International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Enhancing AODV Routing Protocol to Eliminate Black Hole Attack in MANET

Ei Ei Khin
Faculty of Information and Communication Technology
University of Technology (Yatanarpon Cyber City)
Pyin Oo Lwin, Myanmar

Thandar Phyu
Department of Advanced Science and Technology
Ministry of Science and Technology
Nay Pyi Taw, Myanmar

ABSTRACT
MANET is an open wireless system that includes several mobile nodes to form an arbitrary and temporary network. As the lack of infrastructure network, the mobile nodes send the routing packets to each other in the network when they want to communicate. So, the nodes use the routing protocols. However, as the lack of security mechanism of the routing protocols, MANETs are facing various severe attacks. Black hole attack is such types of attacks and can carry great damage to the network. As a result, an efficient and simple routing algorithm for MANET is very important. This paper presented a simple approach to find and eliminate the black hole attack for MANET. The proposed system slightly modifies ad hoc on-demand distance vector (AODV) routing protocol by adding two tables and packet type alarm. The proposed mechanism removes the malicious node and chooses the reliable node by using these tables. When the malicious node is detected, the proposed system is automatically sending out the alarm packets to all nodes in the network.

Keywords
MANET, AODV, Black Hole, Two Tables, Alarm.

1. INTRODUCTION
MANETs are the wireless network that consists of dynamic mobile nodes. The mobile nodes may be personal digital assistance (PDA), laptop, mobile phone and any devices that are mobile. The mobile device or node can easily join and leave to the network and can design dynamic topologies for the network based on their connectivity. They have the ability to configure themselves without needing any infrastructure. When the nodes want to communicate with each other via a wireless channel, they give the

connectivity by sending the packets among themselves. So, these nodes may be router or host or both at the same time.

MANET have the basic characteristics such as open medium, self-organization, dynamic mobile nodes and topology, limited resources, lack of infrastructure network and lack of defense mechanisms. Because of these factors, MANET often suffers from various security attacks [2]. Moreover, the mobile nodes in the MANET communicate with one another based on the mutual trust. The mobile nodes exist during the range of wireless channel may be overhear and participate to the network. The wireless channel causes MANET more prone to various attacks.

So, the security of transmission and communication in MANET is a challenge and important issue. To get secure communication and transmission in networks, the attacks type and their impacts on the MANET is understanding. There are different types of attacks to harm MANET. They are wormhole attack, selfish node misbehaving attack, routing table overflow attack, flooding attack, black hole attack, sybil attack, impersonation attack, denial of service (DoS) attack and so forth.

In the black hole operation, the intruder node sends the false reply with high sequence number. When it is received the data packets, it discards all. So, it disturbs the network and makes great damage to this network. In this paper, the defense mechanism is presented to identify and remove this attack and the feasible solution is proposed to get a reliable route to the destination. The rest of this paper is arranged such as: Section 2 describes an overview of black hole attack and AODV routing protocol. Section 3 reviews some researches about defense mechanism. Section 4 presents the proposed detection and prevention mechanism. The simulation results are described in section 5. Then, section 6 makes a conclusion about this paper.

2. BACKGROUND STUDY

2.1 Overview of AODV Routing Protocol

AODV is widely used routing protocol for MANETs [7, 9]. It is an extension of destination sequenced distance vector routing protocol[8] and it gives dynamic link conditions, low network utilization, low control message overhead, low memory overhead, and so on. There are two processes in AODV routing protocol. They are route discovery and route maintenance processes.

In the AODV protocol, when the nodes need to communicate with each other to send the data packets, firstly a node find an already route in its routing table. If it is an active or fresh route to the destination, the source node uses this route. If it has no route or it is not fresh route, the source node starts the route discovery process. So, it sends Route Request (RREQ)

packet to all neighbors and the neighbor nodes send back Route Reply (RREP) packet if it's the destination itself or it has a fresh route. Otherwise, they forward the RREQ message. When the source node is received RREP, it can communicate with the destination vice versa.

