A NOVEL INTRUSION DETECTION SYSTEM FOR COLLABORATIVE ATTACKS IN MOBILE AD-HOC NETWORKS

BY

ABDULSALAM SALEM SAEED BASABAA

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER NETWORKS

March 12, 2014

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN- 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **Abdulsalam Salem Basabaa** under the direction his thesis advisor and approved by his thesis committee, has been presented and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORKS.**

Dr. Tarek R. Sheltami
(Advisor)

Dr. Basem Al-Madani
Department Chairman

Dr. TYPE NAME
(Co-Advisor)

Dr. Salam A. Zummo
Dean of Graduate Studies

Dr. Ahmad Almulhem
(Member)

25/3/14
Date

Dr. Zubair A. Baig
(Member)

Dr. TYPE NAME
(Member)

Dedication

I dedicate this thesis to my family for their unlimited love, support and encouragement.

ACKNOWLEDGMENTS

Foremost, a great praise and thank for Allah, the Almighty, who supports and helps me all the time in my life. In particular, thank God for the wisdom and perseverance that he has been bestowed upon me during this research and whole study as well.

Many thank to my thesis advisor Dr. Tarek Sheltami for his support, guidance and advice throughout this research. Indeed, without his guidance, I would have not be able to put the topic together.

Besides my advisor, I would like to thank my thesis committee: Dr. Ahmad Almulhem and Dr. Zubair Baig for their insightful comments, encouragement, and guidance during my master's research.

My sincere thanks also extend to King Fahd University of Petroleum and Minerals (KFUPM) and Hadhramout Est. for Human Development, Hadhramout, Yemen for supporting me during my master study.

Last but not the least, unlimited thanks to my family for their unconditional encouragement throughout my master degree and whole study as well.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

List of Acronyms or Abbreviations according to their appearance in this thesis as follow:

MANETs	:	Mobile Ad-Hoc Networks
DSDV	:	Destination-Sequenced Distance Vector
WRP	:	Wireless Routing Protocol
CGSR	:	Cluster head Gateway Switch Routing
AODV	:	Ad-hoc On-demand Distance Vector
TORA	:	Temporally Ordered Routing Algorithm
DSR	:	Dynamic Source Routing protocol
ZHLS	:	Zone-Based Hierarchical Link State
RREQ	:	Route Request
RREP	:	Route Reply
RERR	:	Route Error
IPSs	:	Instruction Prevention Systems
IDSs	:	Intrusion Detection Systems
A3ACKs	:	Adaptive Three Acknowledgements

ABSTRACT

Full Name : Abdulsalam Salem Saeed Basabaa

Thesis Title : A Novel Intrusion Detection System for Collaborative Attacks in Mobile Ad hoc Networks.

Major Field : Computer Networks

Date of Degree : March 12, 2014

Wireless networking is an emerging technology that allows users to access information and services anywhere regardless of their geographic location. Mobile Ad hoc Network (MANET) is one of the most significant technologies among various wireless communication technologies. In MANETs, all nodes are mobile and can be connected dynamically using wireless link in a random manner. All nodes in MANETs behave as routers and take part in discovery and maintenance of routes to other nodes in the network. They communicate directly with each other only if they are within the communication range. However, they rely on each other and forward packets when they are out of communication ranges. MANETs are infrastructure-less network and have self-configuring features that make them suitable for many critical applications, such as military and emergency applications. However, these features make them also vulnerable for all types of passive and active attacks because of open environment, the rapidly changing topology and the decentralization of nodes in MANETs. In addition, most of the proposed MANET protocols assume that all nodes in the network are cooperative, and do not address security issues in MANETs. Since most of the proposed existing intrusion detection systems (IDSs) of MANETs are based on Watchdog technique, we study the behavior of the Watchdog technique, and propose a solution for its three significant problems, namely: receiver collision, limited transmission power and collaborative attacks (collusion attack), especially when there are two consecutive collaborative malicious nodes in a path. To demonstrate the feasibility of our proposed system, it is implemented and tested under various scenarios using NS2 simulator. To validate the results achieved, we compared our results with the results of AACK IDS technique.

ملخص الرسالة

الاسم الكامل: عبد السلام سالم سعيد باسباع

عنوان الرسالة: نظام كشف التطفل للأعتداءات التعاونيه في الشبكات اللاسلكيه المتحركه

التخصص: شبكات حاسوب

تاريخ الدرجة العلمية : 12 مارس 2014

الشبكات اللاسلكية هي التكنولوجيا المستجده التي تسمح للمستخدمين بالوصول إلى المعلومات والخدمات في أي مكان بغض النظر عن موقعهم الجغرافي. الشبكه اللاسلكيه المتحركه (الشبكه اللاسلكيه المتحركه) هي واحدة من التقنيات الأكثر أهمية بين مختلف تقنيات الاتصالات اللاسلكية . في الشبكه اللاسلكيه المتحركه ، كافة العقد هي المتنقلة و يمكن ان تكون مرتبطة بشكل مباشر باستخدام رابط لاسلكي بطريقة عشوائية. جميع العقد في الشبكه اللاسلكيه المتحركه تعمل كموجهات و يشارك في اكتشاف وصيانة الطرق المؤدية إلى العقد الأخرى في الشبكة.العقد تتواصل مباشرة مع بعضها البعض إذا كانت داخل نطاق الاتصال . ولكنها تعتمد على بعضها البعض عندما تكون خارج نطاقات الاتصالات. الشبكات اللاسلكيه المتحركه هي شبكة البنية التحتية أقل ولها ميزات تكوين الذات التي تجعلها مناسبة لكثير من التطبيقات الهامة ، مثل التطبيقات العسكرية و حالات الطوارئ. ومع ذلك ، هذه الميزات تجعلها عرضة أيضا لجميع أنواع الهجمات السلبية والإيجابية بسبب بيئتها المفتوحة ، المتغيره بسرعة وعدم وجود المركزيه في الشبكات اللاسلكيه المتحركه .بالإضافة إلى ذلك، فإن معظم بروتوكولات الشبكه اللاسلكيه المتحركه تفترض أن جميع العقد في الشبكة هي متعاونه وايجابيه، ولا تعالج القضايا الأمنية في الشبكه اللاسلكيه المتحركه. ولأن معظم النظم الموجوده تعتمد على تقينيهة الوتش دوق ،في هذا البحث نحن ندرس سلوك هذه التقينه ، ونقترح حل لثلاث مشاكل هامه وهي: استقبال الاصطدام، التحكم في الاشاره المحدوده والهجمات التعاونية (الهجوم التواطؤ) ، وخاصة عندما تكون هناك عقدتين خبيثه متعاونه ومتتاليه في المسار. لإثبات جدوى نظامنا المقترح، تم تنفيذهواختباره تحت السيناريوهات المختلفة باستخدام المحاكي NS-2 .ومن اجل التحقق من صحة النتائج لهذه التقينه قمنا بمقارنة نتائجها مع نتائج طريقة الآدابتف اكنولودجمينت.

CHAPTER 1

INTRODUCTION

1.1. Mobile Ad-hoc Networks Overview

Mobile Ad-hoc Network (MANETs) refers to a collection or group of wireless mobile nodes communicating with each other via bi-directional wireless links. Each node has both a transmitter and receiver to communicate either directly or indirectly. Unlike traditional wireless networks, MANETs don't depend on fixed network infrastructure such as base stations or access points. As a result, MANETs are used in a military and temporary networks for a quick deployment and self- organized networks for specific purpose and limited period of time. In MANETs, nodes are free to move arbitrarily inside the network [1] and they have limited transmission range to communicate together. Nodes in MANETs are decentralized, self-organizing, self-configuring and cooperate with each other to manage and forward the packets from source to destination without depending on fixed infrastructure. Thus, nodes in MANETs operate as router by routing the packets of other nodes. Therefore, there are mainly two types of MANETs: single hop and multi-hop networks. In single hop MANET, there are no intermediate nodes and each node can communicates with other nodes in its transmission range, for example using Bluetooth. On the other hand, if the destination node is outside the source node's wireless transmission range, MANET is called multi-hop MANET, where nodes rely on others to

communicate with nodes that are out of their transmission range. More details about MANETs and their related researches can be found in [2] [3] [4] [5].

