An Analysis on Security Threats of Black-Hole and Jellyfish Attacks in Mobile Ad-Hoc Network using HTTP Traffic

Author(s): *1,2Dewan Juel Rahman, 1,2Faisal Ahmed, 1,2Sayma Rashid
Affiliation(s): 1Department of Computer Science and Engineering
BRAC University, Bangladesh
2Rajshahi Science and Technology University (RSTU)
Dhaka, Bangladesh
*Corresponding Author: juelrstu@gmail.com

Abstract - Mobile ad-hoc network (MANET) is an infrastructure less network. This network is a collection of randomly moving mobile nodes. As MANET does not have any centralized management, this network can form anywhere with the participation of randomly moving nodes. Because of such vulnerable behaviour of MANET, this network has to face many security problems. There are so many security threats of MANET, which does not have any solution. Even detection of those problems is not easy. Some of the security threats are very severe. Those threats can even destroy the whole network. Researchers are working to find out the solution of those threats. Among those threats, we have worked with two security threats, which are Black-hole attack and Jellyfish attack. Here, we have found out the threats using HTTP traffic. We use OPNET modeler 14.5 as simulator AODV routing protocol. The aim of this paper is to find out the impact of security threats on MANET using HTTP traffic. We decide the impact using number of events and average number of events utilizing throughput of the OPNET modeler.

Keywords: Network; HTTP; Security; Threats; MANET

I. INTRODUCTION

We are living in the era or technological advancement. In this advanced world Mobile Ad-hoc network (MANET) is one of greatest technology. It has made so many nonviable works easier for us. MANET is a self-determining collection of mobile nodes. MANET is a collection of mobile nodes, which can communicate with each other via radio waves. There are so many security issues in MANET. Such as packet dropping attack data traffic attack, Black-hole attack, Jellyfish attack, Control Traffic attack etc. Here we have focused on two important security attack on MANET, which are Black-hole attack, and Jellyfish attack. Both of these attacks are so threatening for the MANET and can cause a great security disaster in any confidential work, which is performing with the help of MANET.

II. BACKGROUND INFORMATION

A. Security Issues in MANET

Mobile Ad Hoc Network (MANET) is infrastructure less network and each of its nodes is free to move everywhere. Any devices can join this network at any time. These features have brought so many security issues. It has increased probability of much security attack in MANET. There are so many security attacks in MANET. These attacks can classify into three types according to its nature.

- Active attack.
- Passive attack
- Hybrid attack

In our research, we have focused on two attacks, which are Black-hole attack and Jellyfish attack. Black-hole attack is an active attack and Jellyfish attack is a passive attack.

B. Black Hole Attack

Black hole attack is an attack that happens in Mobile ad hoc network (MANET) which disables that particular victim network. It is an active attack. In this attack, a malicious node enters in the network and advertises itself to other nodes, which exist on that network. It advertises itself as a shortest path to the destination node or to the...
packet; it wants to head off. The host node responds by advertising its availability of fresh routes without checking routing table. Then attacker node replies to the host nodes, intercept the data packet and retain it. In protocol, based routing reply of a malicious node will received before the reply of actual node. Later malicious route will be created. It will intercept the data traffic and will dropped with data from the existing network. As in MANET each node stands with keeping hand in hand relying each other, so dropping of one node will cause of dropping other nodes, which lead to destruction of the whole network eventually. Black hole attack can be two types. In single Black hole attack, one malicious node enters in the network. It advertises itself as a shortest path to the destination node. Other neighboring nodes thinks that it is the shortest path for sending data. If the malicious node reply reaches to those nodes before the authenticate nodes reply, then a forged route creates there. All other nodes in the network send all their data traffic to that malicious black hole node and it retains all the data and drops with them. A single black hole attack can easily happen in MANET. In case of collaborative black hole attack, many malicious nodes enter in the network. They advertise as being the shortest path to the destination for attracting other nodes. If those nodes believe them and receives, their reply before the actual nodes reply then forged route creates in MANET. Collaborative attack is efficient than Single black hole attack as there are many malicious nodes to work together for the destruction of the MANET.

C. Jellyfish Attack

Jellyfish attack is one kind of denial of service attack, which is a passive attack. This attack is tough to detect, as it is a passive attack. Most of the defense mechanisms are not able to detect a set of protocol compliant attacks called jellyfish attacks. Jellyfish attack creates delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing provided by TCP and UDP. Jellyfish attack can be three types

- Jellyfish delay variance attack.
- Jellyfish recorder attack.
- Jellyfish periodic dropping attack.

In our research we have worked with jellyfish delay variance attack which creates delay in sending data traffic. In jellyfish delay, variance attack malicious route does not stop the data sending process but it creates delay in sending data. They maintain FIFO order. After getting access in the network system, malicious node creates delay in all the data packets it receives. Delay time is usually ranging zero to ten seconds. Such delay variance attacks

- Can lead to increase collision and loss of important data of the network.
- It can also cause blunder of available bandwidth for the delay-based blockage protocol.

D. AODV Protocol

Ad-Hoc On-Demand Distance Vector routing (AODV) is routing protocol, which creates routing between two nodes in the network based on route discovery. This routing protocol uses a classical distance vector routing algorithm. It is a reactive routing protocol. This routing protocol transmits information based on the demand of nodes. When any node wants to transmit data to other nodes, this routing protocol will generate route request message. AODV provide loop free route to the network when repairing link breakage. One of the best features of AODV is it provides broadcast, unicast and multicast communication. It also faster routing protocol as it finds out entire unidentified network and for newer end, which does not exist on the navigation of that particular network.