In the route maintenance process, whenever there is a link failure or link broken down during the operation, the Route Error (RERR) packet is sent to the nodes in an active link. The Hello message is periodically sent for maintaining the route information. Although AODV is a well known reactive routing protocol for MANET, there is no security mechanism against the types of attack [1]. Thus, the malicious nodes makes the AODV protocol is defenseless various types of attacks.

2.2 Black Hole Attack

It is one type of DoS attacks and active attack [10] in MANET. In the black hole attack [11, 12], the malicious node declares to the nodes that it is the best route to the destination with false route reply message. It is always used the highest sequence number value and the lowest hop count value. However, when it is received the data packets, it discards all packets.

For example, the following scenario in Figure 1 is considered. In this figure, it is assumed that 'S', 'D' and 'M' are the source, the destination and the malicious node respectively. When 'S' wants to communicate with 'D', it first sends Route Request packet to all neighbor nodes. Thus, 'F', 'E' and 'M' receive it. As 'M' is a black hole, it immediately sends back a Route Reply packet with high sequence number. When 'S' receives Route Reply packet from 'M', it is assumed this route is fresh enough route. Then, it communicates with the destination through this way. However, 'M' does not forward any data packet anywhere and discards all them.

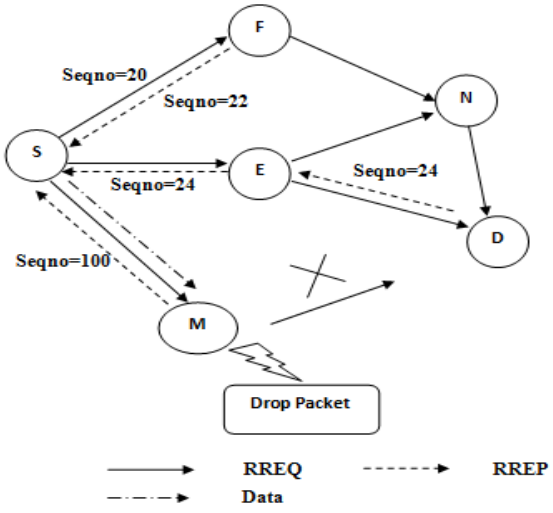

Figure 1. AODV protocol with black hole attack

3. RELATED WORKS

There are various defense mechanisms in the literature to protect black hole attacks. Some of the research papers are reviewed in this regard.

Mohammad Abu Obaida et al. [3] has presented lots of modules such as Threshold Tester, Packet Classifier, RREP sequence number Tester, Extractor, Alarm Broadcaster and Blacklist Tester. This mechanism modifies the format of Route Reply packet and uses a new packet type Alarm. The router calculates the range of the accepted sequence numbers and gives the threshold value. When any node is exceeding the threshold values for many times, this node is identified as attacker. But, the calculation of the threshold value is bit overwhelming. So, it has the network delay. Although the calculation of correct threshold prevent black hole node, the wrong calculation may disgrace an authentic node as a black hole.

Himral, Vig and Chand [5] have defined a mechanism to eliminate the malicious nodes in the MANET and to discover the reliable paths to the intended node by checking the sequence number difference between the source and intermediate node. In AODV protocol, the destination sequence number is very important. It is 32-bit integer value and is used to determine the fresh enough route or not. The larger destination sequence number, the better the route. So, in this paper, the proposed system is assumed that the malicious node sends the first RREP packet with high sequence number to the source node. Then, the source node stores it as the first RREP in the table and compares it with its sequence number. If there is very different, the node is surely the attacker and eliminates this entry from table. However, the proposed method cannot find multiple black hole nodes.