There are several applications for MANETs. It was developed for military or police purposes [6][7]. In addition, MANETs require minimal configuration and fast deployment that make them proper for using in emergency circumstances where an infrastructure is unavailable or infeasible, for example in case of earthquakes or other natural disasters [6][8]. Moreover, MANETs can be used in civilian and commercial uses. For example, in a conference, a group of people use ad-hoc networks to communicate with each other and exchange data by using their difference devices. Finally, in MANETs, one of the most appealing ad-hoc applications is the sensor networks. Sensor networks have a lot of potential applications, so they have been addressed by many researchers in recent years. A more details about sensor networks and their applications can be found in [9][7]**.**

MANETs have several characteristics [10][7] include:

- Autonomous: Each node in MANET is autonomous and works as router and host.
- Decentralized: MANET is distributed in its operation and functionalities, such as routing, host configuration and security. For instance, MANET cannot have a centralized firewall.
- Multi-hop: If the source and destination of a message is out of the radio range of one node, a multi-hop routing is necessary to forward the data.

- Changing topology: Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.
- Unstable link bandwidth: The stability, capacity and reliability of wireless link are always lower than wired links.
- Limit resources: The mobile nodes are often light weight, with less powerful CPU, memory and power.
- Open medium: Due to the infrastructure-less in MANETs and free movement.

In term of merits, MANETs have three merits over wired networks [7] include:

- Regardless geographic position, MANETs provide access to information and services.
- MANETs can be setup anywhere and anytime.
- MANETs work without need to pre-existing infrastructures.

On the other hand, MANETs have several disadvantages or demerits [7] include:

- Resources limitation leads to limited security problem.
- MANETs are much vulnerable to attacks than wired networks due to lack of authorization facilities.
- MANETs have unpredictable time topology as result of network dynamic topology and this lead to hard detection of malicious nodes.

- Security protocols of wired networks cannot be applied for MANETs since MANETs have different architectures than wired networks.

1.2. Routing Protocol in Mobile Ad hoc NETworks

In this section, we discuss different proposed types of routing protocol that are designed mainly for MANETs. At the end, we describe DSR protocol as used protocol in this research.

1.2.1. Overview of Routing Protocol in MANETs

There are many routing protocols proposed for MANETs and according to their routing algorithms, they are divided to three main categories: *proactive*, *reactive*, and *hybrid* [11] as shown in Figure 1-1. For proactive routing protocols, the routing protocol find paths to all nodes in the network even if there is no packet ready to be sent and keep updating all these paths regularly after certain period of time. As a result, they waste limited bandwidth. For example, Destination-Sequenced Distance Vector routing protocol (DSDV) [12], the Wireless Routing Protocol (WRP) [12] and Cluster head Gateway Switch Routing protocol (CGSR) [13].

In contrast, in reactive routing protocols, the routing protocol reduces the routing overhead by updating route information only when there is demand for data transmission without need for periodically updates of the paths when there is no new traffic or change in network topology, such as Ad-hoc On-demand Distance Vector routing protocol (AODV) [14], the Temporally Ordered Routing Algorithm (TORA) [15], and the Dynamic Source Routing protocol (DSR) [16].

Lastly, hybrid routing protocols combine proactive and reactive methods to find efficient routes. For example, ZHLS [17] is a typical example of hybrid routing protocols. It divides the whole network into several non-overlapping zones and it works as proactive if the traffic destination is within the same zone of the source. However, it works as reactive to find the zone ID of the destination in whole network.

In this research, we concentrate on reactive protocols, especially DSR protocol due to its efficiency, dynamic nature, wider acceptance and the consideration for standardization.

A summary of MANETs proposed routing protocols are shown in Figure 1-1.

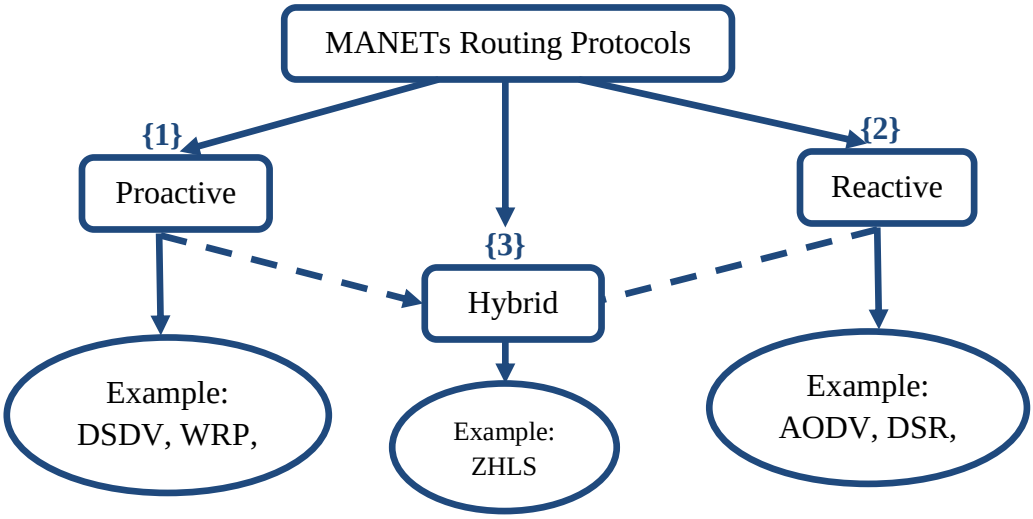

Figure 1-1: MANETs Routing Protocols

1.2.2. DSR Protocol

DSR stand for *Dynamic Source Routing* protocol [16] and it is an example of reactive routing protocol. It is designed to manage multi-hop MANETs and it has two main functions, named, *Route Discovery* and *Route Maintenance*.

DSR protocol performs *Route Discovery* when a node wants to send a packet to a destination that does not have a route to it [7]. Figure 1-2 shows example of *Route Discovery*, if node *S* has a packet wants to send to node *D*. In this case, if node *S* has in his *Route Cache* a route to destination node D, this route is immediately used. However, if node *S* does not have a route in its *Route Cache* for the destination node *D*, the *Route Discovery* protocol is started by node *S* (initiator):

1. Node *S* will send a broadcast *Route Request* packet (*RREQ*) to its neighbor.
2. Node *B* will receive the *RREQ* message from *S*. Node *B* will check if it has recently received the same *RREQ* from the same target or if its address is already added to the *RREQ's* record. If so, node *B* discards the *RREQ*.
3. If node *B* is the target (destination) of the *RREQ*, it will send back *Route Reply* packet (*RREP*) to node *S* as unicast packet over the reverse path of *RREQ* packet that is received. However, if node *B* is not the target of the *RREQ* and its address still not listed in the *RREQ's* record, node *B* will append its address to the *RREQ* packet and rebroadcast the *RREQ* packet to their neighbor except the initiator (node *S*).
4. Finally, the *RREQ* packet is received by the destination *D*, the destination *D* will send unicast Route Reply packet (*RREP*) back to node *S* over the reverse path of *RREQ* packet that is received. The *RREP* packet contains a list of best paths from the initiator node *S* to the destination node *D*. Then, the initiator node *S* caches this route in its *Route Cache* and uses this route to send subsequence packets to this destination (node *D*) in future.

