS-WAIT-TIME and a Mali-node. The Cmg-RREP-Tab maintains the details about the received RREP's from receiving neighbors. MOS-WAIT-TIME is the timer where the source node waits for RREP packets from neighbors. The node which has highest sequence number is marked as malicious and stored in Malicious node. This field is maintained in order to identify the malicious node in future.

Su (2011) propose a security scheme which involves anti black hole mechanism for each node in the network. This technique additionally uses two tables which are RQ table and SN table. In the RQ table it records the details about the RREQ messages within the transmission range of the communication area. The SN table records the suspicious value of each node. The suspicious value is calculated by counting the number of forwarded RREQ messages by each node. If a node is not transmitting RREQ packets for a particular threshold value it is marked as malicious node. All the approaches presented above to detect black hole attack uses only single layer information. Not, only that each technique presented above has its own pros and cons. These solutions introduce additional overhead by introducing new tables and fields. But the proposed approach uses cross layer information. Even though, researchers are using cross layer parameters the network overhead is greatly reduced. We discuss the few cross layer work carried in literature which inspired us to propose the solution. Only little research has been carried out in literature which uses cross layer information against attacks in MANET.

Thamilarasu and Sridhar (2012) propose a cross layer based solution to detect jamming attacks in MANET. They used MAC layer as well as routing layer parameters to detect attacks. In their technique the output from the detection modules is combined with decision module. They used a rule based system to detect attacks in the network. Joseph *et al.* (2008) propose an architecture known as CARDS. It uses an SVM procedure to reduce the data. This technique uses an apriori procedure to reduce the data set. They also used Fischer discriminant procedure to classify attacks from the MANET. The researchers used cross layer information to classify attacks. The cross layer correlation technique is implemented in their research. They have correlated MAC layer features with the network layer. Even though, researchers are using cross layer parameters the network overhead is greatly reduced.

IMPACT OF BLACK HOLE ATTACKS

Analyzing black hole attacks: In order to understand the behavior of AODV protocol first, researchers modified the existing AODV protocol. The malicious black hole behavior in AODV is introduced in following functions:

- AODV:: recv (Packet *p, Handler*)
- AODV:: recv (Packet *p, Handler*)

In ns-2, the function "AODV:: recv" is called for each and every packet arriving to that routing agent. So, in this function, a routing agent can maliciously drop a packet by using this function. The function "AODV::

recvRequest" is called during receiving an AODV route request packet type "AODVTYPE_RREQ". On receiving this route request message from any neighboring nodes, the routing agent tries to resolve the route and send a route reply message if a route is available. So, it call the function "AODV:: send Reply" with appropriate parameters. Hence, an agent tries to send a fake reply for the purpose of attacking a neighboring node by giving wrong routing information; it calls "AODV:: send Reply" and passes wrong routing information to the requesting node. In the implementation, researchers have used a modified function "AODV:: sendFakeReply" for the purpose of sending wrong information to simulate black hole attacks. The following function discusses about the implementation of black hole attack in MANET.

```
Function to implement black hole attack
If (AODV_Packet) {
If (RREQ) {
If (it is a packet which I am originating) {
Handle it in Normal way
} else {
//it is the packet I am forwarding
If {No Attack} {
Handle it in Normal way
} else if (BlackHoleAttack) {
//Maliciously dropping the packet
  Drop the packet
}
}
}
```

TECHNIQUE TO DETECT BLACK HOLE ATTACKS

The proposed detection scheme includes the concept of generating dummy RREQ packet. Researchers are using dummy RREQ packet because the packets does not contain any data field. It contains only header part. In RREQ header the dummy packets has non existing IP address. When the routing process starts between source node and destination node, initially in the routing process before generating normal RREQ packets, researchers first propagate dummy RREQ packets. Whenever a node replies for this packet, researchers mark that node is black hole node. This is because as mentioned before the dummy RREQ packets contains only non existence IP address. Hence, the nodes which are particularly intended to drop packets answers this packets. In this manner, we can detect the malicious nodes in the network. Figure 1 shows the dummy RREQ packets used in the technique to detect malicious packets. Researchers have modified the existing AODV protocol in order to detect the black hole attacks. The following function generates dummy RREQ packets in route request packets.

Fields	Description
F1	Other fields in RREQ packets ---------- ----------
DST	Nonexistence destination IP address
TTL	1

Fig. 1: Dummy RREQ packets

```
Function to generate dummyRouteRequest
Begin
aodv_rt_entry *rt;
//Create a non existing IP address
NEAddress←NonExistingNodeID;
rt←rtable.rt_lookup (NEAddress);
if (rt ==0) {
rt←rtable.rt_add (NEAddress);
}
SendFakeRequest (NEAddress);
End
```

PERFORMANCE EVALUATION

In this study, researchers evaluate the efficiency of the proposed system against various network attributes. First, we analyze the impact of black hole attacks in MANET. For that researchers used the trace as Constant Bit Rate (CBR). Each node transmits 512 byte of data packets at certain rate (packets/sec). The transport agent researchers used was UDP. For each set of parameters, researchers have repeated the simulation for 3 times and calculated the average of the results. For the simulation of normal AODV with 5 different numbers of network sizes and for three repetitions, researchers run the simulation for 15 times.

