An Analysis of Collaborative Attacks on Mobile Ad hoc Networks

By

Cong Hoan Vu, Adeyinka Soneye
This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfilment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):
Cong Hoan Vu
Address: Folkparksvägen 19:08, 372 40 Ronneby, Sweden.
E-mail: vuconghoan@gmail.com

Adeyinka Soneye
E-mail: adso07@student.bth.se

University advisor(s):
Niklas Lavesson
School of Computing

School of Computing  
Blekinge Institute of Technology  
Soft Center  
SE – 37225 RONNEBY  
SWEDEN
ABSTRACT

A Mobile Ad hoc Network (MANET) consists of a set of communicating wireless mobile nodes or devices that do not have any form of fixed infrastructure or centralized authority. The security in MANET has become a significant and active topic within the research community. This is because of high demand in sharing streaming video and audio in various applications, one MANET could be setup quickly to facilitate communications in a hostile environment such as battlefield or emergency situation like disaster rescue operation. In spite of the several attacks aimed at specific nodes in MANET that have been uncovered, some attacks involving multiple nodes still receive little attention. A reason behind this is because people make use of security mechanisms applicable to wired networks in MANET and overlook the security measures that apply to MANET. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to clarify the characteristics of different multiple node attacks. This thesis addresses the aforementioned gap by providing a proper definition and categorization of collaborative attacks against MANET from the various multiple node attacks found.

Simulation using OPNET Modeler was used to investigate the performance impact of a collaborative blackhole attack on a mobile ad hoc network. Network throughput, packet delivery ratio and end-to-end delay are the performance metrics used in our result analysis.

Based on the analyses of performance metrics made, we realised the consequences of a collaborative blackhole attack on MANET. In order to prevent or reduce these consequences, we also discuss a number of mitigation plans to counteract the different kinds of collaborative attacks.

Keywords: MANET, Collaborative Attacks, Multiple Node, Blackhole.
ACKNOWLEDGEMENT

We greatly honour and say a thank you to our supervisor, Dr. Niklas Lavesson for his guidance, invaluable suggestions and huge endurance throughout our thesis period. He always provides welcoming hands and make himself reachable at all times.

We also thank the OPNET Technologies for their valuable provision of OPNET Modeler 14.5, the software licences and their technical supports.

--Cong Hoan Vu:

To my wife Anna Nguyen, my little son Felix Vu, without their love and sacrifice, I would not have completed this thesis.

All praises goes to my parents and my younger brother, their efforts and unconditional support are the eternal source of encouragement which keeps me stood firmly throughout my challenging but interesting studies.

I am also thankful to my friends for their moral support. A special thanks to Raja M. Khurram Shahzad, with his humorous stories, informal discussions, have taken me out of difficult time during this thesis.

--Adeyinka Soneye:

My profound gratitude goes to Almighty Allah, who in His infinite mercies and blessings gave me enough strength, courage and understanding to complete this glorious thesis. To my parents, my siblings and my wife, I say your prayers, supports, sacrifices and love were immeasurable to me not only during my thesis but all through studies. I greatly appreciate and adore you all.

I say thanks to my other relatives, loved one and friends; Johnsons, Babarindes, Osanyins, Phillips, Obalades, Omobos, Adelakuns, May Gulis, Hafeez, Folajimi, Chezz, Shodix, Raja, Imran, Bobby, Zack, BARYIS, to mention a few.

May God Almighty guide and bless us all. Amen!
# Table of Contents

ABSTRACT ..................................................................................................................... 1

ACKNOWLEDGEMENT ................................................................................................. 2

1: INTRODUCTION ...................................................................................................... 5

1.1 Problem Statement ................................................................................................. 5
1.2 Scope and aims ......................................................................................................... 6
1.3 Research Questions ................................................................................................. 6
1.4 Contributions .......................................................................................................... 6
1.5 Outline ...................................................................................................................... 7

2: BACKGROUND ...................................................................................................... 8

2.1 Related Work .......................................................................................................... 8

3: RESEARCH METHODOLOGY ............................................................................... 10

3.1 Overview ................................................................................................................ 10
3.2 Literature Survey .................................................................................................. 11
3.3 Theoretical Analysis ............................................................................................... 12
3.4 Simulation Modeling ............................................................................................... 12
3.5 Result Analysis ...................................................................................................... 13

4: COLLABORATIVE ATTACKS ................................................................................. 14

4.1 Security Issues in MANET .................................................................................... 14

4.1.1 Passive vs. Active attack ................................................................................... 14
4.1.2 Internal vs. External attack .............................................................................. 15

4.2 Multiple Node Attacks ..... .................................................................................... 16

4.2.1 Blackhole attack ............................................................................................... 16
4.2.2 Wormhole attack ............................................................................................. 16
4.2.3 Sybil attack ...................................................................................................... 17
4.2.4 Routing table overflow attack .......................................................................... 17

4.3 Definition of a Collaborative Attack ..................................................................... 18

4.4 Categorization of Collaborative attacks ............................................................... 18

4.4.1 Direct Collaborative Attacks .......................................................................... 18
4.4.2 Indirect Collaborative Attacks ......................................................................... 19

5: SIMULATION MODELING ..................................................................................... 20

5.1 Explanation of Simulator/Modeler ......................................................................... 20

5.2 MANET in Simulator ........................................................................................... 20

5.2.1 MANET model limitations .............................................................................. 21

5.3 Simulation Modeling Workflow ............................................................................ 21

5.3.1 System .............................................................................................................. 22
5.3.2 Assumptions document .................................................................................. 22
5.3.3 Simulation program ......................................................................................... 22
5.3.4 Simulation results ............................................................................................ 22
5.3.5 Results used in analysis and evaluation .......................................................... 23

5.4 Performance Metrics ............................................................................................. 23

5.4.1 Network throughput ......................................................................................... 23
5.4.2 End-to-end delay ............................................................................................... 23
5.4.3 Packet delivery ratio ......................................................................................... 23

5.5 Simulation Model ................................................................................................... 23

5.5.1 Setting up the simulation ................................................................................ 24
5.6 Simulation Results ................................................................................................. 25
5.6.1 Scenario 1: 11-Node MANET Network .......................................................... 25
5.6.2 Scenario 2: 30-Node MANET Network ....................................................... 27

6: ANALYSIS ................................................................................................. 30
6.1 Scenario 1 ......................................................................................................... 30
6.2 Scenario 2 ......................................................................................................... 31
6.3 Scenario 1 vs. Scenario 2 ................................................................................ 32

7: MITIGATION .......................................................................................... 33
7.1 Mitigation for Direct Collaborative Attacks .................................................. 34
7.2 Mitigation for Indirect Collaborative Attacks ............................................... 35

8: CONCLUSIONS AND FUTURE WORK ........................................... 36
8.1 Conclusions ................................................................................................. 36
8.2 Future Work ............................................................................................... 36

REFERENCES ............................................................................................ 38

LIST OF FIGURES

Figure 3.1: Overview of Research Methodology .................................................. 11
Figure 3.2: Way to study a system .................................................................... 12
Figure 4.1(a): Passive attacks ......................................................................... 15
Figure 4.1(b): Active attack .............................................................................. 15
Figure 4.2: Internal vs. External attack ............................................................... 15
Figure 4.3(a): Blackhole attack ....................................................................... 19
Figure 4.3(b): Wormhole attack ...................................................................... 19
Figure 5.1: Classification of Ad hoc Routing Protocol ..................................... 21
Figure 5.2: A valid, credible and appropriate simulation model workflow .......... 22
Figure 5.3: Simulation Workspace with selected mobile nodes (1500x1500) .... 25
Figure 5.4: Throughput of 11-node MANET Network ..................................... 26
Figure 5.5: Packet Delivery Ratio of 11-node MANET Network ....................... 26
Figure 5.6: End-to-End Delay of 11-node MANET Network ......................... 27
Figure 5.7: Throughput of 30-node MANET Network .................................... 28
Figure 5.8: Packet Delivery Ratio of 30-node MANET Network ....................... 28
Figure 5.9: End-to-End Delay of 30-node MANET Network ......................... 29

LIST OF TABLES

Table 6.1: Data of 11-Node MANET Network .................................................. 31
Table 6.2: Data of 30-Node MANET Network .................................................. 32
1: INTRODUCTION

During the past few decades the world has become a global village by virtue of the technological revolution. Information Technology (IT) is growing day-by-day. Businesses tend to use more and more complex network environments. Despite the efforts of network administrators and IT vendors to secure the computing environments, the threats posed to personal privacy, company privacy and various assets by attacks upon networks and computers continue unabated. The Mobile Ad hoc Networks (MANETs) are most certainly a part of this technological revolution. A MANET is a collection of wireless devices or nodes that communicate by dispatching packets to one another or on behalf of another device/node, without having any central network authority or infrastructure controlling data routing. MANET nodes have limitless connectivity and mobility to other nodes routing, each node acts as a router and network manager to another node [17].