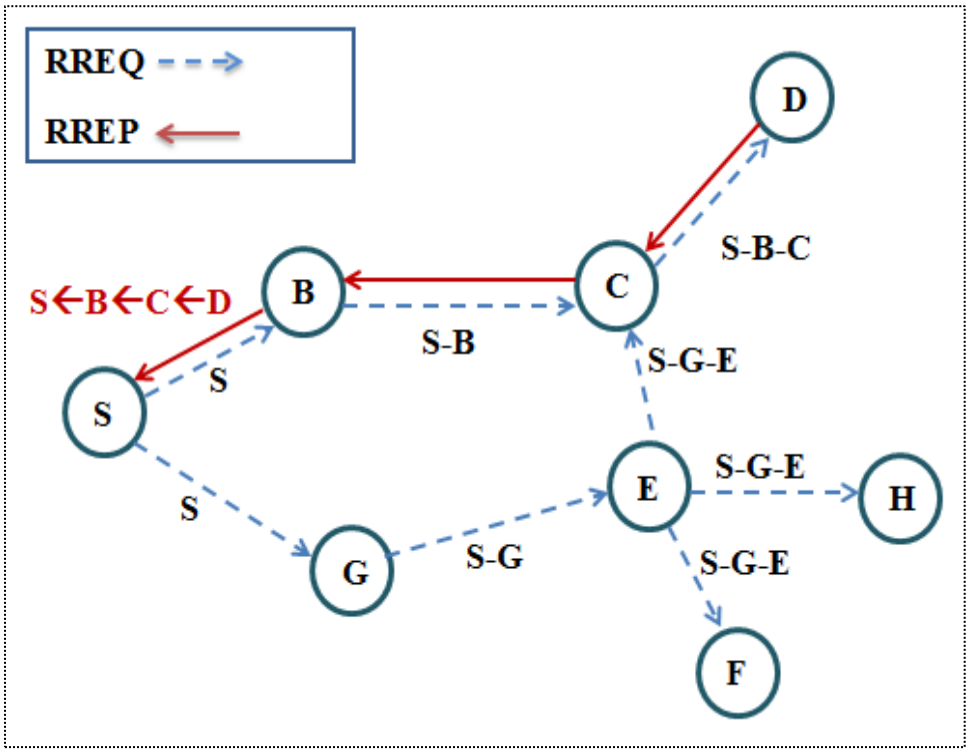

Figure 1-2: Route Discovery Procedure

On the other hand, DSR performs *Route Maintenance* to discover link failure on an active path, where the source node informed of the link failure and updates it routing cache appropriately. Figure 1-3 shows example of Route Maintenance, if node *C* does not receive an acknowledgement from node *D* after some number of requests, it returns a *RouteError* message to the initiator *S*. As soon as node *S* receives the *RouteError* message from node *C*, it deletes the *broken-link-route* from its *Route Cache*. If node *S* has another route to node *D*, it sends the packet immediately using this new route [7]. Otherwise the initiator *S* is starting the *Route Discovery* process again.

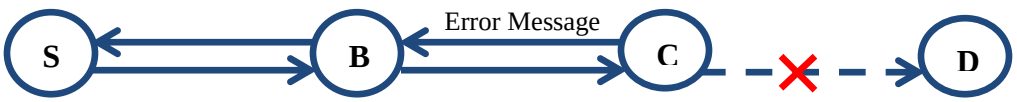

Figure 1-3: Route Maintenance Procedure

Both DSR's functions, *Route Discovery* and *Route Maintenance*, operate on demand manner to reduce routing overhead by updating route information only when there is required for data transmission without need for periodically updates of the paths when there is no new traffic or change in network topology.

1.3. Intrusion Detection Systems in MANETs

In this section, we discuss different proposed Intrusion Detection Systems (IDSs) that are designed mainly for MANETs. Lastly, we describe packet dropping attacks in MANETs.

1.3.1. Overview of Intrusion Detection Systems in MANETs

MANETs are more vulnerable to attacks than wired networks due to their open medium and dynamic change topology that enable attacks to enter network without being detected [7]. Thus, security of MANETs has become one of the primary researches concerns. In general, security threats or attacks in MANETs divided into active and passive attacks [7]. Passive attack: It does not disrupt the operations of network. It includes traffic analysis; snooping; monitoring and eavesdropping. For example, packets containing secret information might be eavesdropped, and lead to a violation of confidentiality. However, active attack attempts to alter or destroy of data being sent on the network. It includes injecting packets to invalid destinations into the network; modifying the contents of packets; deleting packets and impersonating other nodes violate availability and integrity [18][7]. Another classification of attacks is external and internal attacks [19]. In external attacks, misbehaving nodes that don't belong to particular network perform attacks on that network. On the other hand, unlike external

attacks, internal attacks carried out by misbehaving nodes that belong to particular network. Security levels in MANETs are divided into two levels, named, first layer of defense and second layer of defense [20]. The first layer of defense is represented usually as Instruction Prevention Systems (IPSs), which are software that is able to detect and stop possible incidents of external attacks once they enter into the networks, such as cryptography and authentication. But most of these security mechanisms suffer from late detection of attacks and become useless when the misbehaving nodes already enter the network or attacker compromised some nodes inside the network [21]. As a result, the first layer of defense, IPSs, becomes ineffective since the internal attacks are performed by misbehaving nodes inside the network. Here is where the intrusion detection system (IDS) comes in [22]. Unlike the first layer of defense, Intrusion Detection Systems (IDSs) represent the second layer of defense and they are able to detect internal attacks. The IDS is defined as the process of monitoring the occurring events inside a computer system or network and collect activity information for possible events. Then, IDS analyzes this data to determine if there any malicious activity that violate network security rules. Once IDS detects any malicious activity in the network, it generates alarm or initiates proper response to detected malicious activity. It acts as a great complement to the existing prevention systems.

There are many researchers [20][23] have classified existing IDSs based on data collected mechanism to either *host-based* or *network-based IDSs*. For host-based IDSs, they specify intrusion on the bounder of a host machine by analyzing the operating system's audit paths or system and application logs. However, network-based IDSs specify intrusion on the bounder of a network by analyzing captured packets on

network's traffics. More classifications of IDSs based on detection mechanisms [20] as follow:

a. **Signature-based (Misuse detection model) detection**: It compares captured data to known threat signatures to specify intrusion. It is very effective and efficient to detect known attacks and produces less false positive rates. However, it is ineffective and inefficient to detect unknown threats. In addition, it still suffers from detection at complex communications, such as detect threats that comprise multiple events. Furthermore, it fails to detect new kind of attacks like virus detection system.

b. **Anomaly-based detection**: It keeps normal profiles (normal behavior) of users and compares them to captured data over a period of time to identify intrusion. It deals with any activity that deviates from the baseline of the system as possible intrusion and then informs system administrator or start suitable response. It is effective and efficient to detect unknown attacks, but it may produce high false positive rates.

c. **Specification-based detection**: It defines a set of constraints that describe the correct operations of a program or protocol. Then, it checks the execution of programs and compares them to predefined constraints. It has ability to detect unknown attacks and produces low false positive rates. More details about classification and taxonomy of IDSs can be found in [6] [24][20].

