Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 2, August 2017, pp. 577 ~ 582
DOI: 10.11591/ijeecs.v7.i2.pp577-582

Mobile Ad Hoc Networks in Presence of Black Hole Attack

Anshu Prakash Murdan*, Anshuman Bhowon
Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Mauritius
Reduit, Mauritius
*Corresponding author, e-mail: a.murdan@uom.ac.mu

Abstract

This paper analyses three performance metrics namely average throughput, average network load and average video conferencing packet end-to-end delays under the influence of black hole attack in a Mobile Ad Hoc Network, using the ad hoc on-demand distance vector routing protocol. The simulation was carried out on Riverbed Modeler Academic Edition software. Simulation results show that the average throughput, average network load and average video conferencing packet end-to-end delay decreases as the number of black hole attack nodes is increased. Also, the effects of the influence of black hole attack nodes tend to decrease due to mobility of the nodes. It was observed that when the destination nodes move closer to the source nodes and get in to the latter's transmission range, the effects of the black hole attack is greatly minimized.

Keywords*: black hole attack; ad hoc on-demand distance vector routing protocol; Riverbed Modeler Academic Edition*

1. Introduction

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly [1]. The nodes are able to communicate among themselves without depending on a system which is centralized (base stations or access points) or a network infrastructure. The connections between the nodes are said to be dynamic implying that connections can be made, broken and made again whenever it is required to do so. Ad hoc On-Demand Distance Vector (AODV) is a routing protocol for MANETs and other wireless ad hoc networks. AODV is a routing protocol which is reactive and it allows a node acting as a source to get the shortest route to a node which is acting as the destination, when connection between the two is required. The route is sustained as long as the source and destination communicate. According to Barkhodia *et al.*, three messages or signals are involved in the functioning of the AODV protocol [2]. These three messages (signals) are:

a) route request (RREQ)
b) route reply (RREP)
c) route error (RERR)

2. AODV Routing Protocol

Each time a node sends out a message, it results in an increase of its own sequence number. The route emanating from a node with highest sequence number implies a "freshest" route. A fresh route is the route with the highest sequence number. Suppose a packet has to be forwarded to a destination node by a source node but the former is not within the latter's transmission range. The sender will broadcast a RREQ signal to intermediate nodes. An intermediate node will check if it has a route which is fresh to the destination and in case it does have one, it will unicast a RREP signal to the sender node thus forming a route between the sender and the destination. If the intermediate node does not possess a fresh route to the destination node, it will broadcast the RREQ signal from the sender to other intermediate nodes which in turn will broadcast the RREQ signal to other intermediate nodes until a node with fresh route to destination node is reached. Once the RREQ signal reaches the destination node, the

Received May 1, 2017; Revised July 9, 2017; Accepted July 26, 2017

latter will unicast a RREP signal to the sender thus forming a route connecting the sender to the destination.

Upon reception of the RREP signal by the source node, the latter will forward the packet towards the destination node through a shortest path which is the route with the highest sequence number to the destination node and with the least hop count.

A black hole attack is a routing layer attack. It is also categorized as a type of Denial-of-Service attack [3] where the packets are dropped by a malicious node or many malicious nodes. When many malicious nodes are conducting a black hole attack, it is called a cooperative black hole attack [4]. A source node broadcasts a RREQ signal to intermediate nodes until the signal reaches a node with "freshest" route to the destination node. If one of the intermediate nodes turns out to be a malicious node, it immediately responds to the RREQ signal with a RREP signal sent to the source node. The RREP signal has its sequence number intentionally modified by the malicious node to the highest number. This will result in making the source node assume that the node, which is in fact the malicious node, possesses the shortest and "freshest" route to the destination. The source node will forward its packets to the malicious node which in turn will drop the packets resulting in the latter not being able to reach its destination node.