So, for 5 different numbers of network size with black hole attack and 4 different numbers of nodes (malicious), the black hole simulation was run for 40 times. And it was repeated for 3 times and makes it as 120 runs. So, the results were then prepared from the output of 135 simulation runs.

Researchers have used different network scenarios (20, 30, 40, 50 and 60 nodes). The scenario generator available in ns-2 which is used for generating 5×3 scenarios (for three repetitions).

Next, researchers discuss about simulation results and analysis method. The following Table 1-3 illustrate MANET's simulation environment. Now the following Table 4 displays the analyzing of black hole attacks in

Table 1: Manet environment

Property	Values
Channel type drop	Wireless channel
Propagation model	Two ray ground
Antenna type	Omni antenna
Interface queue type	Drop Tail/PriQueue
Maximum packets in queue	50
MAC type	802.11 MAC layer
Topological area	600×600 m
Mobility scenario	10 m sec^{-1}
Pause time	20 sec
Mobility Model	Random way point

Table 2: Traffic parameters

Property	Values
Traffic agent	CBR
Transport agent	UDP
Traffic source	7
Traffic sink	7
CBR rate	10 k bytes sec^{-1}

Table 3: Variable parameters

Property	Values
Routing protocol	Normal AODV, AODV with black hole
Number of black holes	1, 2, 3 and 4
Number of nodes	20, 30, 40, 50 and 60

various node densities. The following displays analysis of the black hole under various types of attributes in MANET. The following table displays the solution of AODV attack without proposed detection technique.

Both Table 5 and 6, we compare that the packet drop ratio reduced for the proposed solution. The routing packets is increased for the proposed solution. Packet delivery ratio is increased and normalized routing load is decreased throughout the network. Researchers discuss about the analysis of the network in front of various node densities.

Packet delivery ratio:

- Packet delivery ratio decreases with increasing node densities and percentage of black hole nodes. Figure 2 discusses the packet delivery ratio under various node densities
- In the case of black hole AODV with 10% of malicious nodes, the packet delivery ratio decreases from 97.60 (0% malicious nodes) to 67.73, (10% malicious) when the nodes are moving with the mobility of 10 m sec^{-1}
- With 40% of malicious nodes, the packet delivery ratio has the fall from 97.60-39.17%
- Researchers observes that when the black hole nodes are increased the packet delivery ratio gets decreased

Normalized routing load

Normalized routing load for black hole attack: Normalized routing load can be evaluated based on

Table 4: Variable parameters

Protocols	Nodes	PDF	NRL	Routing packets	Dropped
With black hole 1	20	67.73	0.45	493.33	590
	30	54.13	1.12	938.00	796
	40	67.53	0.91	1003.67	588
	50	65.03	1.18	1323.00	603
	60	79.23	1.75	2355.33	413
With black hole 2	20	44.13	0.72	430.00	983
	30	35.17	1.17	652.00	1125
	40	53.83	1.03	893.67	821
	50	57.87	1.30	1097.00	707
	60	54.00	2.23	1724.33	820
With black hole 3	20	26.87	1.01	445.67	1271
	30	19.93	1.79	596.67	1381
	40	39.50	1.61	731.67	1057
	50	27.07	2.24	839.00	1246
	60	48.60	1.69	1304.67	897
With black hole 4	20	22.53	110.70	350.67	1350
	30	11.73	6.03	563.00	1523
	40	20.13	5.33	764.00	1387
	50	17.00	3.30	933.33	1413
	60	39.17	2.26	1338.67	1052

Table 5: With black hole attack

Black holes	PDF	NRL	EED	Routing packets	Dropped
1	67.73	0.45	68.24	493.33	590
2	44.13	0.72	49.17	430.00	983
3	26.87	1.01	42.34	445.67	1271
4	22.53	110.79	37.71	350.67	1350

Table 6: Without black hole attack and with proposed detection technique

Black holes	PDF	NRL	EED	Routing packets	Dropped
1	89.03	0.48	52.37	721.00	229
2	73.37	0.53	42.52	631.67	470
3	61.30	0.53	38.86	505.33	683
4	48.87	0.62	32.03	481.33	895