Having a secured transmission and communication in MANET is a challenging and vital issue due to the fact that there are various types of attacks that the mobile network is open to. In order to secure communication in such networks, understanding the liable security attacks to MANET is a great task and concern. MANETs suffer from a variety of security attacks and threats such as: Denial of Service (DoS), flooding attack, impersonation attack, selfish-node misbehaving, routing table overflow attack, wormhole attack, blackhole attack, and so forth. MANET is open to vulnerabilities as a result of its basic characteristics like: no point of network management, topology changes vigorously, resource restriction, no certificate authority or centralized authority, to mention a few [1, 2, 4].

Previous studies show that there are different categories of attacks on MANET [1, 2, 8] such as Passive and Active attacks, Internal and External attacks and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are referred to as attacks on multiple nodes and are malicious. In this thesis, we make investigation on the multiple node attacks against MANET and provide a new categorization of multiple node attacks. In addition, based on the characteristics of these attacks, we will present a proper definition of such attacks in MANET. After that, the simulations of different network sizes are performed to see the impact on MANET’s performance with and without collaborative attack. Finally, the various mitigation plans for collaborative attacks are discussed and highlighted.

1.1 Problem Statement

Studies on MANET have focused more on single attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are unanticipated and combined attacks. There have been no proper definition and categorization of these kinds of attacks (multiple node attacks) in MANET. Some mitigation plans have been proposed to counteract against some form of multiple node attacks; thus, there is need to figure out the consequences of the category of collaborative attacks and their possible mitigation plans. Moreover, the effects of these kinds of attacks on MANET have not been well measured since each researcher tends to use different simulators to visualize those attacks and determine the consequences such as impact on packet delivery ratio, throughput, and end-to-end delay.
1.2 Scope and aims

Based on the features related to MANETs and the cause of problems and vulnerabilities in such networks, our study on MANET has focused more on non-single attacks and some kinds of attacks involving multiple nodes. We have not been able to find any proper definition and categorization of this kind of attacks in MANET. This issue is our main focus in the thesis. In addition, there is a need to figure out the consequences of this category of attacks and their possible mitigation plans.

There are several types of multiple node attacks. We discuss a number of them based on their characteristics and we will show that it is possible to categorize four multiple node attacks as collaborative attacks. In our simulation experiment, we focus on the blackhole attack and its impact on MANET. We did not implement other types of collaborative attack because of the time constraints. We also did not simulate mitigation plans but we provide a list of possible mitigation plans against collaborative attacks in MANET.

The aim of this thesis is to analyze collaborative attacks against MANET. In order to achieve this aim we establish the following objectives:

- A generic definition of collaborative attacks and a categorization of possible collaborative attacks on MANET.
- Experimental measurements of some important performance metrics of MANET such as throughput, end-to-end relay and packet delivery ratio.
- A list of suitable mitigation plans to combat collaborative attacks against MANET.

1.3 Research Questions

We will answer the following research questions in this thesis:

**Question 1:** Which types of collaborative attacks can be launched against MANET?
Within the context of this thesis, our focus is to investigate different kinds of multiple node attacks that can be classified as collaborative attacks.

**Question 2:** What are the consequences of collaborative attacks against MANET?
Another contribution of this research work is to measure the performance impact of MANET under normal operation and under a specific collaborative attack.

**Question 3:** Which are the previously proposed mitigation plans to combat the attacks on MANET and which of these plans can be used to combat collaborative attacks on MANET? Theoretically, we analyze previously proposed mitigations plans and then we determine which plans are liable to prevent or mitigate the collaborative attacks.

1.4 Contributions

Our research may help in understanding the various types of collaborative attacks on MANET and provide a broad understanding of how such attacks could be defined and categorized. In this thesis, we visualize and measure the impact of collaborative attacks on MANET. Finally, our research evaluates the mitigation plans that can be used to combat collaborative attacks. In other words, the presented results of this research would give way for further researches on different kinds of collaborative attacks against MANET or aid to identify other directions that can give further results.
1.5 Outline

The first chapter introduces the mobile ad hoc network and we state the thesis scope, aims and objectives. We also present the research questions and give an explanation of how we intend to address the research questions. Chapter 2 then provides a detailed background of the possible security attacks against MANET. We analyze the weaknesses in MANET as well as the reason behind MANET being vulnerable. Some multiple node attacks are highlighted along with some mitigation plans proposed to combat the security attacks.

In chapter 3, we explain the research methodology used to conduct this study. This is followed by chapter 4, which contains the theoretical analysis made on multiple node attacks, collaborative attacks and their categorization. In chapter 5, we present our simulation modeling of blackhole attack against MANET, while in chapter 6, we analyze the results. In chapter 7, we discuss the mitigation plans against attacks on MANET in general and later discuss mitigation plans against collaborative attacks in particular. Finally, chapter 8 concludes our thesis and provides pointers to future work.
2: BACKGROUND

MANET is a rising research area with many practical applications. Its technology provides a flexible way to set up communications in situations with geographical constraints that demand distributed networks without any centralized authority or fixed base station, such as: disaster relief, emergency situations (rescue team), battlefield communications, conference rooms and military applications [1]. Typical examples of practical applications of MANET are: developed sensor networks that have several low-powered nodes with sensing resources usually used by the military in battlefields [1, 13]. Flexible mobile network set up for rescue operation of hurricane Katrina on August 29, 2005 close to New Orleans and the rescue operation after the September 11, 2001 attack in New York, USA where large network parts were destroyed [4] are practical applications as well.

Compared to the traditional wireless and wired networks, MANET is prone to larger security vulnerabilities and attacks because of certain features of MANET like no centralized authorities, distribution cooperation, open and shared network wireless medium, severe resource restriction, and high dynamic nature of network topology [1, 2]. These factors have made MANETs to receive great attentions and also because of their capabilities of self-configuration and self-maintenance. Another unique feature of MANET that poses security threats is its unclear defence line; i.e. no built-in security. MANET does not have dedicated routers and switches, its nodes usually operate by forwarding the packets to one another thereby having no security in the communication; granting access to both legitimate users and attackers [2].

2.1 Related Work

Many studies on MANET focus on the protocols used, their security issues such as data encryption, authentication, trust, cooperation among nodes, attacks on the protocols and proposed solutions or preventions, cf. [2-5, 8, 12]. Most ad hoc routing protocols such as Optimized Link State Routing (OLSR) protocol [3], Ad hoc On-Demand Distance Vector (AODV) routing protocol [12], Micro-mobility support with Efficient Handoff and Route Optimization Mechanisms (MEHROM) protocol [4, 5] and wireless MAC protocols, like the 802.11 [6] usually make assumptions about suitable and trusted environments, giving room for malicious activities and attackers. Distributed protocols like the link-layer protocols and network-layer protocols used in multi-hops wireless (MANET) channels communication assume that the nodes are cooperative in the synchronization process. However, these assumptions are usually untrue in a harsh environment. Attackers can interrupt the network by violating the protocols requirement because MANET assumes trust and cooperation; it does not enforce node cooperation [2, 12].

Despite of the different specific attacks on MANET such as Denial-of-Service (DoS), impersonation, Node hijacking and so on that have been exposed [7, 8], the attacks involving multiple nodes seem to have received little attention. One of the possible reasons could be that most researchers tend to adopt ideas about security measures from wired networks to ad hoc networks and forget that security issues regarding MANET are more complicated since MANET is unable to rely on pre-existing infrastructure. In other words, all nodes are communicating without a central authority or base station to keep a network connected. Therefore, the existing security solutions for wired network cannot be directly applied to the MANET [2].

