Impact of Black-hole and Jellyfish Attacks in MANET using HTTP Traffic

Supervisor: **Dr. Jia Uddin**

Faisal Ahmed	12101123
Sayma Rashid	12101094
Md. Ashikur Rahman	14301127

Department of Computer Science and Engineering,

BRAC University

Submitted on: 14th December 2016

DECLARATION

We, hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This Thesis, neither in whole or in part, has been previously submitted for any degree.

Signature of Supervisor

Dr. Jia Uddin

Signature of Author

Faisal Ahmed

Sayma Rashid

Md. Ashikur Rahman

ACKNOWLEDGEMENTS

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, our thesis supervisor, for his help, guidance and support in completion of our project. We also thankful to the BRAC University Faculty Staffs of the Computer Science and Engineering, who have been a light of guidance for us in the whole study period at BRAC University, particularly in building our base in education and enhancing our knowledge.

Finally, we would like to express our sincere gratefulness to our beloved parents, brothers and sisters for their love and care. We are grateful to all of our friends who helped us directly or indirectly to complete our thesis.

CONTENTS

LIST OF FIGURES

ABSTRACT

Mobile ad-hoc network (MANET) is an infrastructure less network. This network is a collection of randomly moving mobile nodes. As MANET doesn't have any centralized management, this network can form anywhere with the participation of randomly moving nodes. Because of such vulnerable behavior of MANET, this network has to face a lot of security problems. There are so many security threats of MANET which doesn't 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 thesis 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.

CHAPTER 01

INTRODUCTION

1.1 Motivations

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 [1]. There are other wireless technologies such as cellular networks, IEEE-802.11 networks etc. But MANET's functionality is different from them. MANET is self-organizing and robust network. It can reform itself on the fly without the need for any system administration [2]. It can transfer data without any valid network infrastructure. Network like MANET is not only very dynamic, but also very swiftly changeable, haphazard, consists of multi-hop topologies and also composed of relatively bandwidth constrained wireless links [3]. As there is no background network in MANET, here all the nodes act as a superior in the network. That means all the network function control of operation and security depends on the nodes of the network. They fully rely on each other and help every neighbor node to communicate. They also help to the neighbor node to implement routing and security function [4]. If any node is out of communication range, then they help to send data via intermediate nodes. Here every nodes act not only as host but also behave like a router which forwards packets for other nodes [5].

MANET is the most fabulous form of advanced technology, it is widely using everywhere throughout the world. Most difficult communication works are done with the help of MANET. It is used to communicate in very remote places. Even it is using by military at the time of war. As MANET is using widely for so many confidential work, it has also many security issues. These security issues have brought challenges for this infrastructure less network. For this reason ensuring security has become one of most spectacular topic in the research world. Many researchers have been working for so long on this security issues, trying to find out its solution.

There are so many security issues in MANET. Such as packet dropping attack data traffic attack, Black-hole attack, Jellyfish attack, Control Traffic attack and etc. [6]. 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.

1.2 Contribution Summary

The summary of the main contributions is as follows:

- Our project highlights the key limitations of the MANET network infrastructure. In this thesis we have found out some vulnerabilities and loophole, in terms of node density and simulation area which signifies the characteristics of this type of network.
- From the analysis of particular security threats, we came up with some equations relating node density to area. Later on, it can be used to form custom algorithms for routing.
- From the results of statistical data and comparison, optimality of network environment can be maximized for a given scenario. Network parameters and attributes can be chosen using the data to achieve maximum efficiency.

1.3 Thesis Orientation

The rest of the thesis is organized as follows:

- Chapter 02 includes the necessary background information regarding MANETs security attacks.
- Chapter 03 presents the experimental results of the security threats and comparisons.
- Chapter 04 concludes the thesis and states the future research directions.

CHAPTER 02

BACKGROUND INFORMATION

2.1 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 be classified into three types according to its nature [7].

a. Active attack.
b. Passive attack.
c. 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.

2.1.1 Active attack

An active attack injects capricious packets in a network and tries to disrupt the operation or stop other packets which were supposed be transferred to other nodes [8]. The goal of this attack is mainly disable the network. As this attack prevents MANET from providing its services, so these types of attacks are more dangerous. However, detection of active attacks is very easy.

2.1.2 Passive attacks

A passive attack does not disable the normal flow and structure of the network. It attacks the MANET and tries to discover vulnerable information from that particular network [9]. The goal of these types of attack is not destroy the network, but to obtain sensitive information. As this attack does not interrupt or disable MANET network, its detection is not easy.