1.3.2. Packet Dropping Attacks in MANETs

As discussed, security of MANETs has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in

the network is cooperative and not malicious [25][26]. Thus, a compromised node may cause the failure of the entire network. In addition, this assumption enables misbehaving nodes or malicious attackers to compromise the whole network by inserting malicious or non-cooperative nodes to MANETs. Therefore, a node is assumed to be helpful to other nodes to forward packets toward the correct destination. However, if a node does not forward packets for other nodes but drops them, it is called a *packet dropping attack*. The packet dropping attack is defined as a misbehaving node participates at routing information exchange and drops all data packet pass through it. In MANETs, the reasons for packet dropping can be intentionally or unintentionally as shown in Figure 1-4. The unintentionally packet dropping [27][28] can be happen as results of 1) node overload due to CPU overloaded or buffer overflow; 2) network congestion due to network applications; and 3) link error, such as interference or fading due to unreliability in wireless channels. However, as mentioned, intentionally packet dropping in a MANETs called *packet dropping attack* and nodes that drop packets intentionally named misbehaving nodes [27][28]. We can classify these nodes into *selfish nodes* and *malicious nodes*. For the first type, *selfish nodes*, node participates to carry out routing control packets (discovery and maintenance) inside a network to extract information from them, and drops data packets to save its energy since in MANETs the most energy consume as result of transmission as well as it drops data packet to save its bandwidth to send and receive only its own packets. However, in the second type of intentionally packet dropping, *malicious nodes*, node also participates to carry out routing control packets and drops all data packets to disrupt the network and effect availability and connectivity of the network. In addition, the malicious nodes are divided into two types,

named, black hole attacks and gray-hole attacks [29]. In black hole attacks, the malicious node drops all data packets that pass through it without dropping routing control packets. On the other hand, in gray hole attacks, the malicious node is smart enough to drop some of data packet that pass through it by adjusting its packets dropping ratio to IDS's detection threshold. Thus, it is difficult to the IDS to detect the gray-hole attack unlike black hole attack. However, the black hole attacks have affected the network's performance more than the gray-hole attacks as the first one drop all data packet pass through. As a result, it disrupts the availability and connectivity of the network, which are considered serious metrics for network's performance.

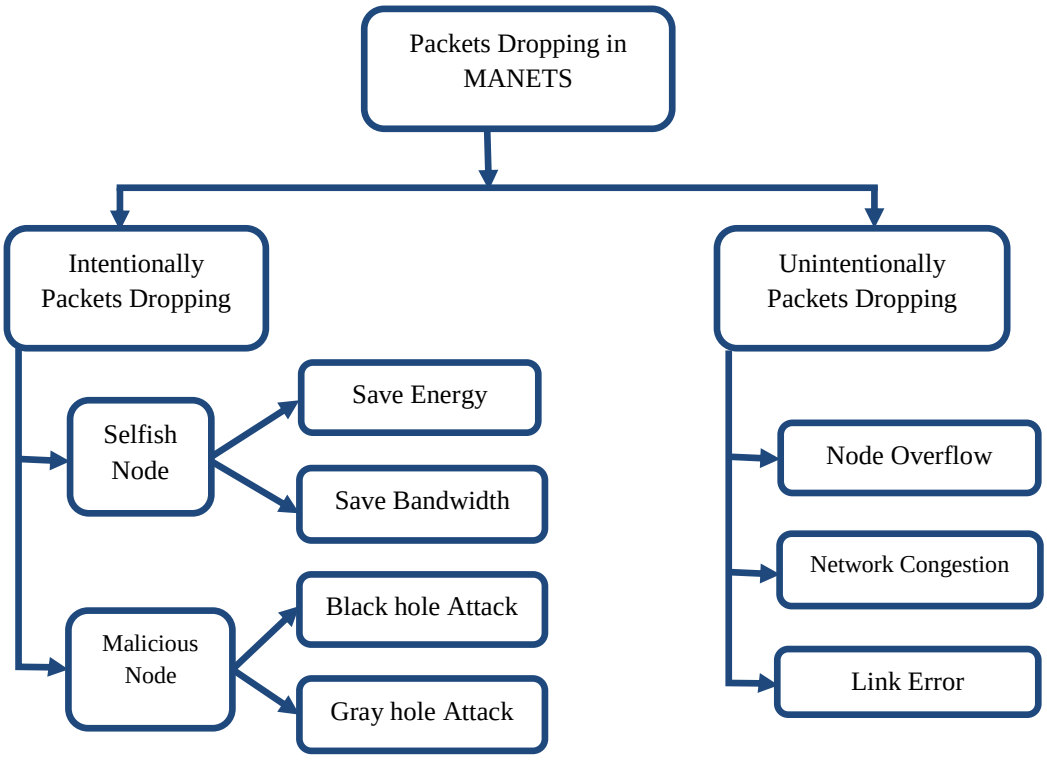

Figure 1-4: Packets Dropping in MANETs

1.4. Research Overview

This section includes research background as well as research challenges. Finally, it includes summary of our research contributions.

1.4.1. Research Background

As discussed before, most of the proposed MANETs protocols assume that all nodes in the network are cooperative, and do not address security issues in MANETs. In additions, the open medium, rapidly changing topology and decentralized of nodes in MANETs, make them vulnerable for all types of passive and active attacks. On the other hand, the encryption and authentication mechanisms, which are considered as the first line of defense, are no longer sufficient to protect MANETs. Thus, IDSs are needed as a second line of defense to protect the network from such security threats. However, the traditional wired IDSs that were designed for wired network cannot be used in MANETs since MANETs have different features and architecture than traditional wired networks. As a result, there are many recent IDSs designed especially for MANETs and most of them based on the Watchdog mechanism that was proposed in 2000 by Sergio Marti et al. [30].

In Watchdog, each node monitors its neighbors using overhearing promiscuous mode to be sure that they forward received packets or not. Even though, Watchdog mechanism improves the throughput in MANETs with the existence of selfish or malicious nodes. It has six weaknesses include: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collaborative

(collusion) of malicious nodes, and 6) partial dropping. However, there are many researches are proposed to solve these weaknesses including TWOACK, AACK and EAACK schemes. The TWOACK scheme was proposed in 2005 by Balakrishnan et al. [31]. It is acknowledgement base scheme that solves two weaknesses of Watchdog, named, limited transmission power and receiver collision. However, it solves these two weaknesses with more routing overhead and calculations that effect network's performance as well as it still suffers from collaborative attacks. On the other hand, the AACK scheme was proposed in 2009 by Al-Roubaiey and Sheltami [29] [32] as enhancement to TWOACK scheme. Like TWOACK scheme, AACK is acknowledgment base scheme that solves the same two weaknesses of Watchdog, named, limited transmission power and receiver collision but with less routing overhead and calculations. However, it still suffers from false misbehavior report and collaborative attacks. However, Nan et al. [33] proposed EAACK scheme in 2010 as enhancement to AACK. It solves the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and false misbehaving report. However, it still suffers from collaborative attacks. More details about these schemes were explained in next section (related work).

According to failure of mentioned existing IDSs to work within presence of consecutive collaborative attacks, in this research, we proposed a new technique that overcomes the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and collaborative attacks with the presence of consecutive malicious nodes in a rout path.

1.4.2. Research Challenges

It is challenging to design a new instruction detection system (IDS) for MANETs. Due to the infrastructure-less and lack of administration point in MANET, it makes the collection of data in the whole network difficult. In addition, MANETs have limited resources, such as limited wireless bandwidth, computation ability and energy supply that we need to be considered when designing a new IDS framework for MANETs. Moreover, the distinction between false alarms and true alarms as a result of mobility are very difficult. For instance, a node can send wrong routing information due to free movement randomly or due to being compromised. Finally, it is challenging tradeoffs to increase network performance and reduce routing over head in MANETs.

1.4.3. Research Contributions

The contributions of this research include:

- Obtain general understanding of the security protocols in MANETs.
- Due to the failure of mentioned existing IDSs to work within presence of collaborative attacks, we proposed a new IDS that overcomes the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and collaborative attacks with the presence of collaborative attacks especially under the presence of two consecutive malicious nodes in a rout path.

- Implement the proposed IDS using NS-2 simulator and test it in low speed and high speed networks under various scenarios as well as compare the results with existing IDSs, such as AACK technique.