Kaur and Singh [5] analyzed the effect of black hole and grey hole attack on Wireless Mesh Networks where OLSR routing protocol was used. The parameter that was recorded to observe the performance of the network was the delay in the network. It was found that OLSR routing protocol managed to decrease the effect of the attacks to a small extent only. Gupta and Aggarwal [6] investigated the effects of a cooperative black hole attack on the throughput, the packet delivery ratio and the end-to-end delay. The authors concluded that the throughput, packet delivery ratio and end-to-end delay showed a drastic decrease when exposed to the attack. Esmaili et al. [7] assessed the performance of AODV under black hole attack. They proposed solutions such as securing routing and intrusion detection system. The performance metric that was analyzed was the packet delivery ratio in the presence of up to four malicious nodes. The conclusion was that the packet delivery ratio decreased by large values in presence of black hole nodes. Shree and Talib [8] studied the performance of wireless ad hoc networks when black hole attack is prevailing in the network. The simulation was carried out using different number of nodes to demonstrate the variance of the packet delivery ratio when the number of nodes is increased. It was concluded that the packet delivery ratio gradually decreased when subjected to a black hole attack.

In this research work, the performance of a network, involving AODV routing protocol, File Transfer Protocol (FTP) and Video Conferencing traffic, under black hole attack was analyzed. The network environment in which the simulation was carried out was 802.11b which allows transmission of packets up to 11 Mbps. The performance metrics that were observed and analyzed were the average throughput, the average network load and the average video conferencing packet end-to-end delay. The simulation was performed with 15 nodes and each of them was configured accordingly. The project involved a total of five scenarios, with no malicious node, one malicious node, two, three and four malicious nodes, for each scenario.

3. Results and Analysis

Riverbed Modeler Academic Edition 17.5 was used for the simulation. The network scale chosen was a campus of size 800m*800m. Fifteen wireless LAN workstations, representing the nodes were configured to act as both clients and servers. The applications selected to generate traffic were FTP and video conferencing. The parameters of the receivers and transmitters were configured with RX-Group. The attributes of the 15 mobile nodes, the application configuration, the profile configuration and RX Group configuration were configured according to the work done by Shrestha and Tekiner [9]. The mobility configuration was based on research done by Kaur and Singh [5].

3.1 Parameter Configurations for the network with no malicious nodes present

The wireless parameters were configured on the nodes based on the research work of Aboelela [10], with the following modifications:

(1) In order to decrease the probability of collisions occurring amongst packets, the RTS (Request to Send) Threshold has been modified to 256 bytes instead of 0.

(2) As the flow of application traffic is heavy, the buffer size has been brought to 102,400,000 bits.
(3) Due to heavy traffic resulting from heavy flow of applications, the transmission power has been modified from the default value 0.005 watt to 0.030 watt.

In order to add traffic to the network, the following application and profile configurations were carried out.

(1) Application Configurations

Application configuration demonstrates the type of traffic that will flow in the network. The two applications that were configured were the FTP (File Transfer Protocol) application and the Video Conferencing application.

The FTP application was named as FTP_Application_AB and was set to High Load. The Video Conferencing application was named VideoConferencing_Application and was assigned as High Resolution Video. The other parameters were set to the default values already available in the simulator.

(2) Profile Configurations

A profile consists of applications defined in the application configuration. The profile will be assigned to nodes allowing the latter to transfer traffic in terms of application configured. Once the profile configurations were over, both the FTP_Profile_AB and the VideoConferencing_Profile were assigned to all the 15 nodes present in the topology.

The AODV parameters were configured on all of the 15 nodes. The mobility model chosen was random waypoint. In random waypoint, all the nodes move in a zig-zag line pattern from one waypoint to another waypoint. A waypoint is a point at which a node will stop momentarily before moving to another point. All parameters in the mobility configurations were left to their default values apart from the speed of the nodes which was set to 10 m/s.

The duration of the simulation was 10 minutes (600 seconds) and the values collected per statistic was 100. The other parameters available were left to their default values.

3.2 Parameter Configurations for the network in presence of malicious node/s

Nodes were configured to carry out the effect of a black hole attack, that is, to drop packets being sent. To achieve this, modifications were brought to the AODV routing protocol parameters. The parameters in section B were left unchanged except the Active Route Timeout (seconds) and the Packet Queue Size (packets), which were set to zero.