III. FLOORPLAN & PROPOSED SYSTEM

A. Setup of OPNET Modeler

First, we set our attributes for the simulation scenarios for our paper. Some of the parameters were fixed and we changed some for simulating it on different criteria.
affected scenarios with jellyfish attack. From that we can come to know which attack is affecting which parameters of our network.

C. Generated Model

From the analysis of different area vs. different nodes, we can select a security attack preventive scenario. It will be an avoidance procedure not a solution to the security attack. From the analysis, we can select how much area is suitable for a given number of node or how many nodes are suitable for different area size. From the analysis of black hole vs. jellyfish attack, we can point out which parameters of our scenarios are being affected. The results can be used to form customize algorithm in replace to conventional routing algorithms like AODV, OLSR, TORA etc.

IV. EXPERIMENTAL ANALYSIS
We have already discussed how black-hole and jellyfish attack occurs in a network scenario. Black-hole attack blends into the network and causes dropout of packets whereas jellyfish attack disrupts the net packet transfer. In the proposed model we have measured what effects does these two security forge attacks have on a given network scenario by measuring the output of different parameters of the network. Then we compared the results with default (scenarios with no attack) scenarios and observed the outcome. For our proposed model, OPNET Modeler 14.5 is used. All the experiments done in a personal computer (PC) with the configuration Intel(R) Core i3-4160 CPU @ 3.6 GHz, 8GB RAM, running Windows 8. In this paper, we have analyzed the effects of the security attacks on different areas against different number of nodes per simulation. Firstly, we measured the throughputs of the scenarios throughout the entire attack simulation. Secondly, we calculated the change in number of events after the simulation per scenario. Lastly, we compared the results generated for different areas with results found for different nodes

A. Environmental Setup for different areas of simulation
For measuring the after effects of black-hole and jellyfish attack on different areas, we ran the simulation for 500mx500m, 1000mx1000m, 1500mx1500m, 2000mx2000m, 2500mx2500m

Figure 2 Represents the scenario selected for this simulation. Here, we kept the number of nodes fixed to 100 and ran the paper for different simulation areas. Simulation runtime was set to 15 minutes, model family was selected MANET, protocol was fixed to AODV, traffic was set to HTTP, mobility of the nodes was set to default random waypoint, node movement speed was 10 meter per second. After that 5 malicious nodes were injected to the scenarios to compare the results against default scenarios with no malicious nodes.

For different nodes, we created 5 different scenarios consisting of 35 nodes, 75 nodes, 100 nodes, 130 nodes and 150 nodes

Figure 3 represents the network parameters and attributes selected for the simulations. For each simulation, the numbers of nodes were changed. Simulation area was fixed to 1500mx1500m. Simulation time was 15 minutes, simulation protocol was set AODV, traffic was selected HTTP, node mobility was default random waypoint and node mobility. Speed was set to 10 meter per second. The numbers of malicious nodes in the scenarios selected
accordingly to compare the results against different areas of simulation.

V. RESULT ANALYSIS

A. Impact of Black-hole attack on number of events for different areas and nodes

Figure 4 shows the impact of black-hole attack on total number of events for different areas. Here we can observe that the total number of events occurred for the affected scenarios are much less compared to the default scenarios.

\[
\forall x \in B (\sum E (a) > \sum E (n)) \quad (1)
\]

Where,

- B = Black-hole attack
- x = Network scenario
- E = Reduction in number of occurred events
- a = Rate of change in area
- n = Rate of change in number of nodes

B. Impact of Jellyfish on number of events for different areas and nodes

Figure 6 represents the impact of jellyfish attack on average number of events for rate in change of area. Jellyfish attack effects the average number of events per seconds rather than total number events as it adds delay in packet transferring.

\[
\forall x \in J (\sum (E (a)) > \sum (E (n))) \quad (2)
\]

Where,

- J = Jellyfish attack
- x = Network scenario

Similarly, figure 5 represents the impact on number of events for different scenarios with different number of nodes. However, in this case the data shows that the number of total occurred events for attack scenario is not as reduced as the case before. Therefore, from that we can explain, for black-hole attack, rate of change in area has greater impact than rate of change in number of nodes. If we represent it with equation, we can obtain,

\[
\forall x \in B (\sum E (a) > \sum E (n)) \quad (1)
\]

Figure 7 shows the impact of Jellyfish attack on average number of events. In here, we can again observe that, the average number of events per second reduced much in rate in change area than rate in change of number of nodes. Representing the result with equation, we get,

\[
\forall x \in J (\sum (E (a)) > \sum (E (n))) \quad (2)
\]
VI. CONCLUSIONS

In this paper, based on the experimental result, showed that for black-hole and jellyfish attack rate of change in area affects the network scenario more than rate of change in number of nodes. This paper also proved that, black-hole and jellyfish attack effects two different parameters of a given network scenario, black-hole effects the net throughput whereas jellyfish attack effects the packet transfer ratio between nodes. As everyday new flaws and limitations are being identified, we believe that this brief research will help in identifying the key problems of MANET network and to improve and overcome those limitations gradually.

ACKNOWLEDGMENT

All thanks to Almighty ALLAH, the creator and the owner of this universe, the most merciful, beneficent and the most gracious, who provided us guidance, strength and abilities to complete this research? We are especially thankful to Dr. Jia Uddin, Professor, BRAC University, for his help, guidance and support in completion of our paper. Finally, we would like to express our sincere gratefulness to our beloved parents, brothers and sisters for their love and care.

REFERENCES