2.2 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 [10]. The host node responds by advertising its availability of fresh routes without checking routing table. Then attacker node reply to the host nodes, intercept the data packet and retain it [11]. In protocol based routing reply of a malicious node will be received before the reply of actual node [12]. Later malicious route will be created. It will interrupt the data traffic and will be dropped with data from the existing network. As in MANET each and every nodes stand 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 [14].

a. Single Black-hole attack.
b. Collaborative Black-hole attack.

2.2.1 Single Black-hole attack

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 be easily happened in MANET [15].

2.2.2 Collaborative Black hole attack

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 believes 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.

2.3 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 [18]. Jellyfish attack creates delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP [13]. Jellyfish attack can be three types [16].

a. Jellyfish delay variance attack.

b. Jellyfish Recorder attack.

c. Jellyfish periodic dropping attack.

In our research we have worked with jellyfish delay variance attack which creates delay in sending data traffic.

2.3.1 Jellyfish delay variance attack

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 ranges zero to ten seconds [17]. Such delay variance attacks

1. Can lead to increase collision and loss of important data of the network.

2. It can also cause blunder of available bandwidth for the delay based blockage protocol.

2.4 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 on the basis of 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

[19]. It also faster routing protocol as it finds out entire unidentified network and also for newer end which doesn’t exist on the navigation of that particular network.

CHAPTER 03

PROPOSED MODEL

3.1 Setup of OPNET Modeler

First we set our attributes for the simulation scenarios for our project. Some of the parameters were fixed and we changed some for simulating it on different criteria.

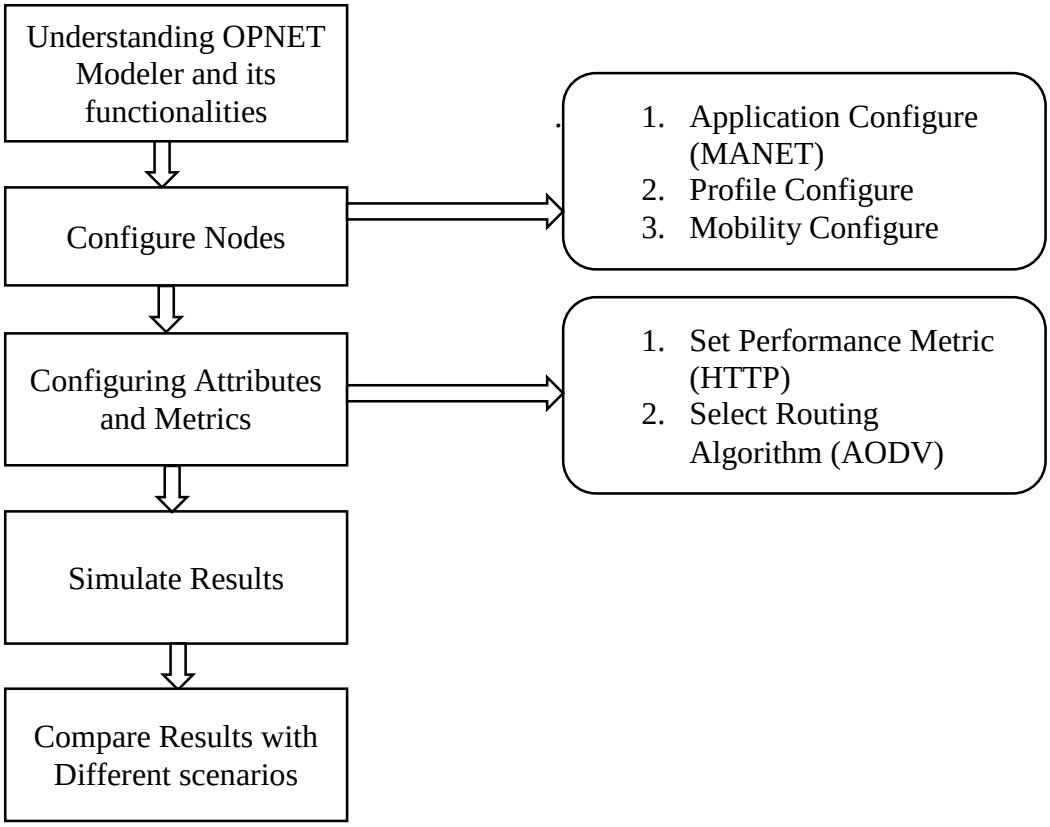

Figure 3.1: Proposed Model Diagram

3.2 Configure Nodes

We considered mobile nodes for the simulation. The mobility of the nodes were fixed. Protocol fixed as AODV throughout the network scenario.