Active Route Timeout is the amount of time for which a path is active and once the time has elapsed, the route will be disabled but not deleted. An Active Route Timeout of 0 seconds will disable a route thus preventing packets from being transmitted to the destination node of the path. This results in packets being dropped.

Packet Queue Size is the number of packets that are waiting in a queue in order to be processed and transferred from one node to the destination node of a path. A Packet Queue Size of 0 will result in 0 packets bring processed and transferred from a node to the destination node of the route thus causing packets to be dropped.

In scenarios where more than one malicious nodes are involved, the same configurations are applied to each malicious node as described previously in this section.

The statistics that were collected and analyzed were:

a) Average Throughput
   Average throughput is the average rate of successfully transmitting packets from one node to another node over a network.
b) Average Network Load
   Average network load is the average amount of traffic circulating in a network.
c) Average Video Conferencing Packet End - to- End Delay
   The average amount of time it takes for packets to travel from a source node to a destination node in a communications network is called the average packet end-to-end delay. It is measured in seconds.

3.3 Analysis of Results

The results for the average throughput for all the five scenarios are illustrated in Figure 1. The Table 1 defines the traces on the Figures 1-3. Minimum Average throughput

= 250 bits/sec, for all scenarios. With no malicious node (trace0), the average throughput increases, stabilizes and increases further, with time.

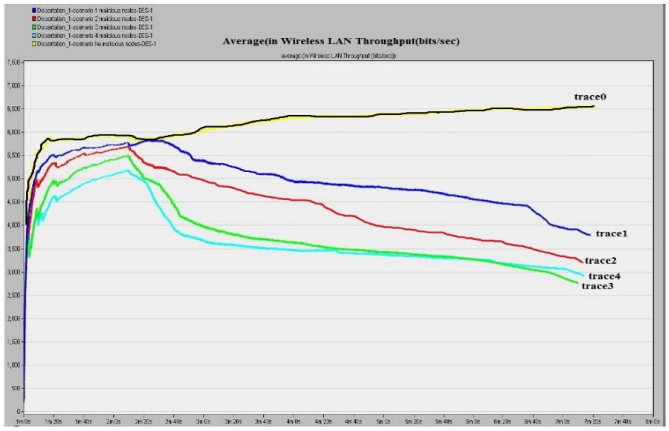

Figure 1 Average throughput for all the scenarios

Table 1 Trace on figures

No. of malicious nodes	Trace on Figures
Zero	trace0
1	trace1
2	trace2
3	trace3
4	trace4

In all other cases, i.e trace1 to trace4, there is an increase in throughput, then a gradual decrease after around 2 minutes 30 seconds. It is also observed that trace1 to trace4 take lower values of throughput than trace0. This is because the packets reach the malicious node/s and the latter starts dropping them. As the number of malicious nodes increases, the average throughput decreases.

The results for the average network load for all the five scenarios are shown in Figure 2. All the traces follow the same pattern for the first 2 minutes of the simulation. They all start from an average network load of approximately 250 bits/sec to reach a value of approximately 6200 bits/sec in around 1 minute 20 seconds. They maintain this value of approximately 6200 bits/sec till around 2 minutes. From around 2 minutes 15 seconds onwards, the traces start to diverge.