In a blackhole attack [9], several malicious nodes falsely claim a new route to the destination in order to absorb all packets coming from the source. To combat this kind of routing protocol attack, Hongmei et al. proposed a solution that revolved around waiting and
checking the replies from all other neighbouring nodes and then deciding on the safe route [1]. In other words, this solution has some problems and limitations since it increases the delay time and reduces the efficiency in the whole network. Using a fidelity table is another solution, in which every node will be assigned a fidelity level and the node with “0” level will be considered as malicious and be eliminated from the MANET [9]. Distributed Denial of Service (DDoS) attack is another kind of attack on multiple nodes; it is because of the nature characteristic of this attack. DDoS attack involves breaking into hundred or thousand of machines and from those machines, attacker launches several attacks aim at target machine in order to consume bandwidth and create bottleneck in the network [10]. To mitigate this attack, a framework for statistical filtering that uses a cluster-based approach has been proposed in [11]. The statistical filtering framework gathers set of packet statistics such as source and destination IP addresses, time to live (TTL), protocol types, etc that are used but this method of combating DDoS attack against MANET does not offer a completely guaranteed solution; yet offers a good defence mechanism against DDoS attacks [11].

Basic vulnerabilities in MANETs have been researched previously [1, 2, 4], ranging from their open network medium, severe resource restriction, selfishness, dynamic nature, to vulnerabilities in some protocols. In addition, there are different categories of attacks against MANET [1, 2, 8]. These categories in pair are Passive and Active attacks, Internal and External attacks and the two categories of network-layer attacks: Routing attacks and Packet Forwarding attacks [1, 2, 8]. Our research area on attacks against MANET provides not only the consequences of collaborative attacks but also their mitigation in MANET and attack categorization. From our perspectives, collaborative attacks are non-single attacks; they are attacks launched in multiple malicious nodes acting as a group. Typical examples of these kinds of attacks are Blackhole attack, Sybil attack and Wormhole attack on nodes in a MANET.
3: RESEARCH METHODOLOGY

3.1 Overview

Research methodology defines the research activity, development of research activity and measurements used to advance the research work by implementing these measures which assist to achieve author’s goal [14]. There are 3 approaches used to conduct a research, one can choose among qualitative, quantitative or mixed approach [14]:

- **Quantitative approach:** is an approach that makes use of strategies of investigation such as simulation modeling or a survey in order to gather the statistical data (i.e. the output data collected from simulation or survey result) for analysis. This approach tends to be used for research in which the author wants to test or verify theories or explanations, or to observe and measure information numerically.

- **Qualitative approach:** Alternatively, in this approach, the researcher usually makes use of knowledge claims which are based on a constructivist perspective, a participatory perspective or both. A qualitative approach uses strategies of inquiry like ethnographies, grounded theory and phenomenology. This approach can be used for research in which the author wants to study the context or setting of participants, or to focus on single concept or phenomenon.

- **Mixed approach:** in which the researcher prefers to base knowledge claims on matter-of-fact grounds. This approach employs strategies of inquiry that require gathering data either concurrently or consecutively to best understand research problem. The mixed approach can be used when the researcher wants to collect both qualitative and quantitative data or integrate the data at different stages of inquiry.

In this thesis, we opted for a quantitative approach. The main reason for choosing this approach is based on that we are not only going to define and categorize collaborative security attacks in MANET, but we are also going to make use of simulation modeling to identify the performance impact in MANET under a collaborative attack as well as which mitigation plans can be used to alleviate this kind of attack. Therefore we designed this research using 5 systematic phases. During the starting phase, we perform Literature Survey; the information gained in this phase will play important inputs for Theoretical Analysis (Defining and Categorizing Collaborative Attacks), Simulation Modeling, Result Analysis and Evaluation of Mitigation Plan phases. The following figure 3.1 will illustrate these phases we have employed in the research.
3.2 Literature Survey

The literature survey provides a framework for establishing the importance of the study. Within the context of a quantitative research approach, the literature survey occupies a substantial amount of time and effort. It provides direction for the research questions and hypotheses [14]. To understand the current security issues regarding MANET, the literature survey was the essential starting step, which helped us gain in-depth knowledge about different security threats related to MANET. Our literature survey helped us to understand that multiple node attacks on MANET have received a little attention from research community in terms of properly defining and categorizing such attack. We started to formulate problem, and then defined distinct keywords relevant with the topic in order to search the most recent materials produced by researchers.
3.3 Theoretical Analysis

Research and theories related to the multiple node attacks and their characteristics are carefully examined. Based on our analyses on available theories and research, we construct a definition of collaborative attacks and their categorization. The theoretical analysis helps in finding out various kinds of attacks that are in fact multiple node attacks. Based on these findings, we were able to analyze some of the attacks that we categorize as being collaborative. We examine the attacks in light of the correspondence of their behaviours and symptoms.

3.4 Simulation Modeling

To visualize and measure the impact of a collaborative attack on MANET (which can be referred as a system), we need to develop a simulation in which a model of the system will be created using OPNET (a computer software program/modeler) to evaluate the model numerically. With this simulation, output data are gathered to estimate the required model’s characteristics [15]. The way to study a simulation system is illustrated in figure 3.3 below:

![Figure 3.3 - Way to study a system](adapted from figure 1.1 [15])

Roughly speaking, figure 3.3 can be explained as follows. To simulate a system and understand how the system behaves in different conditions, we have two choices; the first is to experiment with the actual system. This is costly and unsuitable in our case. The second option is to experiment with a model of the system (mimicking the real system). We opted for the latter choice because of expenses and it is unsafe to use real systems for such an experiment. The model of the system can be built based on a physical model (iconic model) or mathematical model. To build an iconic model in our case is not a suitable choice since it is rather complicated to build a security attack on MANET using an iconic model. Thus, we choose to use the mathematical model. Normally, a vast majority of models built to run on the computer are mathematical models, used in place of a system in terms of logical and
quantitative relationships, then manipulated and changed according to a set of assumptions to see how the model reacts, and therefore how the system would react in the same condition. Our mathematical model is indeed too complicated to use analytical simulation to fully explain why it reacts to various conditions; instead we used discrete-event simulation in which several inputs (parameters) can be used to numerically exercise the model to see how they affect the performance output [15].

3.4 Result Analysis

Normally, a great deal of money and time are devoted on model programming and development, but just a little effort is made to analyze the output data which were rendered from simulation output [15]. In this thesis, we put much effort to study and analyze the output data in systematic way and then to compare the behaviour of MANET under regular condition and MANET under a collaborative attack.
4: COLLABORATIVE ATTACKS

4.1 Security Issues in MANET

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is more susceptible to be attacked by inside the network while comparing to other type of networks. Practically, MANET could be attacked by several ways using multiple methods; before going to deeper investigation, it is necessary to classify security attacks within the context of MANET.

The classification can be based on the behaviour of the attack (Passive vs. Active), the source of the attacks (Internal vs. External), the processing capacity of the attackers (Wired vs. Mobile) and the number of the attackers (Single vs. Multiple) [8, 21]. We choose these attack classifications because they are applicable to the collaborative attacks we are categorizing. We illustrate further on the latter two as the collaborative nature of the attack could take any of the methods.

4.1.1 Passive vs. Active attack

Typically, passive attacks aim to steal valuable information in at least two communicating nodes (as illustrated in Figure 4.1(a)) or even in the whole network. There are many variations of passive attacks, but in MANET, there exist two types: eavesdropping and traffic analysis. Practically, depending on situations, passive attacks can be considered as legitimate or illegitimate actions. If the purpose is benign, for example, if the administrator wants to use some tools to probe the network traffic, in order to troubleshoot or account the network then it is legitimate. On the contrary, if the purpose is malicious, one attacker can steal valuable information by probing the network traffic such as credit card information, credential email, and then use the information to illegally withdraw money from bank accounts or blackmail the victims.

Roughly speaking, passive attacks do not intend to disrupt the operation of the particular network, but active attacks are able to alter the normal network operation [23]. Typical example of active attacks can be: masquerade attack, replay attack, modification of message (illustrated in Figure 4.1(b)) and Denial of Service (DoS).
4.1.2 Internal vs. External attack

As the name implies, external attacks are launched by attackers who physically stay on outside of the attacked network. These attacks usually aim to deny access to specific function in the network (i.e. http traffic), or to cause network congestion or even to disrupt the whole network. While external attacks would be difficult to be launched if the network was properly configured and protected, the internal attacks are much tougher to defend against. One of the reasons is because we tend to protect the network from being attacked by outsiders rather than insiders. Also because of the fact that an external attack can easily be traced compared to the internal attack.
As illustrated in figure 4.3, one external attacker node can hijack an internal node, and then control the internal node to attack other nodes in MANET. Therefore, an external attack can become an internal attack and the consequence of the attack would be more serious. Therefore, there exist two types of internal attacker nodes, one is the compromised node, which was discussed above, and the other one is the misbehaving node, which is authorized to access the system resources but fail to use them according to the way it should be used [23]. Attacks caused by these internal misbehaving nodes are difficult to detect, for example, selfish attack in which the node is unwilling to consume battery power, CPU cycles or network bandwidth to forward uninterested packets, even though it expects other nodes to forward packets for it.