3.3 Configuring Attributes

Attributes were set to match the simulation scenario for different areas and nodes varying the areas for area wise simulation and varying the amount of nodes for node wise simulation. Performance metric was set to HTTP protocol.

3.4 Calculating and Comparing Results

3.4.1 Calculating and comparing results for different areas vs. different nodes

Firstly we calculated the results for affected scenario for different areas. Then we compared the results for different nodes and observed the relation between varying area and nodes and to come up with equations to generate optimized network solution.

3.4.2 Calculating and comparing results for black-hole and jellyfish attack

We also compared the results of black-hole affected scenarios with jellyfish attack. From that we can come to know which attack is affecting which parameters of our network.

3.5 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 amount 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.

CHAPTER 04

EXPERIMENTAL ANALYSIS

4.1 Introduction

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 are 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 project we have analyzed the effects of the security attacks on different areas against different amount 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.

4.2 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 500m×500m, 1000m×1000m, 1500m×1500m, 2000m×2000m, 2500m×2500m.

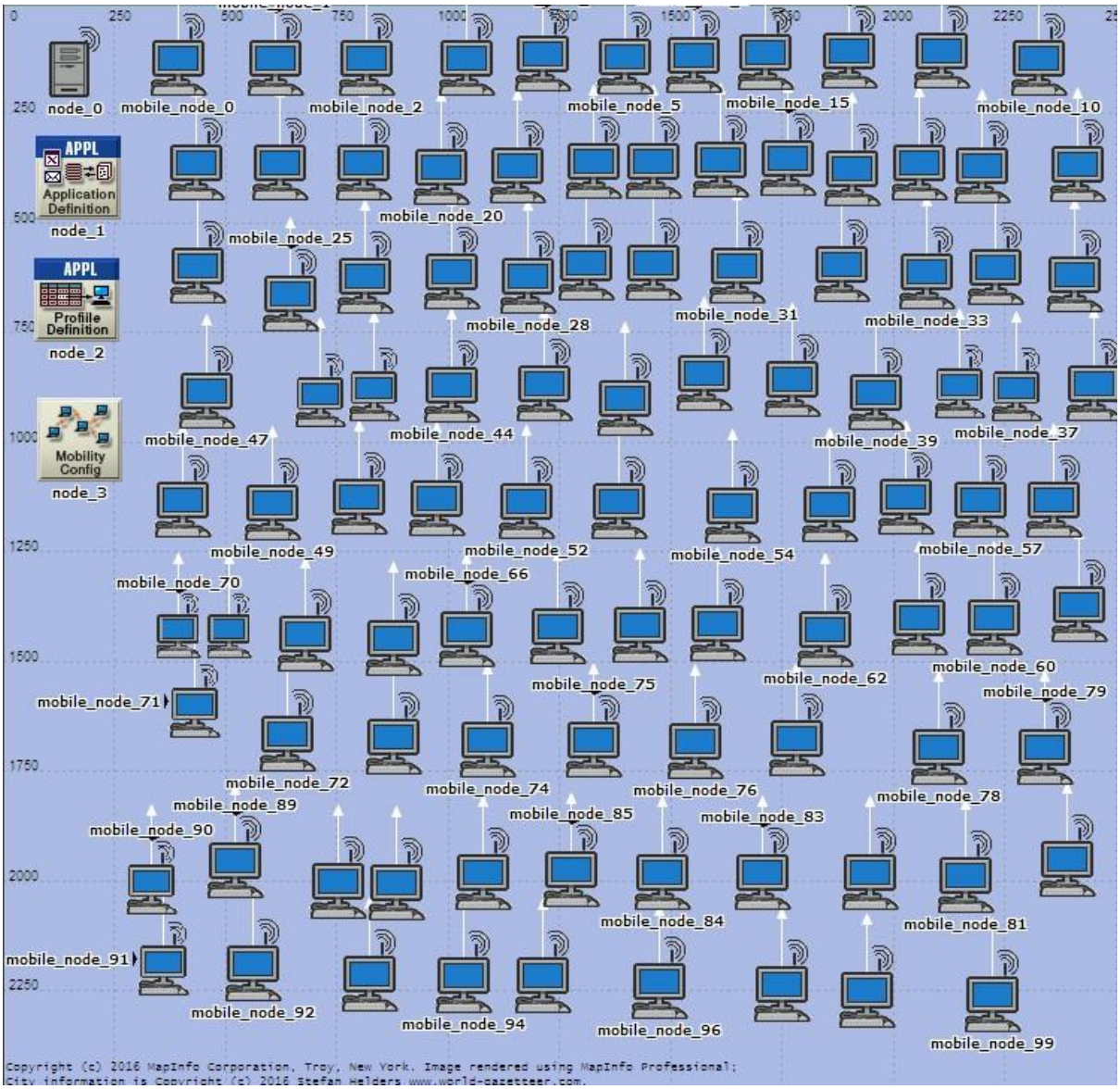

Figure 4.1: Network scenario for different areas of simulation

Figure 4.1 represents the scenario selected for this simulation. Here, we kept the number of nodes fixed to 100 and ran the project 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 were 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.