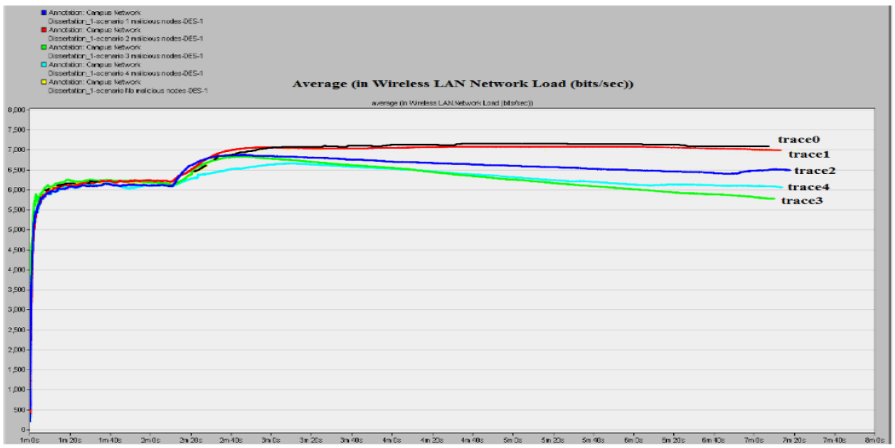

Figure 2 Average network load for all the scenarios

As the number of malicious nodes increase, from 0 to 4, the average network load gradually decreases, because of the packets being dropped by the malicious node, resulting in gradual decrease in network traffic.

From around 2 minutes 15 seconds to around 3 minutes 0 seconds, there is a sudden rise in average network load in all of the 5 scenarios. This can be due to more packets being pumped into the network during this particular time interval. Another possible reason could be the destination nodes being in the transmission range of the source nodes causing increase in the traffic circulating in the network.

The results for the average video conferencing packet end-to-end delay for all the five scenarios are illustrated in Figure 3. The average video conferencing packet end-to-end delay can be approximately defined as the summation of all end-to-end delays of video conferencing packets being successfully transmitted from source nodes to destination nodes divided by the number of packets being introduced by the source nodes in the communications network. It is observed that the trace0 increases almost linearly because nearly all the packets introduced in the network are being successfully sent by the source nodes to the destination nodes.

Trace1 - the average video conferencing packet end-to-end delay increases linearly to reach a value of approximately 92.5 seconds at 5 minutes 45 seconds. It maintains this value for some time. This value could be due to two reasons: Firstly, the number of packets being introduced is constant and all the packets being introduced are being successfully transmitted to the destination nodes. But as from 6 minutes 45 seconds, a decrease is noticed. This can be due to the effect of the malicious node having started dropping packets causing a decrease in the sum of video conferencing packet end-to-end delays which in turn leads to a decrease in the average video conferencing packet end-to-end delay.

Secondly, effects of the malicious nodes could have started as from 5 minutes 45 seconds only. Since the number of packets being dropped is constant, the sum of the video conferencing end-to-end delays will also remain constant. This results in the average video conferencing packet end-to-end delay to be constant. A decrease is noticed as from 6 minutes 45 seconds and this could be due to the malicious node dropping more video conferencing packets.

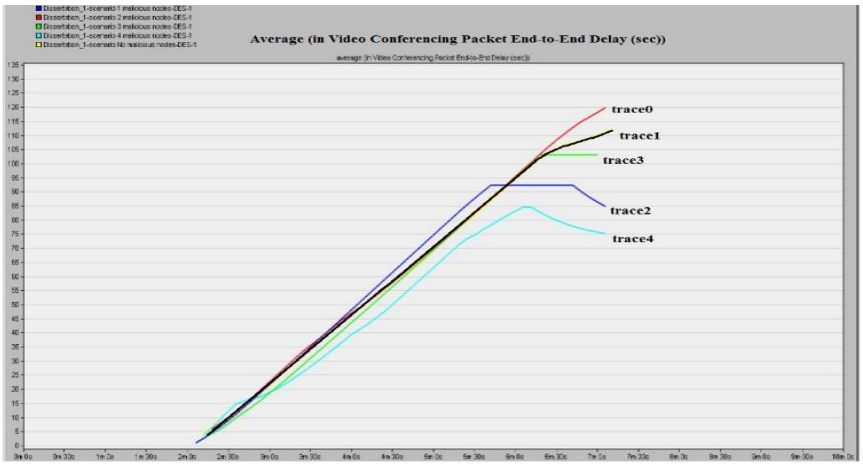

Figure 3 Average video conferencing packet end-to-end delay

As the number of malicious nodes increases from 2 to 4, the number of packets which are dropped is much higher. This results in a decrease in the sum of all video conferencing packet end-to-end delays leading to the average video conferencing packet end-to-end delay to also decrease.