4.2 Multiple Node Attacks

4.2.1 Blackhole attack

A blackhole attack occurs when a malicious node impersonates the destination node or forging route reply message that is sent to the source node, with no effective route to the destination. The malicious node may generate unwanted traffics and usually discards packets received in the network [17]. When this malicious node (blackhole node) has effects on one or more nodes, making them malicious as well, then this kind of attack can be referred to as multiple node attack or collaborative attack.

In a blackhole attack, the malicious node presents itself as having the shortest path to the node it is impersonating, making it easier to intercept the message. To achieve this, the malicious node waits and tries to get the replies from nearby nodes in order to discover a safe and valid route [9]. This route could be forged, illegitimate or an imitation but it appears genuine to the source node.

4.2.2 Wormhole attack

A wormhole attack is an attack in which the attacker provides two choke-points that are used to degrade the network or analyze traffic as preferred any time. False impressions are used in creating these choke-points with two or more nodes joint together [24]. In other words, wormhole attack creates a tunnel that records traffic data (in bits or packets) at one network place and channels them to another place in the network. This kind of attack is usually against many ad hoc routing protocols and the attacker is hidden at higher layers; thus the wormhole and both colluding attacker nodes at each choke-point of the wormhole are invisible in the MANET route [25].

There are different adaptations of wormhole attack where in-band and out-of-band wormholes are the two main variations [24]:

- **In-band Wormhole**
  This method of wormhole attack builds up a secret overlay tunnel within the active wireless medium. In-band wormhole could be more dangerous than out-of-band wormhole because it does not have any need for an extra hardware device or node and it also utilizes the existing communication medium in its routing. Self contained wormhole and extended in-band wormhole are two types of in-band wormhole. The self-contained wormhole promotes a false link connecting the attacker nodes while the extended in-band wormhole promotes its fake link between two nodes, which are none attacker nodes. The latter type produces a wormhole that goes further than the attacker nodes, thus creating the end choke-points.
- **Out-of-band Wormhole**
In this variation of wormhole, the attacker nodes create a direct connection linking the two choke-points. This established link is an external link that could be wired or a kind of wireless medium. One end of the connection is used to accept packets while it is forwarded using the second end of the connection, thus giving room for huge amount of data to be transmitted through the wormhole.

### 4.2.3 Sybil attack

A Sybil attack is a situation where a malicious node acts like two or more nodes rather than just a node like previously mentioned attacks. The Sybil nodes are created by series of false identities, imitations, or impersonation of nodes in a MANET, and these additional node identities could be generated by just a physical device. There exist three proportions of launching a Sybil attack [7]:

- **Direct or Indirect Communication**
In direct communication as the name implies, Sybil nodes get in touch with the benign nodes directly. One of the malicious tools of the Sybil node listens to messages sent from benign node to the Sybil node and messages sent by the Sybil node are done from this malicious tool. On the other hand, indirect communication between a benign node and a Sybil node is done using a malicious node as an intermediary, not a malicious tool within the Sybil node as in the case of direct communication.

- **Stolen or Fabricated Identity**
The two alternatives a Sybil node uses to get a node’s identity to itself are either by stealing the identity of a benign node or by fabricating a fresh identity it uses. Stolen identity by a Sybil node seems to be the easier method here because this can be best achieved by using node impersonation. Unlike fabrication of identity that can be hard or complicated, for example, the range of identities of benign nodes may be restricted with the aid of some security measures. Another example is that; there could be need to generate random 32 or 64 bit integer number for an identifier because it depends on whether the network is using 32 bit or 64 bit identifiers for its mobile nodes.

- **Simultaneous or Non Simultaneous**
In the simultaneous proportion of launching Sybil attack, the attacker endeavours to launch all available node identities at once or one after the other in the MANET. In this case, a hardware or node entity may act as an identity at one time then it may still rotate or move through other identities to make them appear at concurrently. On the other hand, the non simultaneous way of launching Sybil attack uses some identities of node in a period of time and another set of node identities in the next time period. Attackers can swap node identities if they have many compromised malicious nodes, in order to stay invisible and undetected.

### 4.2.4 Routing table overflow attack

This is the kind of multiple node attack that sends non-existent node data into the MANET and also tries to degrade the rate at which new updates are made into the routing table [26]. This kind of attack is aimed at flooding or disrupting the routing node of the victim with non-existent node data and it usually occurs against proactive routing protocols like OSPF and OLSR. Proactive routing protocols use periodic updates of routes even before they are required to transpire and this make them vulnerable to routing table attack. On the contrary, reactive routing protocols only produce a route when it is required, thus it is not vulnerable to routing table overflow attack [7].
In other words, routing table overflow attack is when an attacker tries to make routes to some non-existent nodes, in order to produce sufficient routes and thwart new routes from being produced [7]. Thus, this is also used to overpower the protocols implementation or leads to denial of service attack on MANET.

4.3 Definition of a Collaborative Attack

A collaborative attack in MANET is a homogeneous attack (i.e. blackhole or wormhole attack), involving two or more colluding nodes; classified as internal active attack that can be processed using wired or wireless link and triggered by single or multiple attackers. It can also be referred to as the first level of attack, in which the adversary only interests in disrupting the foundation mechanism of the ad hoc network, for instance routing protocol, which is crucial for proper MANET operation.

4.4 Categorization of Collaborative attacks

In collaborative attacks, as defined in the previous section, there are numerous nodes involved during the attack. These nodes can be physically existent or not existing at all. These unique characteristics can be observed and were distinguished in the section on Multiple Node Attacks. After the study of different multiple node attacks, and then provided the definition of collaborative attacks, we are now going to categorize these attacks into two different categories.

4.4.1 Direct Collaborative Attacks

Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. Blackhole and Wormhole attacks belong to this category. The reason for this classification is based on the nature behaviour of these attacks. In the blackhole attack, one or more malicious nodes try to disrupt the network routing operation by advertising itself as the shortest path to the destination node. Therefore, there will be at least three physical nodes must be involved in this attack, namely: the source node, blackhole node (malicious node) and the destination node. As illustrated in figure 4.3(a), Node S wants to send data packets to Node D; it will first broadcast the RREQ (Route Request) to the neighbouring nodes. Node B1 and B2 are blackhole nodes and then also received RREQ from source node. These malicious nodes will immediately send out the RREP (Route Reply) to claim that it is the shortest path to destination node D. The RREP from B1 and B2 will reach the source node before other nodes, thus the source node S start transmitting data packets. On the receipt of data packets, B1 can either simply drop them or forward them to B2, and then B2 may simply drop or forward the data packets. Finally, little or no data packet can reach the intended destination node D.

The second attack belonging to this category is the wormhole attack; there always exists two colluding malicious nodes, since they can tunnel data packets back and forth even packets not addressed to them without being known by other nodes. Thus, the wormhole attack involves at least two physical nodes. In Figure 4.3(b), two malicious colluding nodes 5 and 6 can tunnel data packets to each other to analyse and tamper the network by using either a wired link or a long-range wireless medium.
4.4.2 Indirect Collaborative Attacks

The attacks in this category use different non-existent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attacks can be referred to as indirect collaborative attacks. The attacker nodes are not already in existence in the original network but created along the line of their attack. Sybil attack belongs to this category of collaborative attacks. The malicious node in Sybil can generate arbitrary number of additional identities for itself while using only one physical node. This physical node may be a legitimate node or an already compromised or malicious node by Sybil attack in the MANET.

Routing table overflow is another attack in this category in which the malicious node tries to create as much as possible routes to non-existent nodes. It aims to prevent new routes from being produced or to overpower the routing protocol.
5: SIMULATION MODELING

A Mobile Ad hoc Network (MANET) is a multi-hop wireless network, which operates in some varying and constraint conditions without setting up a fixed network infrastructure. Simulating and analyzing a MANET is a task that is wearisome and monotonous. It requires prudent choice of routing protocols, architecture of network and network operating conditions in order to achieve desired and good experiment performance.

This chapter is aimed to establish and analyze collaborative attacks in MANET, showing the consequences of multiple node attacks in such network using the OPNET modeler. It also emphasizes the OPNET potentials in designing and analyzing such MANET deployments and at the same time give helpful insights into various experiments and simulations.