4.3 Environmental Setup for different nodes per simulation

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

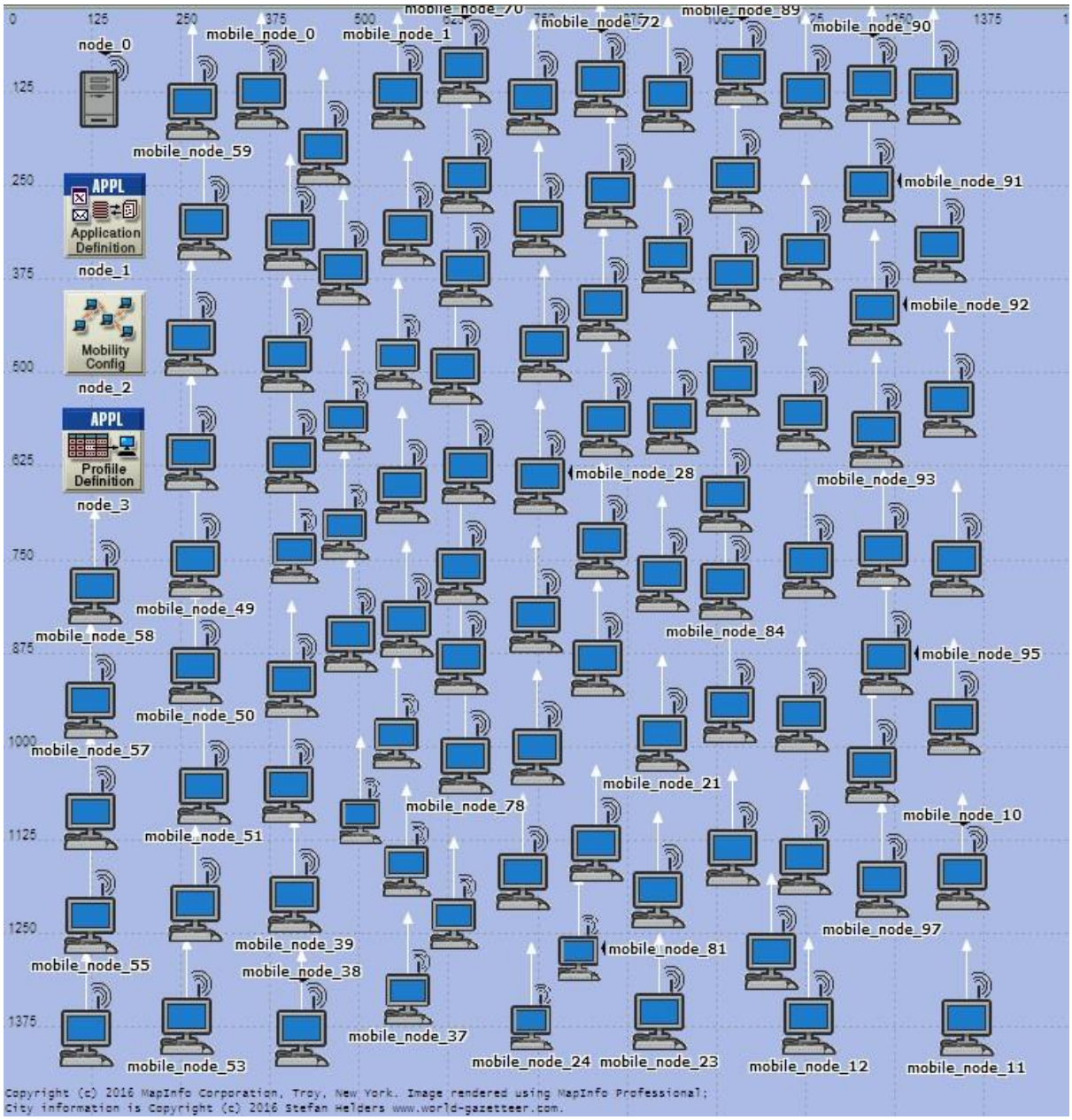

Figure 4.2: Network scenario for different node wise simulation

Figure 4.2 represents the network parameters and attributes selected for the simulations. For each simulation the numbers of nodes were changed. Simulation area was fixed to 1500m×1500m.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 were selected accordingly to compare the results against different areas of simulation.