1.5. Research Organization

Chapter 1 of this thesis gives an overview of mobile ad hoc networks, mobile ad hoc routing protocols, intrusion detection systems, research challenges and research contributions as well. The rest of this thesis is organized as follows. Chapter 2 shows related work and problem statement. Chapter 3 describes system models and implementation of the new proposed A3ACKs intrusion detection system. Chapter 4 discusses research methodology, simulation configuration and the metrics used to evaluate network performance. Details about simulation results are presented in chapter 4 as well. Lastly, conclusions and future work are described also in this chapter.

CHAPTER 2

PROBLEM STATEMENT AND LITERATURE REVIEW

This chapter describes the problem statement, existing literature on malicious node detection mechanisms and describes limitations of existing IDSs as well.

2.1. Problem Statement

This research is based on Watchdog technique, so we start by describing Watchdog technique as well as its weaknesses in details, and then we identify our research problem statement in context of literature review of watchdog scheme.

2.1.1. Watchdog Technique

Watchdog technique was proposed by Sergio Marti et al. [30] and it represents the base intrusion detection technique that many of the recent researches depended on. They proposed two techniques (Watchdog and Pathrater) that improve the throughput in MANETs with the existence of selfish or malicious nodes that agree to forward packets but fail to do so. In ad-hoc network, a node is considered as misbehaving for overloaded, selfish, malicious, or broken. An overloaded node lacks the CPU cycles, buffer space, or available network bandwidth to forward packets. On the other hand, a selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node may launch a DoS (Denial of Service) attack by dropping

packets. A broken node might have a software fault that prevents it from forwarding packets.

The two mentioned techniques (Watchdog and Pathrater) were used to mitigate the decrease in the throughput in MANETs due to the above node characteristics. The Watchdog technique serves as an intrusion detection system that detects the presence of misbehaving nodes in the network, while Pathrater technique is proposed to respond to these misbehaving nodes by helping the routing protocol to avoid these nodes. When a node forwards a packet, the node's Watchdog verifies that the next node in the path also forwards the packet by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, it is considered misbehaving. Watchdog has misbehavior's counter, every time a node fails to forward the packet, the Watchdog increases the failures counter. If the counter exceeds a predefined threshold, it concludes that the node is misbehaving. As a result, this node is avoided in future transmission by choosing a new path from source to destination based on a simple route rating algorithm. The Pathrater run by each node in the network to combine knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. It uses the reliability metric instead of shortest path. Furthermore, each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. The Watchdog technique has its own advantages and drawbacks. The significant advantage of Watchdog is to detect misbehaving nodes

instead of just links. On the other hand, Watchdog has six disadvantages that may fail to detect a misbehaving node in the presence of: [1]

a) Ambiguous collisions: the collection prevents node A from overhearing the transmission of packet 1 from node B to C due to another packet, packet 2, sent from node S to A as shown in Figure 2-1.

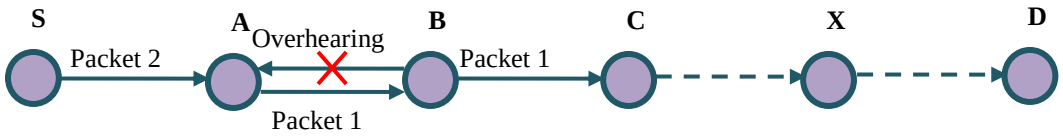

Figure 2-1: Ambiguous Collisions

b) Receiver collisions: Node A assure that node B has forwarded packet 1 to C, but fails to detect that node C didn't receive packet 1 due to collision with packet 2 from node X as shown in Figure 2-2.

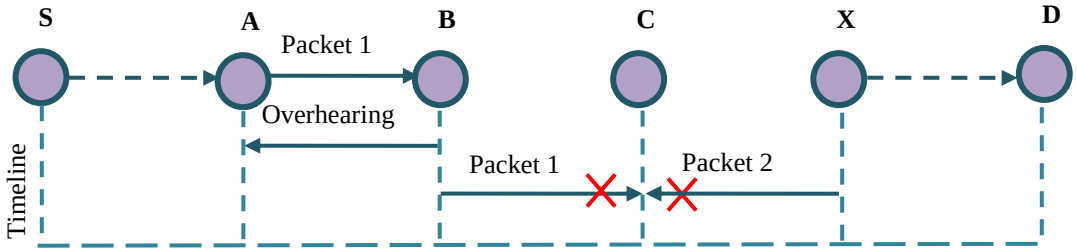

Figure 2-2: Receiver Collisions

c) Limited transmission power: in order conserve energy, a misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the previous node, but too weak to be received by the true recipient, such as node B

[1]All dotted arrow lines in the figures indicate the transmission over the rest of the route. However, all solid arrow lines indicate the transmission that is actually involved in our discussion.

limits it transmission power, so it is strong enough to be overheard by node A but too weak to be received by node C as shown in Figure 2-3.

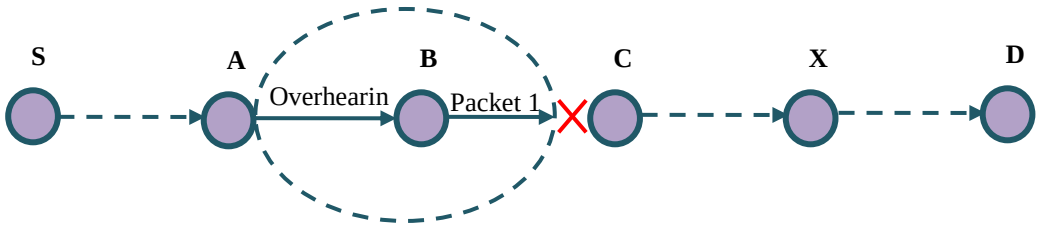

Figure 2-3: Limited Transmission Power

d) False misbehavior: This occurs when a node falsely reports other nodes as misbehaving. For example, node A reports node B as misbehaving node while node B successfully forwarded packet 1 to node C as shown in Figure 2-4.

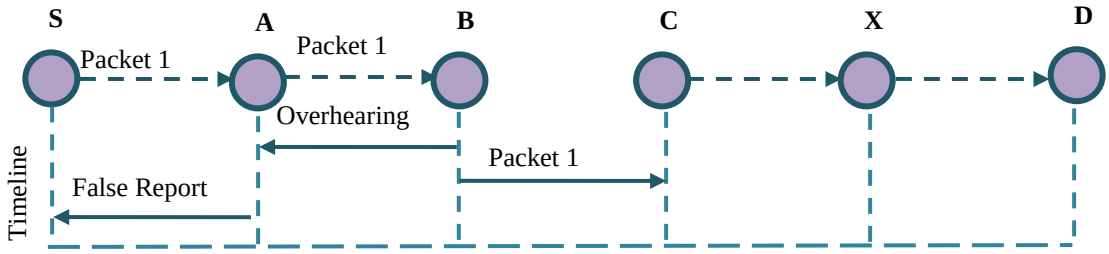

Figure 2-4: False Misbehavior Report

e) Collaborative attack (collusion attack): Multiple misbehaving nodes in ad-hoc network cooperate to perform sophisticated attack. For example, nodes B and C in Figure 2-5 could collude to cause mischief, where node B forwards a packet to node C but does not report to node A when C drops the packet. Because of this limitation, it may be necessary to disallow two or more consecutive untrusted nodes in a routing path.

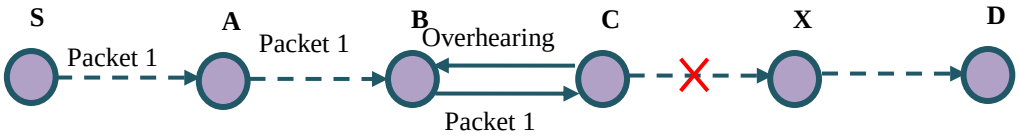

Figure 2-5: Cooperative attack

f) Partial dropping: a node can circumvent the Watchdog by dropping packets at a lower rate than the Watchdog's configured minimum misbehaving threshold, and this is call Gray Hole Attack.