Nital Mistry et al. [4] modifies the original AODV routing protocol by using a new field Mali_node, a MOS_WAIT_TIME timer and a Cmg_RREP_Tab table. The time period that the source node waits for the Route Replies is defined as RREP_WAIT_TIME. The half of RREP_WAIT_TIME is defined as MOS_WAIT_TIME. Route Reply packets are kept in the Cmg_RREP_Tab table and Mali_node is stored the ID of attacker node. The source node analyzes and discards Route Replies with very high sequence number from the Cmg_RREP_Tab table. The experimental results demonstrate that this method has a good packet delivery ratio than the original AODV protocol. However, it has high processing delay and the end-to-end delay is increasing.

Jalil, Ahmad and Manan [6] have proposed an ERDA mechanism that modifies the existing route discovery mechanism recvReply() function of AODV routing protocol. The new elements are mali_list to store the ID of malicious nodes, rrep_table to keep RREP packets from other nodes and

rt_upd to do the update operation of routing table. The source node stores RREP packets in the rrep_tab table and then updates its routing table with first Route Reply of the malicious node from the rrep_tab table. However, the source node updated again the routing table with the next Route Reply packet from other node although it has a lower sequence number because the value of rt_upd is true. If the value rt_upd is false, the source node stops the update operation of routing table. The source node set the value of rt_upd as false when it receives Route Reply from the destination. ERDA mechanism removes the false Route Reply entry by replacing the later entry. However, it has high processing delay.

4. IMPLEMENTATION OF DETECTION AND PREVENTION MECHANISM

In this module, the detection and prevention algorithm for black hole attack on the context of AODV protocol (MAODV) is implemented to isolate the black hole nodes and to discover a safe route from source to destination in MANET.

3.1 Route Reply Record Table and Malicious Node Table

The proposed system modifies the procedure of source node by introducing two tables and alarm packet into existing AODV protocol. These tables are Route Reply (RREP) Record Table (RRT) and Malicious Node Table (MNT). The RRT table stores all RREP packets from the neighbor's node and the MNT table stores the information of malicious node. The examples of these two tables are shown in Table 1 and Table 2. The RRT table is stored only by the source node and the MNT table is stored by all nodes in MANET to eliminate the black hole node.

Table 1. Route reply (RREP) record table (RRT)

Time	Dest Node ID	Dest Node Seqno	Next Hop	Hop Count	Reply Source Address	Lifeti-me	Timesta-mp
5.203	C	100	M	1	M	9	20.4855
5.247	C	12	E	2	A	10	20.4855
5.301	C	10	D	3	B	9	20.4855
5.302	C	11	G	1	H	9	20.4855

Table 2. Malicious node table (MNT)

Node ID	Time
P	5.0143
M	10.6542
T	50.4968

3.2 Threshold Value Calculation

It is the value of averaging the difference between the destination sequence numbers from RRT table and routing table in each time interval (t) for destination. This value is used for detecting and removing the attacker node in the network. β is control parameter and variable. The value of β is different from the number of node, the number of connection, the network area, the mobility speed and the pause time. β is used to avoid the authentic node disgrace to be a malicious node.

$$Threshold = \frac{\sum(RREP_{Seqno\ t} - RT_{Seqno\ t})}{Total\ Number\ of\ Packets} + \beta$$

3.3 Extension to Routing Table

The proposed system has implemented to yield a strong method for detecting and preventing black hole attack. For the design of our scheme, the routing table field of AODV protocol is modified as follows. The reply initiator filed is added to the routing table and is used to store the ID of node that the route reply sends initially. When the malicious node is detected comparing with the threshold value, we can find the malicious node ID by seeing this field. So, the fields of the routing table of our proposed protocol are below:

- Destination IP Address
- Destination Sequence Number
- Hop Count
- Next Hop
- Network Interface
- Valid Destination Sequence Number flag
- Other state and routing flags
- Lifetime
- List of Precursors
- **Reply Initiator (extended field)**

3.4 Alarm Packet

In the original AODV protocol, it uses four different types of packets to communicate with each other. They are:

- Route Request (RREQ) Packet
- Route Reply (RREP) Packet
- Route Error (RERR) Packet and
- HELLO Packet Format.