4.4 Result Analysis

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

Figure 4.3 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.

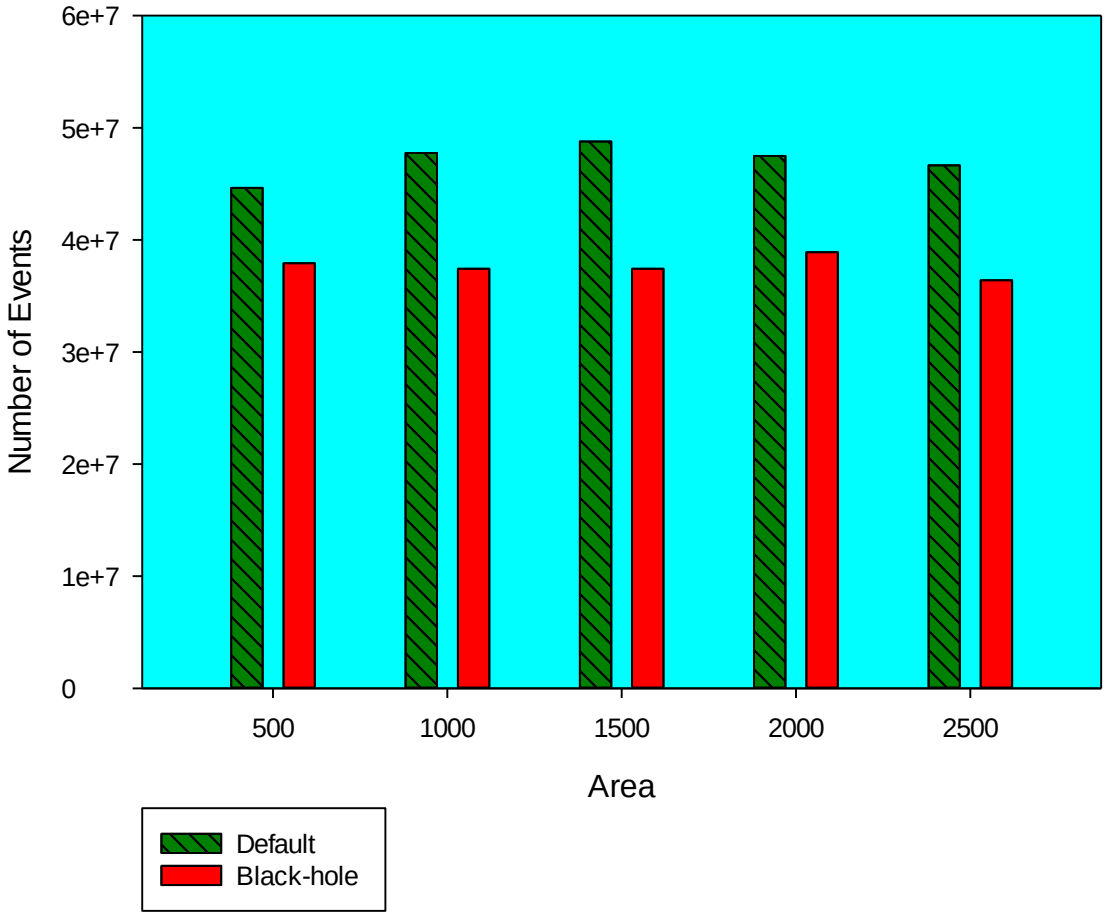

Figure 4.3: Impact of Black-hole Attack on Number of Events for Different Areas

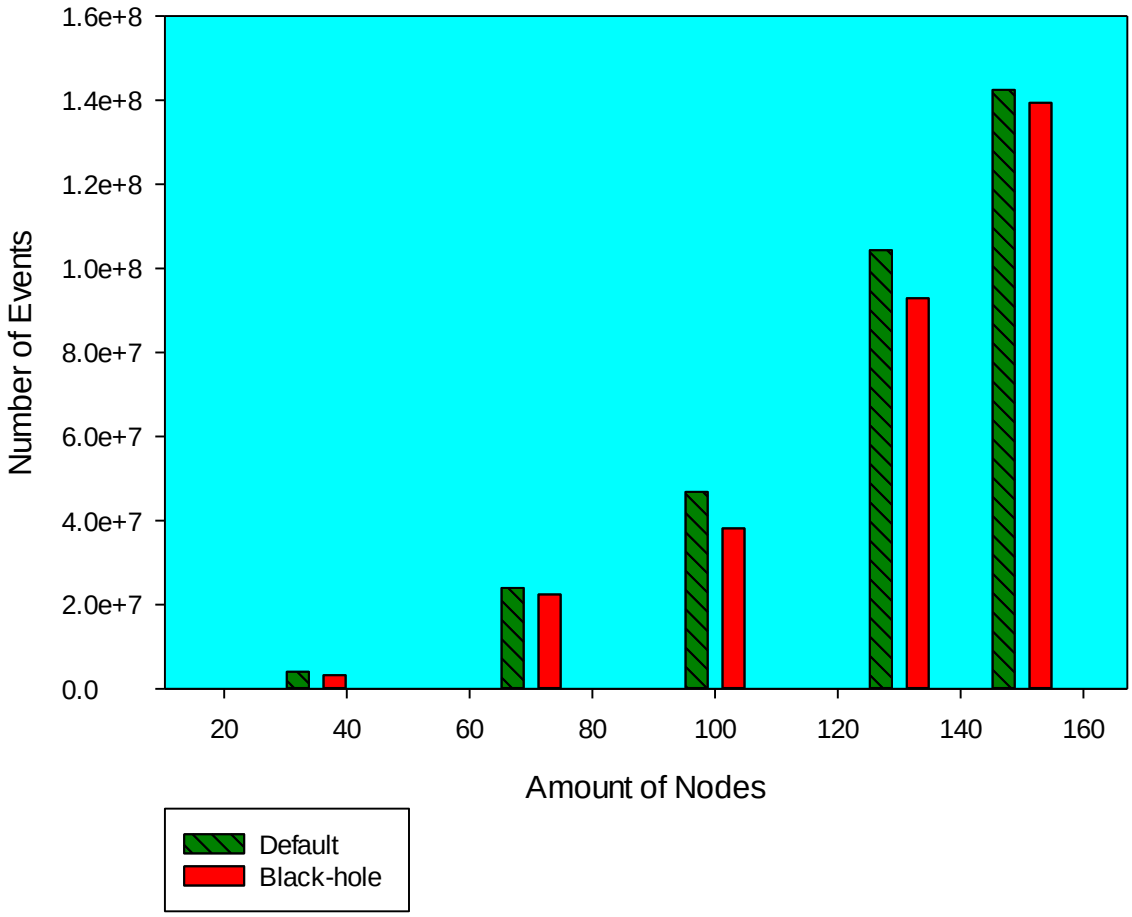

Figure 4.4: Impact of Black-hole Attack on Number of Events for Different Nodes

Similarly figure 4.4 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. So, from that we can explain, for black-hole attack, rate of change in area has greater impact than rate of change in amount of nodes. If we represent it with equation we can obtain,

$$\forall x \in B \left(\sum E(a) > \sum E(n)\right)$$

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 amount of nodes

4.4.2 Impact of Jellyfish on number of events for different areas and nodes

Figure 4.5 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.