2.1.2. Research Problem Statement

As discussed early Watchdog Technique has six weaknesses and some solutions are proposed for limited transmission power and receiver collision problems. To the best of our knowledge, none of the existing IDS protocols works with the presence of consecutive collaborative attacks, in this research, we proposed a novel IDS protocol that overcomes three significant weaknesses of Watchdog, mainly, limited transmission power, receiver collision and collaborative attacks with or without the presence of collaborative attacks especially if there are two consecutive malicious nodes in the route.

2.2. Related Work

Many researches have been proposed to improve the security of MANETs against misbehaving nodes. Watchdog technique, as mentioned early, is considered the basis for many proposed instruction detection system in MANETs. It is proposed by Marti et al. [30] and built based on Dynamic Source Routing (DSR) protocol. It mainly consists of

two parts, called, Watchdog and Pathrater that improve throughput in MANETs in presence of misbehavior nodes that agree to forward packets but fail to do so. The Watchdog technique serves as an intrusion detection system that detects the presence of misbehaving nodes in the network, while Pathrater technique is proposed to respond to these misbehaving nodes by helping the routing protocol to avoid these nodes. In addition, many researches have provided that the Watchdog technique is efficient and capable of detecting misbehavior or malicious nodes at forward level instead of links level. As a result, Watchdog scheme is considered the basis for many proposed instruction detection systems in MANETs. However, Watchdog scheme might not detect malicious nodes with the presence of: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion (collaborative) of malicious nodes, and 6) partial dropping as discussed in the previous section.

An enhancement scheme to Watchdog technique was proposed by Parker et al [34]. Unlike Watchdog, which is applicable just for DSR protocol, they proposed enhancement that can be applied to all routing protocols in MANETs. In contrary to the Watchdog, in this technique, every node in the MANET is able to overhear all the other nodes in its proximity and not just the node that is flow it up on the routing path. This mechanism can be considered as combination of two response modes, named, passive response mode and active response mode. In the first mode, passive response mode, every node works independently and finally the intrusive node blocks from using all network resources. On the other hand, in active response mode, the decision is done by cluster header by initiating a voting procedure to determine a node inside the networks as an intrusive node. If the majority of the nodes determine that the suspected node is fact

intrusive, an alert will be broadcast along the network as well as the intrusive node blocks from using all network resources.

An extended scheme to the Watchdog was proposed by Nasser at el. [35] called ExWatchdog. They proposed extended intrusion detection system for discovering malicious nodes in MANETs. They proposed a solution to the false misbehaving problem of Watchdog technique, where the real intruder or the malicious node falsely reports other nodes as misbehaving. In this technique, ExWatchdog, each node has a table; this table records the number of packets the node sends, forwards or receives respectively. When the source node receives a report about misbehaving node, the source node will find another path to destination node asking about the number of packets that it received. If the number of packets are equal to the number of the packets that the source node has sent, the real malicious node is the node that reported others nodes as misbehaving. Otherwise, the report is valid and the reported nodes are malicious nodes. However, the ExWatchdog still suffers from the availability of the misbehaving node in all available routes from source to destination.

All the previous solutions based on Watchdog mechanism. However, TWOACK was proposed by Balakrishnan et al. [31] replaces Watchdog and solves two of its problems, namely, receiver collision and limited transmission power. It is neither Watchdog- based scheme nor an enhancement to Watchdog technique. The TWOACK scheme detects misbehaving links by acknowledging every data packet transmitted from source to destination over ever three consecutive nodes along the path. It works on Dynamic Source Routing (DSR) protocol and achieved by special acknowledging packet called TWOACK. In TWOACK, the third node along the route from every three

consecutive nodes is required to send back an acknowledgement packet to the node that is two hops away from it down the route. For example, as in Figure 2-6, when node B receives packet 1 from A and forwards to C, node C (two hops away form A) is required to generate acknowledgement packet (TWOACK), which has reverse route from A to C, and send the TWOACK packet back to A indicating B has forwarded the packet 1 to C successfully. If A didn't get TWOACK packet from C within predefined time period, node A reports node B to be malicious node. The same process is carried out by every three consecutive nodes along the rest of route. Even though Watchdog scheme solved the limited transmission power and receiver collision, is still suffer from adds more overhead to the routing protocol because of the multiple acknowledgements for every packet along the route from source to destination, especially on a long path. Furthermore, TWOACK scheme detect misbehaving links instead of nodes and this gives the malicious node more chance to drop more packets on different links in same network.

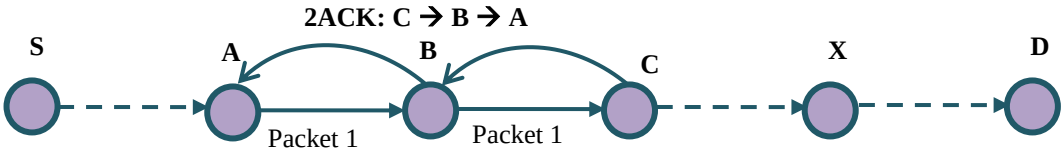

Figure 2-6: TWOACK scheme

A recent related work is done by Al-Roubaiey and Sheltami [29] [32]. In this work, they proposed an enhancement instruction detection system called AACK (Adaptive Acknowledgment) for solving two significant problem of Watchdog, namely, limited transmission power and receiver collision. Unlike TWOACK, AACK scheme reduced network overhead while still maintaining network throughput. Similar to TWOACK,

AACK scheme is an acknowledgment-based network layer scheme. AACK can be considered as combination of two modes controlled by switching system. The first mode called TACK mode where it works exactly similar to TWOACK scheme, as in Figure 2-6, except that it detects malicious nodes instead of links. In the TACK mode, every node needs to send back an acknowledgement packet to the node that is two hops away from it.

The second mode called ACKnowledge (ACK) mode, which is end-to-end acknowledgement. In ACK mode, the destination node is required to send back acknowledgement packet to the source node as shown in Figure 2-7.

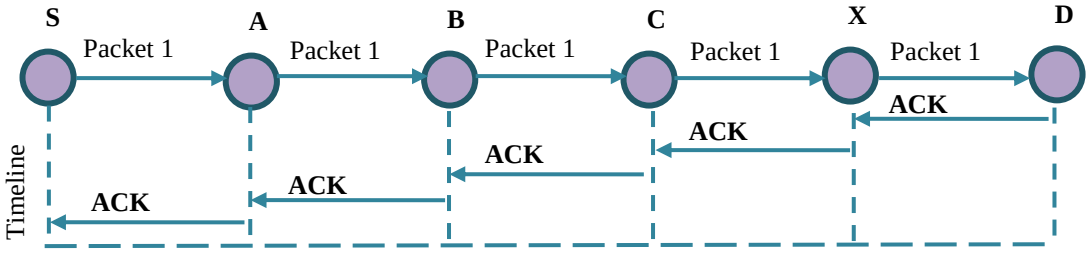

Figure 2-7: AACK scheme

For example, the AACK scheme starts with ACK mode (default mode) to send a packet from source to destination. For instance, packet 1 is forwarded simply by all intermediate nodes from the source node S to the destination node D over the whole path without any overhead except one bit of flag reserved in DSR header indicates the type of packet 1. When the destination node D receives packet 1 and within predefined time, it needs to send back an acknowledgement (ACK) packet along the reverse path to the source node S as shown in Figure 2-7. If the source node receives the ACK packet, then packet 1 has been transmitted successfully from the source node S to the destination node D. Otherwise, the source node S has to switch to the second mode of AACK scheme, TACK

mode, by sending TACK packet to the destination D. The TACK mode works similar to TWOACK scheme to detect malicious nodes along the whole path.