RREQ packet and RREP packet are used for route discovery process to discover a route to the destination. RERR packet is used for route maintenance process in order to notify earlier nodes down the path of such a breakage when a link failure occurs. The HELLO packet is used to maintain the connectivity of the neighbor nodes.

In the proposed system, the ALARM packet is added to the packet types of AODV protocol. The ALARM packet is used to notify all neighboring nodes in the network about the black hole node and the format of ALARM packet type is shown in Table 3.

Table 3. ALARM packet format

Type	Reserved	Hop Count
Broadcast ID		
Malicious Node IP Address		
Originator IP Address		

3.5 Detection and Prevention Algorithm

The following terms are used to express the proposed algorithm.

- SN - Source Node
- IN - Intermediate Node
- MN - Malicious Node
- RT - Routing Table in AODV
- Seqno - Destination Sequence Number
- RREQ - Route Request Packet
- RREP - Route Reply Packet
- MNT - Malicious Node Table
- RRT - RREP Record Table

The proposed detection and prevention algorithm are as follows:

Begin

1. SN broadcasts RREQ to neighbors.

2. Store RREPs into RRT when SN receives RREP from IN until the waiting time.

3. Retrieve the Seqno from RRT and calculate the Threshold value.

4. Detect and remove the malicious node from RRT.

```
while ( RRT is not NULL)
    if (( rep_seqno – rt_seqno) > Threshold ), then
        assume IN is MN
        remove entry from RRT and store this IN as MN to MNT
        send Alarm message
    end
end
```

5. Select the reliable packet from the rest packets and continue the normal operation of AODV protocol.

6. Flush the RRT after completing step 4-5.

End

3.6 Working Principle of the Proposed System

When the source node needs to communicate with the destination to send the data packets, it sends RREQ packet to all neighbors. In original AODV protocol, the source node accepts the first fresh RREP form the neighbor node. Thus, the malicious node always sends the route reply with high destination sequence number ahead of other neighbor node to the source node. As compared, in this paper, the source node keeps all RREP from neighbor nodes in RRT until the waiting time. The waiting time is a timer that the source node waits other RREPs after getting the first RREP. We used 0.1 second as the value of waiting time.

Then, the source node retrieve the destination sequence number from RRT table and routing table and calculate Threshold value using the above equation. To detect the malicious node, we calculate the difference of sequence number from routing table and RRT. If the value of the difference is greater than Threshold, this intermediate node is assumed as the black hole node. The source node stores this malicious node ID in MNT and discards that entry from the RRT table and broadcasts ALARM message to all nodes in the network to notify about this attack node. Then, the source node chooses the reliable node from the resting node and continues the normal operation of AODV protocol. After choosing the reliable node and removing the malicious node, the RRT table must be clear all data.

5. SIMULATION RESULTS

We have implemented the black hole attack behavior in AODV protocol using Network Simulator (NS-2.34) [13]. The main traffic generator used in this simulation is the Constant Bit Rate (CBR) and the overall simulation parameters are presented in Table 4. The performance of the AODV protocol and the proposed protocol with the black hole attack are analyzed and evaluated. The following metrics are used to analyze the results of our solution.

End-to-End Delay: It is the average delay of sending and receiving data packet between the source and the destination. It is measured in milliseconds

Packet Delivery Ratio (PDR): It is the ratio of total number of data packets transmitted by the sources and received by the destinations. Higher value means the better results [14].

Routing Overhead: It is the ratio of total number of control packet generated to the data packets transmitted. .

Table 4. Simulation parameters

Parameter	Value
Simulator	NS-2.34
Area	800m x 800m
Routing Protocol	AODV, BlackholeAODV, MAODV
Simulation time	200s
Application Traffic	CBR
Number of Nodes	50-200
Malicious Node	1-4
Pause time	2s
Packet Size	512 bytes
Transmission rate	2 packets/s
Mobility speed	10 m/s
No of Connections	20-40
Movement Model	Random Waypoint

5.1 Performance Analysis on Variation of Malicious Node

We have created a network by using simulation parameters shown in Table 4. Figure 2 illustrates the effect of malicious nodes on PDR in MANET. The numbers of malicious nodes for simulation are used randomly from one to four. It can be seen that AODV heavily suffers from the black hole attack. In Figure 2, when the number of malicious node in the network increases, the PDR of AODV protocol decreases. On the other hand, the experimental

results show that the PDR of MAODV protocol is above 95% even though the malicious node is increased. MAODV has higher average packet delivery than AODV. This is due to the fact that the proposed protocol can prevent the black hole attack that occurs in the network.