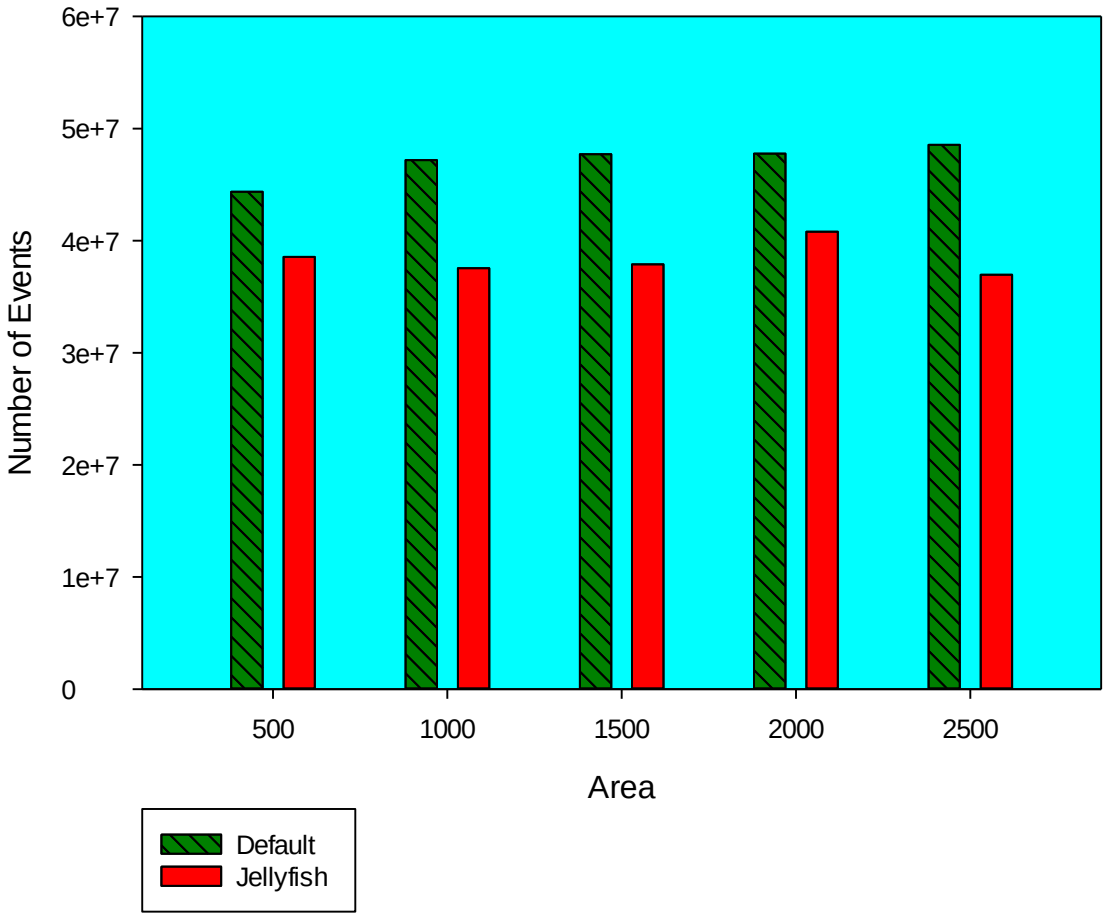

Figure 4.5: Impact of Jellyfish Attack on Number of Events for Different Area

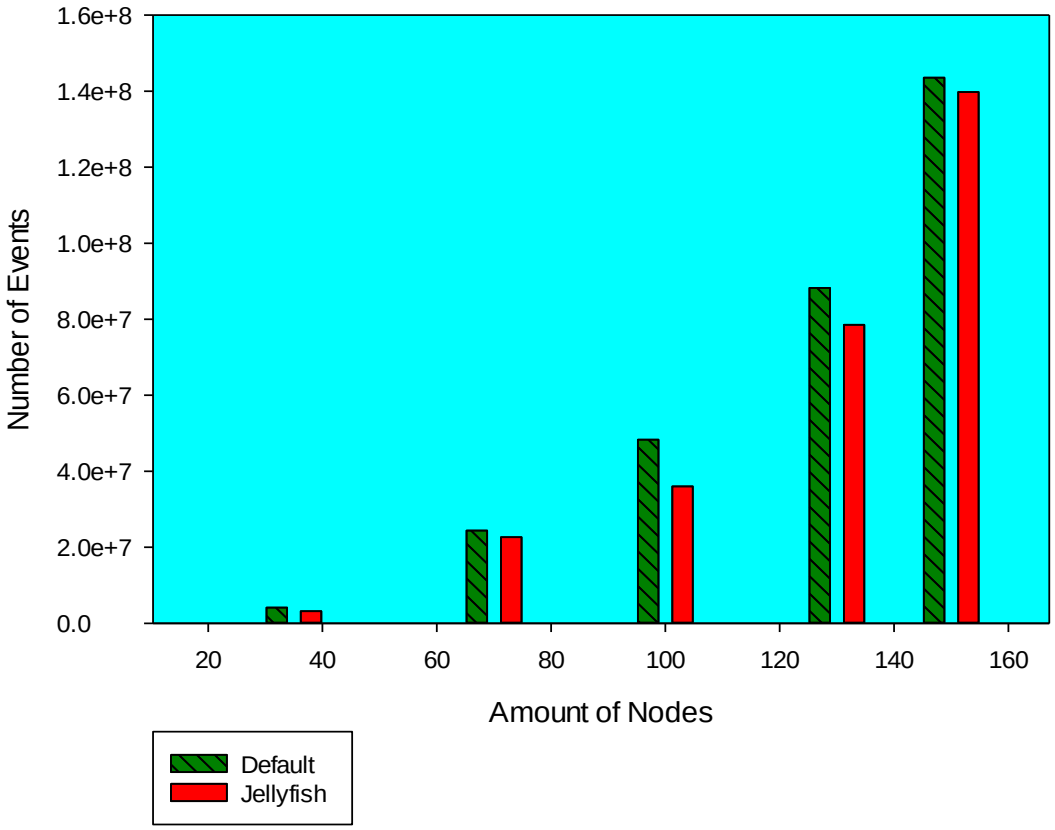

Figure 4.6: Impact of Jellyfish Attack on Number of Events for different nodes

Figure 4.6 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 is reduced much in rate in change area than rate in change of amount of nodes. Representing the result with equation we get,

$\forall x \in J \; (\sum (E(a)) > \sum (E(n)))$

Where,

J =Jellyfish attack

x = Network scenario

E= Reduction in number of occurred events

a = Rate of change in area

n= Rate of change in amount of nodes

CHAPTER 05

CONCLUSIONS AND FUTURE WORKS

5.1 Concluding Remarks

In this thesis, 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 amount of nodes. This project 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.