The AACK scheme uses hybrid modes, ACK and TACK, to reduce the network overhead. However, AACK still suffer from detect malicious nodes when there is a false misbehavior report or forged acknowledgement packet.

As enhancement to the AACK scheme, Nan et al. [33] proposed a new scheme called EAACK (Enhanced Adaptive ACKnowledgement) for solving four significant problems of Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and false misbehavior. The EAACK scheme can be considered as combination of three modes, namely, ACK mode, S-ACK mode (Secure-ACKnowledge), and MRA mode (Misbehavior Report Authenticate) controlled by switch system. The EAACK scheme starts with the first mode, ACK mode, to send a packet from source to destination without any overhead except two bits header of DSR indicate the type of the packet.

The first mode, ACK mode, is end-to-end acknowledgement scheme works exactly identical to ACK mode in AACK mechanism, discussed above in Figure 2-7, where the source node sends out the data packet to destination node after registering its ID and sending time. When the destination node received the data packet successfully, it is required to send back ACK packet to the source node. If the source node received the ACK packet, the packet has been sent to the destination and the transmission completed successfully. Otherwise, the source node switches to the second mode.

The second mode, S-ACK mode, is 2ACK scheme works exactly similar to TWOACK [31] scheme, as in Figure 2-6, except that it detects malicious nodes instead of

links. In the S-ACK mode, every three consecutive nodes, the third node is required to send back an S-ACK acknowledgement packet to the first node to confirm it has received the packet. However, unlike TWOACK scheme, in S-ACK mode, when a misbehavior report is received, instead of trusting the report and mark the node as misbehaving, the misbehaving report forwards to the source node. Then, the source node switches to MRA mode by sending out a MRA packet to the destination node via a different path. If there is no new path exists in the path, the source node creates a new DSR route request to find a new path.

The MRA mode is the third mode of EAACK scheme that is used by destination node to check its local memory looking for a requested packet ID. If it exists, the sending packet has been received successfully by the destination node and the node that is reported the false misbehavior report is a malicious node as shown in Figure 2-8. Otherwise, the misbehavior report is valid.

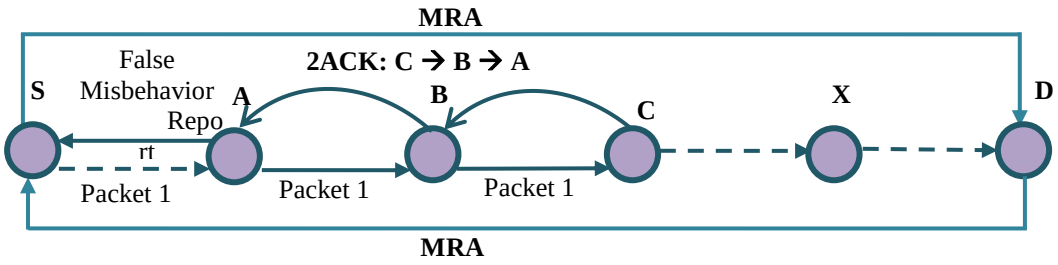

Figure 2-8: MRA scheme

Nevertheless**,** EAACK scheme is able to detect malicious node with the presence of false misbehaving report. It still suffer from detects malicious nodes when the attacker smart enough to forge the acknowledgement packet.

Another enhancement scheme proposed also by Nan et al. [36] called EAACK2. They extended EAACK [33] mechanism by applying Digital Signature Algorithm (DSA) to detect forged acknowledgment (acknowledgment authenticate) by preventing attackers from forging fake acknowledgment and thus conceive its malicious misbehavior. The EAACK2 can be considered also as combination of three modes, namely, ACK mode (ACKnowledge), S-ACK mode (Secure- ACKnowledge), and MRA mode (Misbehavior Report Authenticate) controlled by switch system. The EAACK2 scheme starts with the first mode, ACK mode, to send a packet from source to destination without any overhead except two bits header of DSR indicate the type of the packet.

The first mode, ACK mode, is end-to-end acknowledgement scheme works exactly identical to ACK mode in AACK [29][32] mechanism, as discussed above in Figure 2-7, where the source node sends out the data packet to destination node after registering its ID and sending time. When the destination node received the data packet successfully, it is required to send back an ACK packet to the source node. If the source node received the ACK packet successfully, the packet has been sent to the destination and the transmission completed successfully. Otherwise, the source node switches to S-ACK mode by sending an S-ACK packet to the destination node along the same path.

The S-ACK mode works similar to the TWOACK [31] scheme, as in Figure 2-6, except that it detects malicious nodes instead of links. In the S-ACK mode, every three consecutive nodes, the third node is required to send back an S-ACK acknowledgement packet to the first node to confirm it has received the packet. However, unlike EAACK [33] scheme, in the EAACK2, the third node needs to sign the S-ACK acknowledgment packet with its own digital signature to prevent the second node from forging the S-ACK

acknowledgment packet without forwarding the packet to the third node. In addition, to avoid creating black-hole in the network by a malicious node without detecting, when the first node received the S-ACK packet from the third node, it has to verify the third node's signature using predefined public key. However, if the first node didn't receive this S-ACK packet with the predefined time, the first node reports both the second and the third nodes as malicious node by sending a misbehavior report packet to the source node. However, when the source node receives the misbehavior report packet, it switches to MRA mode instead of trust the misbehavior report immediately and mark the nodes as misbehavior nodes.

In the MRA mode, the source node sends MRA packet to the destination node via different route. If there is no new path exists in the path, the source node creates a new DSR route request to find a new path. When the destination node receives the MRA packet, the MRA packet has data packet ID, it checks its local memory to find out if the request packet's ID exists or not. If it exists, the sending packet has been received successfully and the node that is reported the false misbehavior report marks as a malicious node as shown in Figure 2-8 above. Otherwise, the misbehavior report is valid and confirmed. Even though**,** EAACK2 mechanism is able to solve the problem of forge acknowledgment packets. It suffer from detects malicious nodes with the presence of collaborative attacks.

Shakshuki et al. [37] proposed another enhancement mechanism for AACK scheme named EAACK. They extended AACK [29][32] mechanism by applying Digital Signature Authenticate using DSA (Digital Signature Algorithm) and RSA (Rivest, Shamir and Adleman) algorithms to detect forged acknowledgment by preventing

attackers from forging fake acknowledgment as well as they implemented both DSA and RSA algorithms to find the most optimal solution that can be used in MANETs. Like EAACK2 [34] scheme, the EAACK can be considered as combination of three modes, namely, ACK mode (ACKnowledge), S-ACK mode (Secure- ACKnowledge), and MRA mode (Misbehavior Report Authenticate) controlled by switch system. The EAACK scheme starts with the first mode, ACK mode, to send a packet from source to destination without any overhead except two bits header of DSR indicate the type of the packet.

The first mode, ACK mode, is end-to-end acknowledgement scheme works exactly similar to ACK mode in AACK [29][32] mechanism, as discussed above in Figure 2-7, where the source node sends out the data packet to destination node after registering its ID and sending time. When the destination node received the data packet successfully, it is required to send back an ACK packet to the source node. If the source node received the ACK packet successfully, the packet has been sent to the destination and the transmission completed successfully. Otherwise, the source node switches to S-ACK mode by sending an S-ACK packet to the destination node along the same path.

The S-ACK mode works identical to the TWOACK [31] scheme, as in Figure2- 6, except that it detects malicious nodes instead of links. In the S-ACK mode, every three consecutive nodes, the third node is required to send back an S-ACK acknowledgement packet to the first node to confirm it has received the packet. However, in the EAACK, the third node needs to sign the S-ACK acknowledgment packet with its own digital signature to prevent the second node from forging the S-ACK acknowledgment packet without forwarding the packet to the third node. In addition, to avoid creating black-hole in the network by a malicious node without detecting, when the first node received the S-

ACK packet from the third node, it has to verify the third node's signature using predefined public key. However, if the first node didn't receive this S-ACK packet with the predefined time, the first node reports both the second and the third nodes as malicious node by sending a misbehavior report packet to the source node. However, when the source node receives the misbehavior report packet, it switches to MRA mode instead of trust the misbehavior report immediately and mark the nodes as misbehavior nodes.