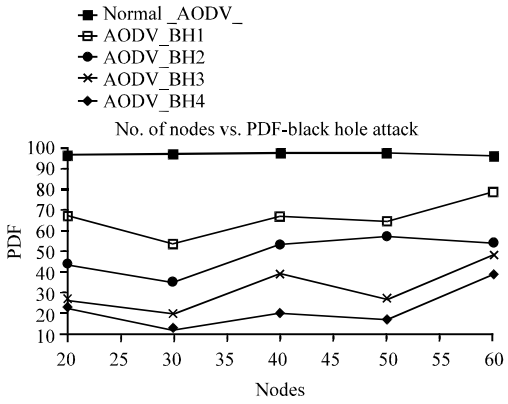

Fig. 2: Analyzing packet delivery ratio with black hole nodes

messages like RREQ and RREP with the statistics of number of routed packets to that of received packets. Figure 3 explains about normalized routing load in the presence and absence of malicious nodes. From the results, the following observations can be drawn:

- No constant trend is observed in normalized routing load

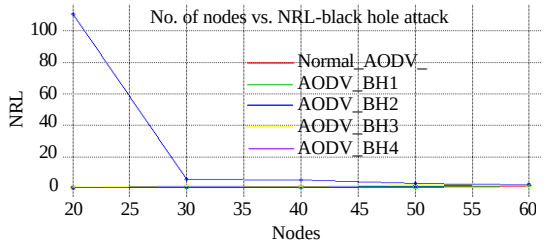

Fig. 3: Analyzing normalized routing load with black hole nodes

- In the case of black hole AODV, the normalized routing load shows an increase
- With 10% of malicious nodes the normalized routing load increases from 0.38-1.75, likewise with 40% of malicious nodes, the normalized routing load shows the increase from 0.38-2.26

Researchers also observe that when the black hole nodes are increased the normalized routing load also increased.

Dropped packets

Dropped packets for black hole attack: This metric not identifies other reasons for packet loss but it is useful towards detecting packet drop attacks. From the results in Fig. 4 the following observations can be drawn:

- Packet drop count increases with increasing node densities and percentage of black hole nodes
- In the case of black hole AODV with 10% of malicious nodes, the packet drop count increases from 73 (0% malicious nodes) to 413 (10% malicious) when the nodes are moving with the mobility of 10 m sec^{-1}
- With 40% of malicious nodes, the packet drop count has the steepest fall from 73-1052
- We observe that when the black hole nodes are increased the packet drop count gets increased

Overhead

Overhead for black hole attacks: Overhead is the useful metric for analyzing extra bandwidth consumed to deliver data packets. From the results in Fig. 5 the following observations can be drawn:

- Overhead increases with increasing node densities and percentage of black hole nodes
- In the case of black hole AODV with 20% of malicious nodes, the overhead increases

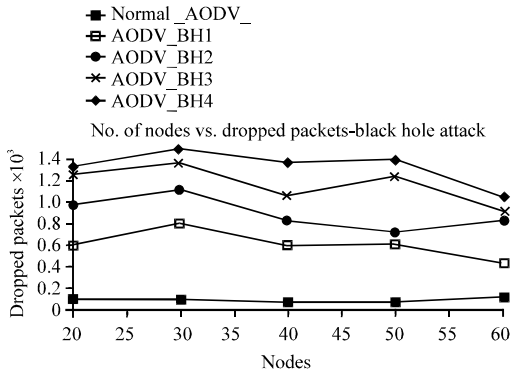

Fig. 4: Analyzing dropped packets with black hole nodes

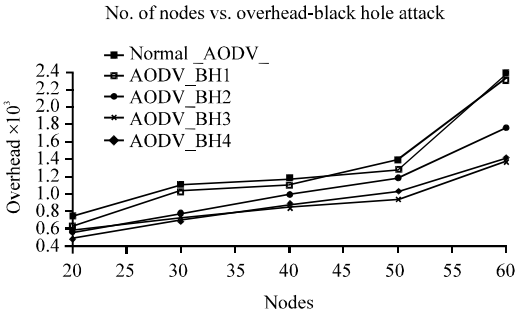

Fig. 5: Analyzing overhead with black hole nodes

- With 40% of malicious nodes, the overhead increases from 2399.00-1338.67
- Researchers observe that when the black hole nodes are increased the overhead gets increased

Figure 2-4 explain the effectiveness of the proposed solution. The proposed new technique considerably improves the PDF as shown in Fig. 6. Researchers have compared in both the cases with detection and without detection.

The performance in terms of dropped packet is increased with the increase of number of black holes in both cases. But after detection the dropped packet count is decreasing considerably. It means, the proposed method successfully detects black holes in the network and avoids forwarding packets through them. Figure 7 explains the packet drop ratio for the proposed scheme. Researchers have measured the overhead as the count of total generated and forwarded routing messages. With detection, the overall change in overhead is minimum. It means, the extra messages used for black hole detection is very minimum and not consuming much network resources. Figure 8 discusses about the overhead caused by black hole nodes with and without detection.