5.2 Future Works

The potential future directions for research based on the results presented in this thesis can be characterized into the following sections.

5.2.1 Improvised algorithm for network simulation

Exploring the characteristics of the security threats, improvised routing algorithms can be developed to avoid these issues.

5.2.2 Optimized Network infrastructure

Based on the research statistical data, optimized network can be formed analyzing suitable network area for a given amount of nodes and vice versa.

REFERENCES

1. Aarti, S.S.Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks". Department of computer science & Engineering, MRIU, Faridabad, India, VOL.3 Issue.5, pp.252-257, May 2013.
2. C. R. Davis "Security protocols for mobile ad hoc networks". McGill University Montreal,Quebec,Thesis submission, pp.1-134, August 2006.
3. N, Garg. R.P.Mahapatra, "MANET Security Issues". IJCSNS International Journal of Computer Science and Network Security, Vol..9 ,No.8, pp.241-246, August 2009.
4. Aarti, S.S.Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks". Department of computer science & Engineering, MRIU, Faridabad, India, VOL.3 Issue.5, pp.252-257, May 2013
5. R.K.Singh, R.Joshi, M.Singhal, "Analysis of Security Threats and Vulnarebilities in Mobile Ad Hoc Network (MANET)". International Journal of Computer Application [0975-8887], Vol. 68,No.4, pp.25-29, April 2013.
6. S.Hans, J Kumar, "A Review of Jellyfish Attack in MANET". International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 24, Issue.01, pp.191-195,May 2015.
7. M.N.Ahmed, A.H.Abdullah, A.EL-Syed, " A Survey of MANET Survivability Routing Techniques". Int. J. Communications, Network and System Sciences, pp176-185, April 2013.
8. N.Shukla, S.Gupta, A.Virmani, "Mobile Ad-Hoc Network (MANET): Security Issues Regarding Attacks". International Journal of Computer Applications (0975 – 8887), National Conference on Recent Trends in Engineering and Management "NCRTEM-2013",pp.16-18.
9. N.Shukla, S.Gupta, A.Virmani, "Mobile Ad-Hoc Network (MANET): Security Issues Regarding Attacks", International Journal of Computer Applications (0975 – 8887), National Conference on Recent Trends in Engineering and Management "NCRTEM-2013".
10. C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning," An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network". 24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp.775-780, April,2010.
11. K.Biswas and M.Ali, "Security threats in Mobile Ad-Hoc Network". Master

Thesis,Blekinge Institute of Technology, Sweden, pp.1-38,March 2007.

12. I.Ullah, S.U.Rehman,“Analysis of Black Hole attack on MANETs Using different MANET routing protocols”. Master Thesis,Blekinge Institute of Technology, Sweden, pp.1-38, September,2010.
13. S.Hans, J Kumar, “A Review of Jellyfish Attack in MANET”. International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 24, Issue.01, pp.191-195,May 2015.
14. C.Vu and A.Soneye,"An Analysis of Collaborative Attacks on Mobile Ad hoc Networks". Blekinge Institute of Technology, Sweden, pp.1-38,June 2009.
15. H. Changela, A. Lathigara, “A Survey on Different Existing Technique for Detectionof Black Hole Attack in MANETs”. International Journal of Science and Research, pp.415-419, Vol.4, Issue.1, January 2015.
16. S. Begum, "Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks".International Journal of Scientific & Engineering Research,Vol.3, Issue.3, pp.1-6, March 2012.
17. Hepikumar R. Khirasariya,“Simulation Study Of Jellyfish Attack In Manet (Mobile Ad Hoc Network) Usind Aodv Routing Protocol”. Journal Of Information, Knowledge And Research In Computer Engineering,Vol.02, Issue. 02,pp.344-347, NOV 12 TO OCT 13.
18. I. Aad and J.P. Hubaux, E.W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks”,IEEE/ACM Transactions on Netwroking,Vol.16,pp.791-802,Aug.2008.
19. M.Ali, Y.Sarwar, “Security Issues regarding MANET (Mobile Ad Hoc Networks):Challenges and Solutions”. Master Thsis, School of Computing Blekinge Institute of Technology, Sweden,pp.10-62, March 2011.