5.1 Explanation of Simulator/Modeler

Our simulations are carried out using OPNET Modeler Version 14.5 software platform. OPNET stands for Optimized Network Engineering Tools and was developed by OPNET Technologies Incorporation. OPNET is a provider of Network Engineering, planning and operations, Application performance management and Network Research and Development (R&D) that are used to provide solutions for managing applications and networks [16].

In performing simulations, there are a variety of software applications or platforms widely available, such as NS2, QualNet, OMNeT++, in which we decided to use OPNET Modeler. Our reason for selecting OPNET is as a result of its key features; providing solutions for building networks and applications and it usually gives accurate results. OPNET supports University Programs allowing students to apply for free educational version license that lasts for 6 months. Another reason is that OPNET has been largely recognized; there are instances of its recognition by Audit Integrity ranking amongst “America’s Most Trustworthy Companies” analyzed and featured in [18].

5.2 MANET in Simulator

There are various network routing protocols that are applicable in OPNET when it comes to simulating a mobile ad hoc network (MANET). The basic MANET Routing Protocols are:

- Ad hoc On-demand Distance Vector (AODV)
- Optimized Link State Routing (OLSR)
- Zone Routing Protocol (ZRP)
- Landmark Ad hoc Routing (LANMAR)
- Location Aided Routing (LAR)
- Dynamic Source Routing (DSR)
- Temporally Ordered Routing Algorithm (TORA)
- Destination Sequence Distance Victor (DSDV)
- Open Shortest Part First (OSPF)

The above MANET routing protocols and other Ad hoc routing protocols can be classified under the three main classes of routing namely: Flat, Hierarchical and Geographical Position Assisted Routing [19]. The flat routing protocols are further divided into either reactive or proactive routing mode. Figure 5.1 below shows details of these classifications.
5.2.1 MANET model limitations

Modeling mobile ad hoc networks in OPNET has certain limitations because some features are yet to be implemented in the simulator; thus they may be implemented in the later versions of OPNET Modeler. The following are a few limitations concerning our simulation work [20].

- The OPNET Modeler version 14.5 currently supports four out of the MANET routing protocols which are the AODV, DSR, OSLR and TORA routing protocols.
- A node supports only a single MANET routing protocol i.e. all the interfaces of a router node should run the same MANET routing protocol.
- Re-distribution among MANET routing protocols is not implemented.
- The modeler does not support re-distribution between MANET and Internet routing protocols like the OSPF, RIP, and so on.

Based on the facts that only one MANET routing protocol can be used at a time and mixing more than one MANET and Internet routing protocols are not permitted we have decided to make use of the AODV routing protocol in our simulation work. The reasons for selecting AODV are because it is a reactive routing protocol that collects routing information when required unlike proactive routing protocols that discover routing data prior to when they are needed [7]. Also, it is because AODV is a popularly used MANET routing protocol.

5.3 Simulation Modeling Workflow

This subsection describes the modeling workflow used in our simulation work as shown in figure 5.2 below.
There are five states or steps of modeling the desired system represented by each rectangular box above. The horizontal arrows depict the actions to be taken in order to move from a state to another, while the bent dashed arrows represent where the validation, verification and credibility concepts are prominently established [15].

5.3.1 System

This is the first step of the model that requires building the network model. The network model is built using the OPNET Modeler. Desired MANET nodes (fixed or mobile nodes) are selected depending on the aim of the network model being created. We make use of mobile nodes and they are usually configured using the OPNET’s predefined parameters or done manually.

5.3.2 Assumptions document

This step is essential before the state of simulation programs. Some kind of information, data and analysis are necessary between here and the first state of the model. Development of a walk-through list of assumptions or assumptions document is presented before the simulation is done. An assumptions document is an explanation of how a system works relative to the specific issues to be addressed by the model [15]. As part of assumptions document, it is important that we choose the necessary statistics to be collected during the simulation model. The necessary statistics related to obtain desired result of collaborative attacks on MANET are selectively applied on the model in OPNET simulator. The major statistics selected in this simulation model are the performance metrics, discussed in subsection 5.4. Some other assumptions are made in this simulation model and would be explained accordingly as each one arises.

5.3.3 Simulation program

At this state, the simulation programs are run after series or stages of configuration or programming required. The performance metrics generated from the simulation are stored while the simulation is run several times in order to obtain accurate results.

5.3.4 Simulation results

Simulation results are now available and ready to be used for analysis to establish credibility of the simulation model and the built system. Statistics to display are applied to the OPNET Modeler to obtain the results because OPNET does not automatically determine and generate the statistics.
Two kinds of statistics can be obtained as the results in OPNET; the Global Statistics and the Object Statistics. The global statistics are results obtained collectively from the entire network including all nodes and the object statistics are from discrete nodes in the network.

5.3.5 Results used in analysis and evaluation
The collected results are analyzed and evaluated. Results can be used in the current project as well as in future projects.

5.4 Performance Metrics
In evaluating a MANET routing protocol as well as evaluating a security attack against MANET as a network, different statistics or performance metrics are used. In this subsection, we discuss the essential metrics required to evaluate and determine the possibility of multiple node attacks on a MANET. The performance metrics: network throughput, end to end delay, and packet delivery ratio.

5.4.1 Network throughput
A network throughput is the average rate at which message is successfully delivered between a receiver (destination node) and its sender (source node). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination [22]. Throughput can be measured as bits per second (bps), packets per second or packet per time slot and OPNET Modeler expresses it using bits per second. For a network, it is required that the throughput is at high-level. Some factors that affect MANET’s throughput are mentioned in [22]: these are unreliable communication, changes in topology, limited energy and bandwidth.

5.4.2 End-to-end delay
Packet end-to-end delay is the time delay it takes a network source to deliver a packet to its destination. Thus, the end-to-end delay of packets is the total amount of delays encountered in the whole network at every hop going to its destination. In MANETs, this kind of delay is usually caused by certain connection tearing or/and the signal strength among nodes been low. The reliability of a routing protocol can be determined by its end-to-end delay on a network, thus a steadfast MANET routing gives less packet end-to-end delay.

5.4.3 Packet delivery ratio
This refers to the ratio of the total number of data packets that reach the receiver (destination node) to the total number of data packets sent by the source node. This is another performance metric that is used to determine the efficiency and accuracy of MANET’s routing protocol because it is used to calculate the rate of loosing packets. Similar to the network throughput, packet delivery ratio (PDR) is expected to be high.

5.5 Simulation Model
Our simulation model was carried out using the OPNET Modeler software platform. It is a useful research tool for achieving good simulation results. This subsection explains the simulation model according to the simulation workflow presented earlier (see figure 5.1), while results are presented in the results section.
5.5.1 Setting up the simulation

The first phase in building the system is to set up a Mobile Ad hoc Network, which is done by creating a blank scenario in OPNET that provides the project editor (workspace) where the desired MANET is designed. A fresh scenario is created with the aid of the start-up wizard where a number of MANET mobile nodes are selected into the network workspace.

Next step is the configuration of each MANET node, which is done both by using the predefined parameters in OPNET and manual configuration of node’s attributes. The entire system and MANET nodes in this system are built based on some values and settings that we believe would enable us obtain reliable results. These are subject to change at any required time during the simulation modeling. In our simulation, we used the following network environment, tools, values, parameters and made certain assumptions (referred to as the assumption document).

- **Assumption Document**
  - TCP/IP Network transmission
  - IEEE 802.11b (Media Access Control) MAC
  - Campus Network Environment with 1.5 X 1.5 kilometers squared space
  - Between 10 to 30 nodes allocated randomly
  - Between 512 to 1024 bytes of data transmission
  - Application of the Constant Bit Rate (CBR)
  - Node mobility is used
  - Node transmission of about 250 M power rate
  - 30 seconds selected time of pause (exponential or constant)
  - All MANET nodes on the network run on AODV routing protocol

After building the network with required node configuration in terms of parameters, network environment and on the assumption document, we then need to run the simulation model. Prior to running a simulation in OPNET Modeler 14.5, the output data options to be obtained need to be selected; these are referred to as the performance metrics. OPNET provides two kinds of performance metrics (usually called statistics), Object Statistics and Global Statistics [20]. The object statistics are results from the discrete nodes in the network while global statistics are results obtained from the entire network including all nodes.

We chose the preferred metrics such as packet delivery ratio, delay and throughput according to how adequate results could be analyzed. Some configurations or runtime options such as common settings, inputs, outputs, executions and duration of simulation can still be changed or selected before running the model.