The following observations were made:

(1) The maximum average throughput, maximum average network load and maximum average video conferencing packet end-to-end delay of the network depends on the number of nodes present. The greater the number of nodes:

a) the greater the number of packets being transmitted resulting in higher average throughput
b) the greater the traffic circulating in the network resulting in higher average network load
c) the greater the video conferencing packet end-to-end delays as more packets are being successfully transmitted from the source nodes to the destination nodes.

(2) Throughout the simulation, not all the packets in the circuit are being dropped. Some of the packets circulating do manage to reach their destination nodes. This can explain the fact that the traces of the performance metrics obtained have not reached zero at all.

4. Conclusion

The results revealed that black hole attacks can cause tremendous damage to a network. It has been observed that the average throughput has the tendency to decrease when the number of malicious nodes increased. Dropping of the packets resulted in lesser number of packets being able to successfully reach their destination. The average network load results have shown more or less the same tendency as the average throughput results. They also showed a decrease as the number of malicious nodes increases. The greater the number of packets being dropped, the lesser the traffic circulating in the communications network. The average video conferencing packet end-to-end delay increased linearly during the early minutes in all scenarios. But as the malicious nodes got into action, the delay in question became either constant or started to decrease. The decrease, without any doubt, does not mean that packets are travelling faster. The dropping of the packets results in the decrease in the sum of all the video conferencing packet end-to-end delays resulting in the average video conferencing packet end-to-end delay to also decrease or remain constant in cases where packets are being dropped constantly.

Another important observation is that when the destination nodes move closer to the source nodes and get in to the latter's transmission range, the effects of the black hole attack is greatly minimized. This is because the source nodes do not have to send RREQ messages which get intercepted by the malicious nodes. The source nodes communicate directly with the destination nodes for sending packets.

Further research could be carried out to make a deeper analysis of the effects of black hole attacks in other types of networks such as wireless local area networks. Also different routing protocols could be examined in order to determine the effects of black hole attacks on their performance.

References

[1] Chai Keong Toh*,* Ad Hoc Mobile Wireless Networks: Protocols and Systems 1st Edition, Prentice Hall PTR, 2002.
[2] E. Barkhodia, E. Singh, P. and G. Kaur, *"Performance Analysis of AODV using HTTP traffic under Black Hole Attack in MANET"* Computer Science and Engineering: An International Journal, 2(3), 2012, pp. 99 - 108.
[3] A. D. Wood and J. A. Stankovic, *"Denial of service in sensor networks*," in *Computer*, vol. 35, no. 10, pp. 54-62, Oct 2002. doi: 10.1109/MC.2002.1039518
[4] Tamilselvan, Latha, and V. Sankaranarayanan, *"Prevention of co-operative black hole attack in MANET.*" Journal of networks, 2008, pp 13-20.
[5] R. Kaur and P. Singh, 2014, *"Black Hole and Greyhole Attack in Wireless Mesh Network"*, American Journal of Engineering Research, 3(10), 2014, pp. 41 - 47.
[6] H. Gupta and H. Aggarwal, *"Simulation to Detect and Removal of Black Hole in Manet*", SSRG International Journal of Electronics and Communcation Engineering, 2015, pp. 35 - 40.
[7] H. A. Esmaili, and M. R. Shoja, *"Performance analysis of AODV under black hole attack through use of OPNET simulator.*" arXiv preprint arXiv: 1104.4544 , 2011.
[8] O. Shree, O. and M. Talib, "*Wireless Ad-hoc Network under Black-hole Attack",* International Journal of Digital Information and Wireless Communications, 1(3), 2011, pp. 591-596.
[9] A. Shrestha and F. Tekiner, *"On Manet Routing Protocols for Mobility and Scalability"* in 2009 International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 451-456. IEEE, 2009.
[10] Aboelela, Computer Network A Systems Approach, 4thn ed., Morgan Kaufmann Publishers, 2008, pp. 185 – 190.