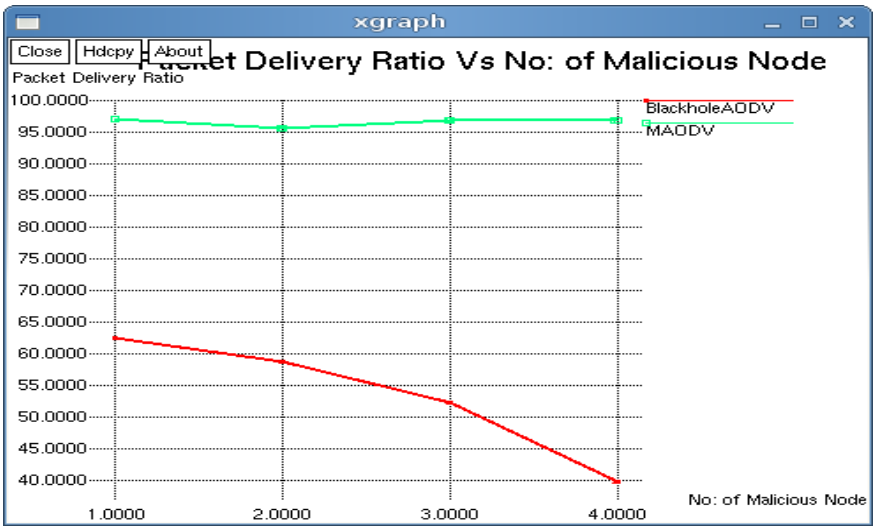

Figure 2. Packet delivery ratio over number of malicious nodes

The impact of malicious nodes to the routing overhead and the average end-to-end delay are presented in Figure 3 and Figure 4. In AODV under attack, the routing overhead is very high comparing to MAODV protocol. The delay of MAODV is higher than the AODV protocol under attack due to the additional waiting time for route replies. There is decrease in the delay of the AODV protocol with black hole attack as the immediate reply of malicious node without checking its routing table.