Finally, results are available after the simulation is run. Each result can be viewed as long as the project or scenario is saved after running the simulation. Required results must have been chosen as part of the performance metrics earlier selected, likewise to view results on the screen, one has to click the check-box of the nodes or options whose results are needed. Results can be displayed in different views with the aid of the two presentation options available on the results window. This is done by making a combination of the options that help present the results better.
5.6 Simulation Results

Different scenarios can be created in a simulation in OPNET. We created different scenarios during the simulation model in order to provide another phase of designed project space that we used for different experiments and results analyses. Another reason for having different scenarios is to enable us to determine the consequences of mobile network under regular operation, under collaborative attack and in terms of varying network size. Here, we present the various results obtained in our two main scenarios and explain each scenario.

5.6.1 Scenario 1: 11-Node MANET Network

Our first scenario is simulation of a small network of 11 mobile nodes. In this scenario, we carried out two different simulations. The first simulation in this scenario is building a regular MANET in terms of noting the outcome and behaviour of nodes of the mobile ad hoc network without any form of attack launched on them. This would enable us to take note and measure the effects of the network when there is an attack (in second simulation). We carried out different simulations that were run many times to ascertain the results and we were able to present relevant and comparable results.

5.6.1.1 MANET network under regular operation

This simulation has a MANET of 11 mobile nodes, which were configured based on the above stated assumption documents and with traffic generation sources. The 11 nodes are simple mobile nodes that are benign and none is malicious node. The aim of this is to determine the actual network throughput, the overall data packet delivery ratio (PDR) and end-to-end delay. Figure 5.3 below shows the MANET model layout and workspace with 11 mobile nodes while figures 5.4 through 5.6 show the result based on the obtained performance metrics (throughput, PDR and end-to-end delay).

Figure 5.3 – Simulation Workspace with selected mobile nodes (1500x1500)
5.6.1.2 MANET network under direct collaborative attack

This experiment is a simulation of a blackhole attack which has been characterized as a direct collaborative attack. It is an attack that impersonates on the Mobile Ad hoc Network and its collaborative nature shows its effect on some of the other MANET nodes and the entire network.

This second phase of scenario 1 is also a MANET of 11 mobile nodes, which were configured according to the assumption documents and with traffic generation sources. Out of these 11 mobile nodes, 10 nodes are benign nodes while one is a malicious node (a blackhole node). We also performed different simulations and we present relevant and comparable results to the results of regular network obtained earlier. The results of these performance metrics are shown in figures 5.4, 5.5 and 5.6.

Figure 5.4 – Throughput of 11-node MANET Network

Figure 5.5 – Packet Delivery Ratio of 11-node MANET Network
5.6.2 Scenario 2: 30-Node MANET Network

This is the second scenario; a simulation of a larger network in term of size compared to the first scenario. The network environment is still the same 1.5 x 1.5 kilometre square space of a campus network but the network size is bigger; having 30 mobile nodes compared to the earlier two simulations with 11 mobile nodes. Here, we present two simulations in which the first is a network of MANET under regular operation while the latter is a MANET network under direct collaborative attack and both include 30 nodes. The model layout in this scenario is similar to that depicted in figure 5.3 except that it contains mobile nodes 0 to 29.

5.6.2.1 MANET network under regular operation

This is a simulation of a regular network in terms of noting the outcome of the mobile ad hoc network without any form of attack launched on the MANET. The 30 nodes are also configured according to the assumption document. These 30 mobile nodes are mobile nodes that are benign. Our aim is also to measure the effects of the network in its regular operation and compare with the operation during a collaborative attack. The network throughput, packet delivery ratio and end-to-end delay of this network are given and compared with an attacked MANET in figures 5.7 through 5.9.

5.6.2.2 MANET network under direct collaborative attack

This experiment is simulation of a direct collaborative (blackhole) attack on a MANET of 30 mobile nodes. It is an attack that impersonates on the Mobile Ad hoc Network and its collaborative nature shows its effect on some of the other MANET nodes and on the global network. We also performed various simulations in line with those performed in regular MANET network of 30 nodes then we obtained relevant and comparable results as shown in figures 5.7, 5.8 and 5.9. The simulation workspace used is replica to that in figure 5.3 except that it contains normal mobile nodes 0 to 27 while the source node and malicious node make the completion.

Figure 5.6 – End-to-End Delay of 11-node MANET Network
Figure 5.7 – Throughput of 30-node MANET Network

Figure 5.8 – Packet Delivery Ratio of 30-node MANET Network
Figure 5.9 – End-to-End Delay of 30-node MANET Network
6: ANALYSIS

After presenting the basic results of all simulations carried out in both scenarios, in this chapter, we analyze and discuss all these results. The performance metrics collected and presented in our results are either based on the object statistics or global statistics of the MANET model i.e. the entire network. In representing these data, we presented the average or time_average values of the results in this report.

We start our discussion and analysis with the two main scenarios in which the first scenario comprises of 11 mobile nodes and the latter holds 30 mobile nodes. In each scenario, we performed two simulations of a regular network operation in MANET and a MANET under direct collaborative attack, a blackhole attack to be precise. All simulations i.e. both scenarios were run for a time period of 10 minutes, which ranged from 0 to 600 seconds as shown in the result graphs. After that, we analyze and compare within each scenario and also both scenarios based on their throughput, packet delivery ratio and end-to-end delay.

6.1 Scenario 1

The first scenario was completed using two different simulations to easy the presentation and analyses of results. These two simulations followed the model workspace in figure 5.3. Figure 5.4 shows the throughput performance metrics of simulations 1 and 2, which are based on MANET’s regular operation compared with when under collaborative blackhole attack, respectively. We observe that without collaborative blackhole attack, the MANET has a high throughput varying from 9,072.00 to 2,008.16 bits per second. On the other hand, with collaborative attack, its throughput dropped and ranged from 1,861.33 to 506.03 bits per second (see table 6.1).

Similarly, figure 5.5 shows the effect of the packet delivery ratios in both cases; with and without collaborative blackhole attack. It is seen that the PDR dramatically decreases as a result of collaborative blackhole nodes in the MANET because some of the packets received are being dropped by the malicious nodes. Also considering figure 5.6, we noticed that the MANET operation decreased a little in its average end-to-end delay when under collaborative attack, as compared with MANET regular operation. The operation of MANET under the attack has lower average end-to-end delay as there is usually immediate route reply from the blackhole nodes because they claim to have shortest routes to destinations. Another reason is that the malicious blackhole nodes do not check its MANET routing table. The initial and final values obtained as well as minimum and maximum values of each of these performance metrics obtained in scenario 1 are provided in table 6.1.
Table 6.1: Data of 11-Node MANET Network

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
<th>Sim 1: Regular Operation</th>
<th>Sim 2: Collaborative Blackhole Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput (Bits/Sec)</td>
<td>Initial</td>
<td>9,072.00</td>
<td>1,861.33</td>
</tr>
<tr>
<td></td>
<td>Final</td>
<td>2,008.16</td>
<td>506.03</td>
</tr>
<tr>
<td></td>
<td>Minimum</td>
<td>2,001.14</td>
<td>502.74</td>
</tr>
<tr>
<td></td>
<td>Maximum</td>
<td>9,072.00</td>
<td>1,861.33</td>
</tr>
<tr>
<td>Packet delivery ratio (Bits/Sec)</td>
<td>Initial</td>
<td>6,912.00</td>
<td>597.33</td>
</tr>
<tr>
<td></td>
<td>Final</td>
<td>1,530.03</td>
<td>440.48</td>
</tr>
<tr>
<td></td>
<td>Minimum</td>
<td>1,524.68</td>
<td>199.11</td>
</tr>
<tr>
<td></td>
<td>Maximum</td>
<td>6,912.00</td>
<td>597.33</td>
</tr>
<tr>
<td>End-to-End Delay (Sec)</td>
<td>Initial</td>
<td>0.0008120</td>
<td>0.0007659</td>
</tr>
<tr>
<td></td>
<td>Final</td>
<td>0.0003465</td>
<td>0.0003055</td>
</tr>
<tr>
<td></td>
<td>Minimum</td>
<td>0.0003465</td>
<td>0.0003052</td>
</tr>
<tr>
<td></td>
<td>Maximum</td>
<td>0.0008120</td>
<td>0.0007659</td>
</tr>
</tbody>
</table>

6.2 Scenario 2

This scenario comprised of 30 nodes which is a larger network size compared to the first scenario with 11 nodes. It also consisted of two simulations referred to as Sim 3: Regular Operation and Sim 4: Collaborative Blackhole Attack, respectively. Considering the result presented in figure 5.7, we make observation that the average throughput of the network when it was under collaborative blackhole attack was much less compared to when it was under regular operation. In the result of average packet delivery ratio presented in figure 5.8, similar observation made realizing it is modestly larger when MANET operation was normal compared to the decrease that occur when the network was under collaborative attack. This is as a result of the malicious nodes in the MANET dropping some of the packets that reach them rather than forwarding to the other nodes or destination.