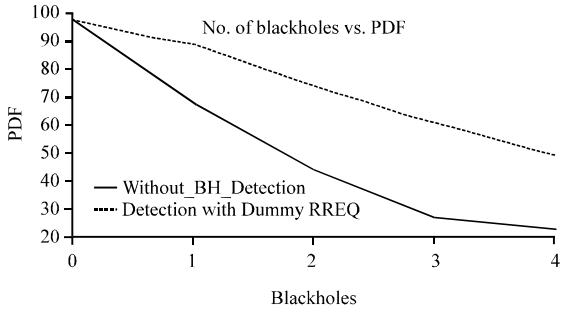

Fig. 6: Packet delivery ratio for with detection and without detection

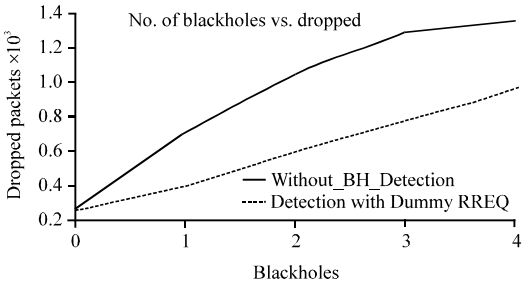

Fig. 7: Packets drop for with detection and without detection

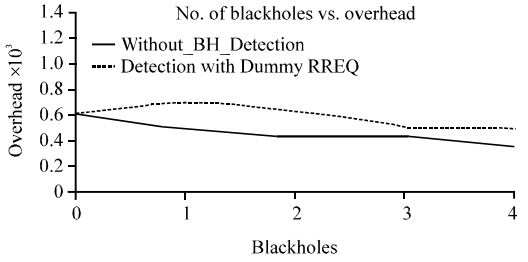

Fig. 8: Packets drop for with detection and without detection

CONCLUSION

In this study, researchers have successfully analyzed and detected black hole attacks in MANET. Researchers have implemented modified AODV which implements the concept of dummy RREQ packets. The proposed detection scheme is compared with normal AODV without any attacks. Packet delivery ratio increased in the proposed scheme. Packet drop ratio also decreased considerably. The detection process is called periodically and the routing table is updated dynamically accordingly. The proposed detection algorithm uses only a single spoofed RREQ message to detect the presence of black holes in the MANET environment. So, overhead also greatly reduced in the network packet delivery ratio improved and packet drop ratio reduced.

REFERENCES

Al-Shurman, M., S.M. Yoo and S. Park, 2004. Black hole attack in mobile Ad Hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, April 2-3, 2004, Huntsville, AL. USA., pp: 96-97.

Burbank, J.L., P.F. Chimento, B.K. Haberman and W.T. Kasch, 2006. Key challenges of military tactical networking and the elusive promise of MANET technology. IEEE Commun. Mag., 44: 39-45.

Issariyakul, T. and E. Hossain, 2009. Introduction to Network Simulator NS2. Springer, New York, USA., ISBN-13: 9780387717593, Pages: 435.

Jaisankar, N., R. Saravanan and K.D. Swamy, 2010. A novel security approach for detecting black hole attack in MANET. Proceedings of the International Conference on Recent Trends in Business Administration and Information Processing, March 26-27, 2010, Thiruvananthapuram, India, pp: 217-223.

Joseph, J.F.C., A. Das, B.C. Seet and B.S. Lee, 2008. CRADS: Integrated cross layer approach for detecting routing attacks in MANETs. Proceedings of the IEEE Wireless Communications and Networking Conference, March 31-April 3, 2008, Las Vegas, NV., USA., pp: 1525-1530.

Lu, S., L. Li, K.Y. Lam and L. Jia, 2009. SAODV: A MANET routing protocol that can withstand black hole attack. Proceedings of the International Conference on Computational Intelligence and Security, Volume 2, December 11-14, 2009, Beijing, China, pp: 421-425.

Mistry, N., D.C. Jinwala and M. Zaveri, 2010. Improving AODV protocol against black hole attacks. Proceedings of the International MultiConference of Engineers and Computer Scientists, Volume 2, March 17-19, 2010, Hong Kong, pp: 1-6.

Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems Comp. Communi., 34: 107-117.

Tamilselvan, L. and V. Sankaranarayanan, 2007. Prevention of blackhole attack in MANET. Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, August 27-30, 2007, Sydney, Australia, pp: 21.

Thamilarasu, G. and R. Sridhar, 2012. A cross-layer game for energy-efficient Jamming detection in ad hoc networks. Secur. Commun. Networks, 5: 364-373.

Yang, H., H. Luo, F. Ye, S. Lu and L. Zhang, 2004. Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Commun., 11: 38-47.

Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. IEEE Network, 13: 24-30.