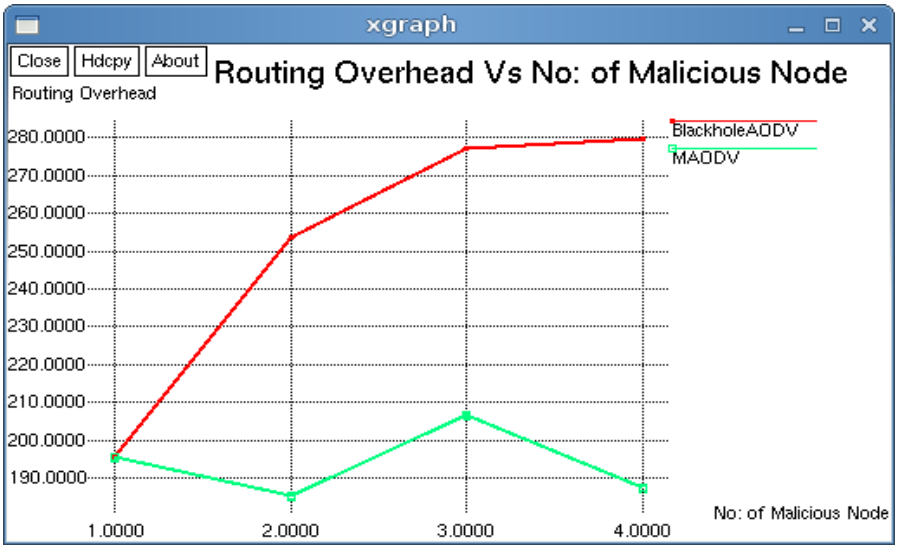

Figure 3. Routing overhead over number of malicious nodes

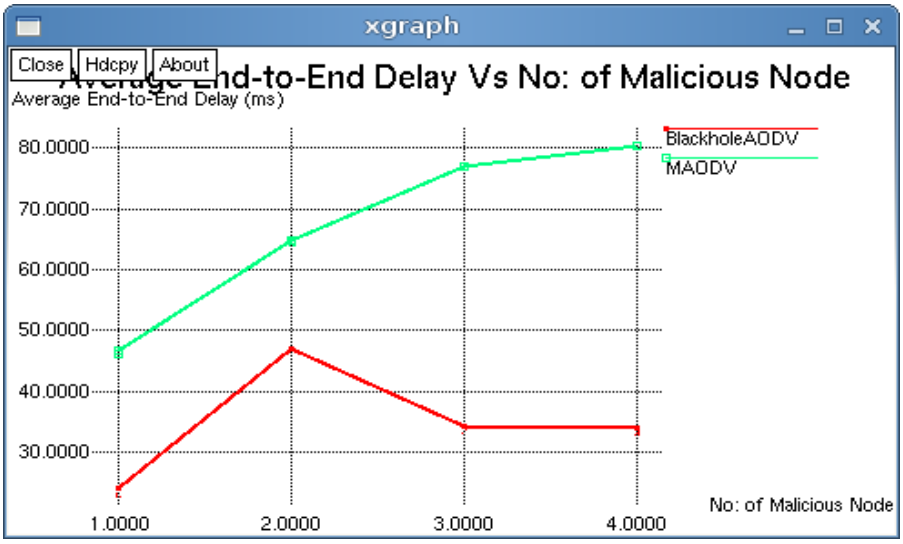

Figure 4. Average end-to-end delay over number of malicious nodes

5.2 Performance Analysis on Variation of Node

The performance results of all protocols are shown in Figure 5 to Figure 7 when the network size is increasing. When the number of nodes in the network increases, the PDR of AODV also decreases in Figure 5. It is due to the larger the number of intermediate nodes on an active route, the more increases the route failure. The PDR of AODV with attack decrease even more due to the probability that the malicious node become an intermediate node. On the other hand, the PDR of MAODV is greater than AODV with attack because our detection approach is able to identify and eliminate the malicious node which greatly increases the network PDR.