In figure 5.9, we display the assessment of the average end-to-end delay of the 30-node MANET network. We realize that the average end-to-end delay of the mobile ad hoc network slightly increased under regular operation compared to that with collaborative blackhole attack. The reduction of end-to-end delay when it was under collaborative attack is as a result of the blackhole nodes claiming shortest routes; sending immediate replies to destination nodes and these blackhole nodes do not have a check on the routing table. The table 6.2 below presents some comparable data from the three performance metrics taken into consideration for our analyses.
Table 6.2: Data of 30-Node MANET Network

<table>
<thead>
<tr>
<th>Scenario 2: 30-Node MANET</th>
<th>Metric</th>
<th>Value</th>
<th>Sim 3: Regular Operation</th>
<th>Sim 4: Collaborative Blackhole Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Throughput (Bits/Sec)</td>
<td>Initial</td>
<td>45,808.00</td>
<td>2,576.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final</td>
<td>15,485.12</td>
<td>1,781.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum</td>
<td>13,512.00</td>
<td>444.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum</td>
<td>45,808.00</td>
<td>2,576.00</td>
</tr>
<tr>
<td></td>
<td>Packet delivery ratio (Bits/Sec)</td>
<td>Initial</td>
<td>34,901.33</td>
<td>1,962.67</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final</td>
<td>11,798.18</td>
<td>1,479.93</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum</td>
<td>10,294.86</td>
<td>343.56</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum</td>
<td>34,901.33</td>
<td>1,962.67</td>
</tr>
<tr>
<td></td>
<td>End-to-End Delay (Sec)</td>
<td>Initial</td>
<td>0.0034772</td>
<td>0.0005455</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final</td>
<td>0.0003078</td>
<td>0.0002874</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum</td>
<td>0.0003079</td>
<td>0.0002874</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum</td>
<td>0.0034772</td>
<td>0.0005455</td>
</tr>
</tbody>
</table>

6.3 Scenario 1 vs. Scenario 2

In comparing scenarios 1 and 2 with all the results presented and also when comparing the data in tables 6.1 and 6.2; we observe that our measurement based on some metrics; throughput, packet delivery ratio and end-to-end delay, scenario 2 has higher network performance both when the MANET was with and without collaborative blackhole attack. This is expected because of the obvious reason that scenario 2 has higher number of mobile nodes compared to scenario 1. On the other hand, comparing the margins of each performance parameter of the different scenarios, we observe that the rate of degradation and collaborative effects of the malicious nodes make the data margin of scenario 2 to be wider. This is as a result of the collaborative blackhole attack, which affects more nodes compared to the number of nodes affected in scenario 1.

In order to find differences in the simulation results and to be able to compare results, our simulation was performed in two scenarios based on different network sizes. Each scenario has first experiment for regular operation of MANET and second experiment for MANET operation under a collaborative blackhole attack. Our experiments show encouraging results obtained from the two scenarios of the simulation. The regular MANET outperforms the MANET under attack in terms of throughput and packet delivery ratio. These results show the effect of the collaborative blackhole attack on MANET because the packet delivery ratio and throughput of a good network is usually high. On the other hand, in terms of the end-to-end delay performance metric, the result obtained when the MANET was under collaborative blackhole attack shows there was a slight decrease in the delay because the malicious nodes provide a quick route reply to the source node claiming to be benign nodes and having the shortest route to the desired destination node.

In conclusion, we detect that the larger the MANET network size is in terms of the number of nodes, the more nodes that would be compromised and thus malicious; the more powerful the effect of the collaborative attack would be in terms of degradation of performance.
7: MITIGATION

Counteracting the various types of attacks in MANETs is challenging but interesting. Thus, there are many research papers that propose different schemes. Practically, there are two mechanisms, which are mainly used in those schemes to immunize MANETs against different attacks.

- **Preventive Mechanism:** This mechanism provides the first line of defence, like conventional security approaches that are used to protect wired networks. In mobile networks, we may also use some security modules such as: pass phrases, biometric verification, tokens or smart cards. However, from our point of view, the most important security module is the secure routing protocol. In MANETs, each node is required to forward the data packet of its neighbour to the node closer to the destination node, if one of the neighbouring nodes is selfish or compromised, the data packet simply cannot traverse to the intended destination node. Thus, utilizing a well-designed routing protocol is essential to make sure that the MANET operation runs smoothly and securely. There are many protocols used in MANETs (see Figure 5.1) but to design a security aware ad hoc routing protocol one needs to ensure the following properties: Timeliness, Ordering, Authenticity, Authorization, Integrity, Confidentiality, and Non-repudiation [21].

- **Reactive Mechanism:** The reactive mechanism provides the second line of defence. Currently, this mechanism is quite significant, especially for MANETs. There are two reasons; the first one is because of the natural weak-security characteristic of MANETs, which have been discussed so far. The second reason comes from hackers, so much advancement in hacking has been developed, if the hackers spend enough effort, they will eventually bypass the first line of defence and break into the system. One of the vital schemes developed based on the reactive mechanism is Intrusion Detection System (IDS). An IDS may sound like a very complicated system for many of us, but practically, it does just these functions: monitor audit data, check against intrusions to the system or network and initiate appropriate responses [21].

Finding the mitigation plans to combat against collaborative attacks in MANET is quite a demanding task. As we have already explained, collaborative attacks aim to disrupt routing operation. Apparently, these kinds of attacks are launched at the network layer, and the network layer in MANET is considered as the most vulnerable layer for being attacked compared to other attacks in MANET [26]. Therefore, the use of a preventive mechanism such as a secure routing protocol seems to be required in order to mitigate collaborative attacks in MANET. Authenticated Routing for Ad hoc Networks (ARAN) [27] is considered as the most secure routing protocol for MANET. Since, collaborative attacks are formed by groups of malicious nodes (direct or indirect), these nodes collude with one another to attack and they eventually affect the other nodes in the network as well. Thus, if a secured routing protocol like ARAN can be used, the chance of experiencing collaborative attacks would be reduced. However, the secure routing protocol is unable to detect and response to different kind of attacks. Thus, the use of an IDS can be considered as a better solution. For example, the Distributed Intrusion Detection System (DIDS) for ad hoc networks, which was proposed by Zhang and Lee [28], can help to detect and mitigate collaborative attacks, since IDS agents are placed on every node. Each agent is able to scan the local data in the node to detect intrusion but when necessary it can also cooperatively participate with other agents to form global intrusion detection actions to combat attacks that involve multiple nodes (i.e., collaborative attacks).
A filtering technique using collaborative nodes in a Danger-Theory driven MANET environment [35] is a possible mitigation plan proposed for all kinds of attacks. The proposed solution makes use of a Danger Theory (DT) model and the architecture Biologically-Inspired Tactical Security Infrastructure (BITSI) to detect and combat attacks ranging from denial of service attacks, routing attacks to multiple node attacks. DT focuses on discovering and mitigating damage to the MANET and each node in the MANET has a BITSI agent in its trusted module that monitors the node behaviour as well as traffic forwarded within the network. The danger theory and collaborative filtering with the use of BITSI function as an Intrusion Detection System (IDS) and/or an Intrusion Detection and Prevention (IDP) system by making collaboration amongst benign nodes in the MANET to counteract the attacking nodes.

Workman et al. [36] also proposed a socio biologically-inspired approach (BITSI) to strengthen security in MANET referred to as structuration agency theory. The authors made a study of MANET security, which is concerned with its nature of being and illustrated a use case for agency based on structuration theory. This proposed structuration agency framework can counteract direct and indirect collaborative attacks with its proactive and reactive methods of protection in MANET. This is achieved with the agents in the MANET exchanging vital information among nodes or wireless devices. However, these agents in MANET make use of three different forms of agency and social co-operation: direct agency, proxy agency and collective agency. These two solutions based on BITSI, discussed above can work to mitigate both direct and indirect collaborative we have categorized because the proposed collaboration between benign nodes could possibly detect or prevent such attacks. However, there is need for further research in order to validate their proposed solutions.