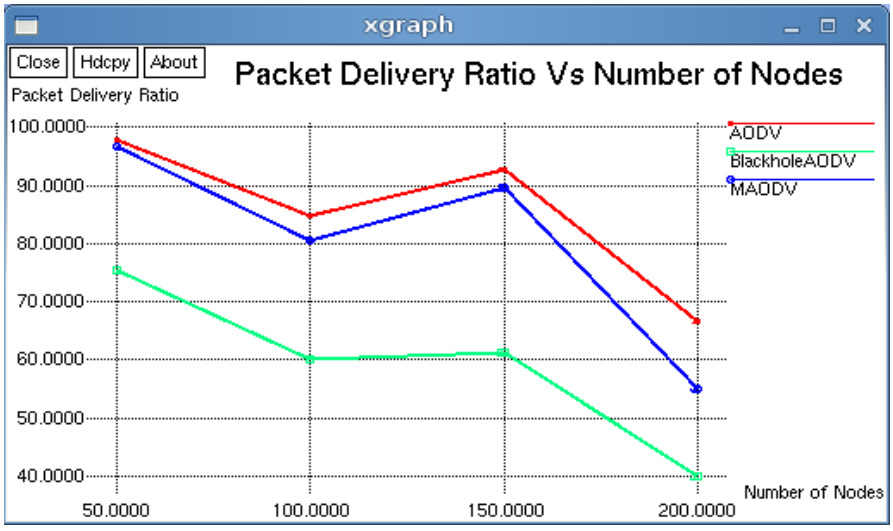

Figure 5. Packet delivery ratio over number of nodes

The routing overhead over number of nodes is depicted in Figure 6. The routing overhead for all protocols increases as the network size is growth. The routing overhead of the blackholeAODV protocol is greater than the normal AODV and MAODV protocol since the black hole node is present. The overhead of MAODV is the same as the normal AODV except 200 node scenario. This is the proposed protocol generate any additional requests for discovering secure routes. The impact of number of nodes on delay is shown in Figure 7. The delay of the proposed protocol increases at 100 node scenario since it has to avoid the malicious node.