In the following subsections, we will go into more details of which countermeasures have been proposed for different collaborative attacks.

### 7.1 Mitigation for Direct Collaborative Attacks

Cross-layer Active RE-Routing (CARE) [29], an attack-resilient routing architecture can be used to combat both Blackhole and Wormhole attacks, which we categorize as direct collaborative attacks. As we have already noticed, the direct collaborative attacks are routing disruption attacks, which involve several physical nodes. Thus, to detect and mitigate these attacks someone needs to operate at the network layer. CARE is a cross-layer scheme; it can detect the attack at the transport layer by monitoring a TCP Congestion Window. If the route is compromised by an attacker, it will respond by initiating a re-routing process to find a new benign route in the network layer.

- **Countermeasure against blackhole attack:** Within the context of security attacks against MANET, the blackhole attack would be considered as a hotspot by which numerous papers have been published to propose schemes to detect and mitigate this attack. Thus, here are some of the schemes which are believed to be effective in countermeasuring the blackhole attack. Satoshi et al. [30] proposed an anomaly detection scheme by using dynamic updating training data; this scheme shows effectiveness in detecting the blackhole attack on AODV-based MANET. Another scheme was proposed by Sanjay et al. [31] in which the authors developed the prevention of cooperative blackhole attacks using two approaches: the first is to identify multiple blackhole nodes and the other is to discover a secure path from source node to destination node (in order to avoid cooperative blackhole paths). Deng et al. [1] proposed an interesting method to overcome the blackhole attack. The method is based on modifying the AODV routing mechanism; instead of all intermediate nodes sending RREP to the source node, only the destination node can
send out RREP. Thus, no intermediate node could claim to be a destination node or the shortest path to the destination node.

✓ Countermeasure against wormhole attack: There are many kinds of security attacks in the context of MANET. Each attack utilizes different mechanisms to exploit vulnerabilities of MANET but they all aim to illegally monitor or disrupt the network operation. However, wormhole attack is interesting to learn about, since it can be classified either as benign or malicious intent. In a wormhole attack, there always exist two colluding nodes. These two nodes exchange data packets back and forth by using a special tunnel. This tunnel can be a wired link or a long-range wireless link. Normally, if the attacker has no malicious intention, this wormhole tunnel can be used as a redundant communication channel but on the other hand, the attacker with malicious intention can control this tunnel to drop data packets randomly or even as a tool to monitor the whole network. Maria et al. [32] proposed a combination method called Protocol Breaking and Packet Timing Analysis to detect the wormhole attack. There are two checks in this method to detect wormhole attacks. The first, reactive check is to use timing analysis of the routing mechanism, such as ‘HELLO Message Timing Intervals’ to discover the intruders based on irregularities of the protocol, which will only occur if the intruders begin to drop the data packets. Secondly, the proactive check can even identify wormhole existence before the intruders start to drop data packets; this can be done by using simple signal processing techniques to monitor the arrival times of routing traffic management.

7.2 Mitigation for Indirect Collaborative Attacks

When comparing indirect collaborative attacks with direct collaborative attacks, the mitigation schemes that have been proposed to combat against indirect collaborative attacks are quite modest. The reason behind this is because of indirect collaborative attacks like Sybil and Routing Table Overflow attacks are not considered as popular security threats as direct collaborative attacks. However, the impact of those attacks on MANET would result in more severe consequences than direct collaborative attacks.

✓ Countermeasure against Sybil attack: As the name implies, the Sybil attack is the kind of attack where a malicious node claims to have multiple identities (Sybil nodes). These identities can deceive other benign nodes to send their data packets to them without noticing that these nodes do not exist at all. Haifeng et al. [33] proposed a SybilLimit scheme to combat against the Sybil attack. This scheme was developed based on leveraging a key insight regarding social networks. The social network contains user identities (which can also be referred to as nodes). The edge connecting two identities can be referred to as a human trust relationship. Malicious users are able to create an arbitrary number of fake identities but a few trusted relationships. SybilLimit exploits this characteristic to limit the number of identities that one user can create. Therefore, SybilLimit can control the number of identities that one malicious node in MANET can create.

✓ Countermeasure against Routing Table Overflow attack: In [34], the authors proposed an IDS system that can combat several attacks on AODV based MANET such as Rushing Attack, Modification of Routing Messages, Dropping of Routing Packets and Routing Table Overflow. This method employs many rules to detect different attacks and to detect Routing Table Overflow attack. It tries to discover if a neighbour node broadcasts more than RREQ_RATELIMIT messages per second. If this occurs the node will be considered as a malicious node, which is certainly launching Routing Table Overflow attack.
8: CONCLUSIONS AND FUTURE WORK

The main aim of this thesis is to analyse collaborative attacks on MANET. In order to achieve this aim, an extensive literature survey and theoretical analysis are done to discover different multiple node attacks which can be categorized as direct or indirect collaborative attacks. The categorization is done based on criterion of whether the attack based on existent nodes (direct) or non-existent nodes (indirect). Furthermore, to find out about negative performance impact with respect to three performance metrics; network throughput, data packet delivery ratio and packet end-to-end delay of a regular network under a specific collaborative attack; a simulation of direct collaborative blackhole attack is intensively performed. The simulation result is then analysed thoroughly to draw a final conclusion about two different network scenarios. Finally, another extensive survey of literature is also done to discover the suitable mitigation plans to alleviate different collaborative attacks.

8.1 Conclusions

In addressing the first research question, we realize that there are number of multiple node attacks in MANET. However, according to our definition and categorization criteria, not all of them can be classified as direct or indirect collaborative attacks. The well-formulated definition and categorization of collaborative attacks can provide substantial benefits to other researchers in understanding and then discovering other possible collaborative attacks in the future.

The answer to the second research question is aimed to measure the consequence of direct collaborative blackhole attack on MANET. Intuitively, the analysis of the consequences of each scenario shows that the throughput, packet delivery ratio and end-to-end delay of MANET under collaborative blackhole attack significantly drop compared to normal MANET operation. Also, a combination of the two scenarios suggests that the more mobile nodes that are malicious or compromised on the MANET; the deeper the consequences and deterioration of its performance will be. Furthermore, the significant negative performance impact which we have collected in the simulation can also provide invaluable inputs for future research in case the researcher wants to perform consequence comparisons between normal attacks with collaborative attacks in MANET.

According to the third research question, there are a few schemes that claim to be able to prevent and mitigate all kind of security attacks in MANET (see chapter 7). In those proposed schemes, the researchers believe that; with their unique mechanisms, such as integrating an agent into each node to monitor the malicious activity in a mobile network and if one of the nodes becomes malicious, the adjacent node can inform other nodes in the network. Then, the agent at the malicious node can also suspend that node from spreading to other nodes. Nonetheless, those schemes show no sign or proof that they could combat against sophisticated security attacks, e.g., like collaborative attacks. Specifically, each type of collaborative attack has a specific mitigation plan or set of mitigation plans that are proposed to counteract against that particular attack. However, Cross-layer Active RE-Routing (CARE), a routing resilient architecture has theoretically claimed to be able to alleviate direct collaborative attacks.

8.2 Future Work

A significant amount of research has been devoted to study security issues as well as countermeasures to various attacks in MANET. However, we believe that there is still much research work needed to be done in the area. The underlying rationale is that, existing
security solutions are well-matched with specific attacks, these solutions have proven to be useful to defend against known attacks, but eventually they fail to counteract unanticipated or combined attacks. In this thesis, we try to discover multiple node attacks and categorize them as direct or indirect collaborative attacks but we still have doubts that there could be some other kind of attacks that can be classified as collaborative attacks. Thus, further research would be carried out in order to validate the theoretical model: the definition of collaborative attacks and in identifying other collaborative attacks (currently not covered). Due to time constraints, we only simulate the blackhole attack on MANET to show how this attack impacts the regular operation in MANET. Therefore, in order to further establish the consequences of collaborative attacks, another direction for future work would be to simulate other types of collaborative attacks, e.g., wormhole, sybil and routing table overflow attacks and compare the results. Such studies may result in a more complete picture of how network performance is affected during a specific collaborative attack or even combined collaborative attacks. The aforementioned research is quite challenging but interesting to conduct. Finally, the development of a mitigation plan capable of defending against various collaborative attacks would be considered as another important direction for future work.
REFERENCES

[19] OPNETWORKS 2006 – OPNET’s annual user conference
[20] OPNET Modeler 14.5 Documentation