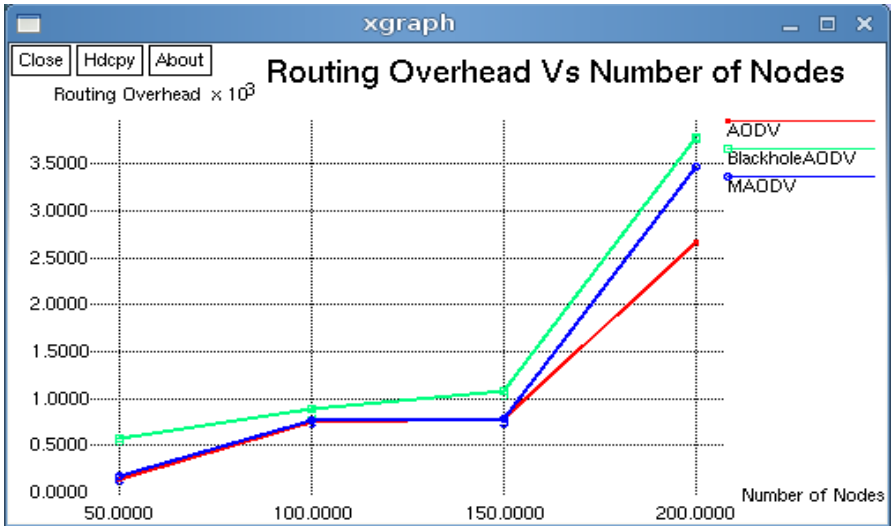

Figure 6. Routing overhead over number of nodes

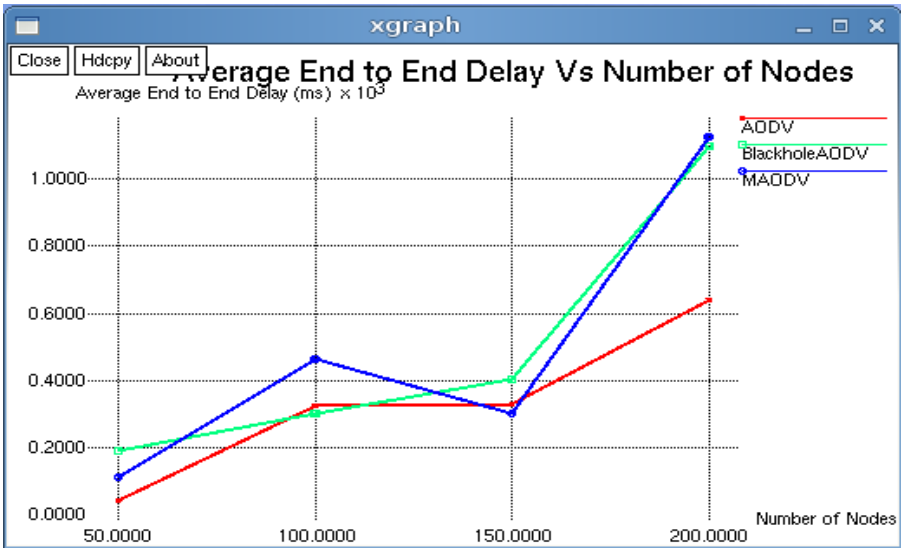

Figure 7. Average end-to-end delay over number of nodes

6. CONCLUSIONS

In this paper, a simple approach for eliminating the black hole attack for MANET is proposed. The proposed mechanism can apply to remove black hole node and to find a reliable route form source to destination in the MANET. In this mechanism, the process of source node in AODV protocol is modified by introducing two tables and alarm packet type. These tables are Route Reply Record Table (RRT) to store Route Reply from neighbor's nodes and Malicious Node Table (MNT) to store the information about the malicious nodes. The black hole node can be removed and the reliable node can be chosen by using these tables. The alarm packet type is also proposed to inform the intruder node to all neighboring nodes when the black hole node is detected.

To evaluate the applicability of this routing algorithm, we simulated different scenarios using AODV protocol and proposed protocol with the black bole node. We considered the performance metrics such as routing overhead, PDR and delay on different scenarios with number of nodes and number of malicious nodes as variable parameters. The experimental results present that the proposed system performs better than the AODV protocol. However, the proposed system assumed that the route reply comes from more than one node within the waiting time. If the source node receives the only one route reply from the black hole node or the route replies from all the black hole nodes during the waiting time, the malicious node can enter the network.

REFERENCES

[1] Ramaswami, S. S., and Upadhyaya, S. Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing. *Proceedings of the 2006 IEEE Workshop on Information Assurance*, 2006.

[2] Luo, J., Fan, M., and Ye, D. Black Hole Attack Prevention Based on Authentication Mechanism. *IEEE*, 2008.

[3] Obaida, M. A., Faisal, S. A., Horaira, M. A., and Roy, T. K. AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes. *International Journal of Advanced Computer Sciences and Applications*, 2, 8 (2011), pp. 97-102.

[4] Mistry, N., Jinwala, D. C., and Zaveri, M. Improving AODV Protocol against Black Hole Attacks. *International Multi Conference of Engineers and Computer Scientists*, 2, (2010).

[5] Himral, L., Vig, V., and Chand, N. Preventing AODV Routing Protocol from Black Hole Attack. *International Journal of Engineering Science and Technology*, 3, 5 (2011).

[6] Jalil, K. A., Ahmad, Z., and Manan, J. A. Mitigation of Black Hole Attacks for AODV Routing Protocol. *Society of Digital Information and Wireless Communications*, 1, 2 (2011).

[7] Perkins, C. E., Royer, E. B., and Das, S. Ad-Hoc on Demand Distance Vector (AODV) Routing. IETF RFC 3561, 2003.

[8] Perkins, C. E., and Bhagwat, P. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, (1994), pp. 231–241.

[9] Ochola, E., and Eloff, M. A Review of Black Hole Attack on AODV Routing in MANET. http://icsa.cs.up.ac.za/issa/2011/Proceedings/Research/Ochola_Eloff.pdf.

[10] Shurman, M. A., Yoo, S. M., and Park, S. Black hole Attack in Mobile Ad Hoc Networks. *Proceedings of the 42nd Annual Southeast Regional Conference ACM-SE 42*, (2004), pp. 96-97.

[11] Deng, H., Li, W., and Agarwal, D. P. Routing Security in Wireless Ad Hoc Networks. *IEEE Communications Magazine*, 40, 10 (2002).

[12] Sandhu, G., and Dasgupta, M. Impact of Black Hole Attack in MANET. *International Journal of Recent Trends in Engineering and Technology*, 3, 2(2010).

[13] Fall, K., and Varadhan, K. The NS Manual. (November 2011), http://www.isi.edu/nsnam/ns/doc/index.html.

[14] Jaafar, M. A., and Zukarnain, Z. A. Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment. *European Journal of Scientific Research*, 32, 3(2009), pp. 430-443.

This paper may be cited as:

Khin, E. E., and Phyu, T., 2015. Enhancing AODV Routing Protocol to Eliminate Black Hole Attack in MANET. *International Journal of Computer Science and Business Informatics, Vol. 15, No.2, pp.1-14*.