In the MRA mode, the source node sends MRA packet to the destination node via different route. If there is no new path exists in the path, the source node creates a new DSR route request to find a new path. When the destination node receives the MRA packet, the MRA packet has data packet ID, it checks its local memory to find out if the request packet's ID exists or not. If it exists, the sending packet has been received successfully and the node that is reported the false misbehavior report marks as a malicious node shown in Figure 2-8 above. Otherwise, the misbehavior report is valid and confirmed.

Regarding the DSA (Digital Signature Authenticate), EAACK is an acknowledgement –based intrusion detection system that means all the three modes, namely, ACK, S-ACK, and MRA are acknowledgement-based detection schemes. Therefore, they all depend on acknowledgement packets to detect malicious nodes in the network. Thus, it is too important to be sure all the packets in the EAACK are authentic and unpolluted. At the end, the authors concluded that the DSA (Digital Signature Algorithms) algorithm is the most optimal solution to be applied in MANETs to solve the

problem of forge acknowledgment packets. However, EAACK scheme still suffers from detects malicious nodes with the presence of collaborative attacks.

2.3. Limitations of existing IDSs for MANETs

There are many researches proposed, as explained early, to mitigate and solve the problem of packet dropping attacks in MANETs. According to the previous literature review, most of these proposed researches depend on Watchdog scheme. Some of these researches have improved the detection efficiency without solving the weaknesses of Watchdog. On the other hand, some of these researches have enhanced Watchdog scheme to work under different types of MANETs routing protocol rather than DSR protocol. In addition, some of them have extended Watchdog scheme to overcome the false misbehaving problem of Watchdog technique, such as ExWatchdo scheme. However, some of these researches are considered replacement to Watchdog scheme by solving Watchdog's drawbacks as well as they are considered acknowledgement base mechanisms. These mechanisms include TWOACK and AACK, EAACK schemes.

The TWOACK scheme was proposed in 2005 by Balakrishnan et al. [31]. It is acknowledgement base scheme that solves two weaknesses of Watchdog, named, limited transmission power and receiver collision. However, it solves these two weaknesses with more routing overhead and calculations that effect network's performance. In addition, it inefficient since it detects misbehaving links instead of nodes in which it gives more chance to the malicious node to drop more packets in each link it appears. Lastly, it still suffers from collaborative attacks.

On the other hand, the AACK scheme was proposed in 2009 by Al-Roubaiey and Sheltami [29] [32] as enhancement to TWOACK scheme. Like TWOACK scheme, AACK is acknowledgment base scheme that solves the same two weaknesses of Watchdog, named limited transmission power and receiver collision but with less routing overhead and calculations since it uses hybrid schemes. However, it still suffers from false misbehavior report and collaborative attacks. However, Nan et al. [33] proposed EAACK scheme in 2010 as enhancement to AACK. It solves the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and false misbehaving report. But, it still suffers from collaborative attacks. More details about these schemes were explained in previous section (related work).

Due to failure of mentioned existing IDSs to work within presence of consecutive collaborative attacks, in this research, we proposed a new technique that overcomes the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and collaborative attacks with the presence of consecutive malicious nodes in a rout path. It also improved the detection accuracy by doing nodes detection instead of links detection.

CHAPTER 3

SYSTEM MODELS AND DESIGN

3.1. Overview

In MANETs, as discussed, misbehaving nodes that participate at routing information exchange and drop data packets pass through called *packet dropping attacks*. Therefore, misbehaving nodes degrade MANETs's performance sharply by dropping data packets that pass through. These misbehaving nodes, as explained, classify into *selfish nodes* and *malicious nodes*. The selfish *nodes* participate to carry out routing control packets and drop data packets to save its energy and bandwidth. The *malicious nodes* also participate to carry out routing control packets and drop all data packets to disrupt the availability and connectivity of the network. In addition, the malicious nodes are divided into two types, named, *black-hole attacks* and *gray-hole attacks* [29]. The black hole attacks drop all data packets that pass through. On the other hand, the gray-hole attacks are smart enough to drop some of data packet that pass through by adjusting its packets dropping rate to IDS's detection threshold. Therefore, it is difficult to the IDS to detect the gray-hole attack unlike black-hole attack. However, the black-hole attacks have affected the network's performance more than the gray-hole attacks as the first one drop all data packet pass through. As a result, it disrupts the availability and connectivity of the network, which are considered serious metrics for network's performance.

There are many solutions are proposed to mitigate the problem of packets dropping in MANETs. Watchdog mechanism was the early technique to mitigate the problem of packets dropping in MANETs and it was proposed in 2000 by Marti et al. [30]. However, Watchdog scheme, as discussed, has six weaknesses include: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion (collaborative) of malicious nodes, and 6) partial dropping. On the other hand, there are several solutions proposed based on Watchdog scheme to overcome its drawbacks. Some of these researches, according to literature review, have improved the detection efficiency without solving the weaknesses of Watchdog. In addition, some of them have enhanced Watchdog scheme to work under different types of MANETs routing protocol rather than DSR protocol. Moreover, some of them have extended Watchdog scheme to overcome the false misbehaving problem of Watchdog technique, such as ExWatchdo scheme by Nasser at el.[35]. Lastly, some of these researches are considered as replacement to Watchdog scheme because they are solving Watchdog's weaknesses as well as they are considering acknowledgement base mechanisms. These mechanisms include TWOACK and AACK, EAACK schemes. The TWOACK scheme was proposed in 2005 by Balakrishnan et al. [31]. It is acknowledgement base scheme that solves two weaknesses of Watchdog, named, limited transmission power and receiver collision by verifying packets delivery over every three consecutive node over a path between a source and a destination. However, it solves these two weaknesses with more routing overhead and calculations that effect network's performance. In addition, it inefficient since it detects misbehaving links instead of nodes

in which it gives more chance to the malicious node to drop more packets in each link it appears. As a result, it still suffers from collaborative attacks.

On the other hand, the AACK scheme was proposed in 2009 by Al-Roubaiey and Sheltami [29] [32] as enhancement to TWOACK scheme. It is also acknowledgment base scheme that solves the same two weaknesses of Watchdog, named limited transmission power and receiver collision but with less routing overhead and calculations since it uses hybrid schemes. But, it still suffers from false misbehavior report and collaborative attacks. However, Nan et al. [33] proposed EAACK scheme in 2010 as enhancement to AACK. Even though the EAACK scheme solves the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and false misbehaving report, it still suffers from collaborative attacks.

Due to failure of mentioned existing IDSs to work within presence of consecutive collaborative attacks, in this research, we proposed a new technique that overcomes the three significant weaknesses of Watchdog, named, limited transmission power, receiver collision and collaborative attacks with the presence of consecutive malicious nodes in a rout path. It also improved the detection accuracy by doing nodes detection instead of links detection.

3.2. Problem Definition

Our proposed approach A3ACKs, pronounced as Adaptive Three ACKnowledgements, is extended to AACK scheme, but it is designed to solve its drawbacks by talking three significant weaknesses of Watchdog scheme, named, limited transmission power, receiver collision and collaborative attacks (collusion attack)

especially when there are two consecutive collaborative malicious nodes in a route path. In this section, we discuss these three weaknesses in details.

a) Receiver collisions: Node A assure that node B has forwarded packet 1 to C, but fails to detect that node C didn't receive packet 1 due to collision with packet 2 from node X as shown in Figure 3-1.

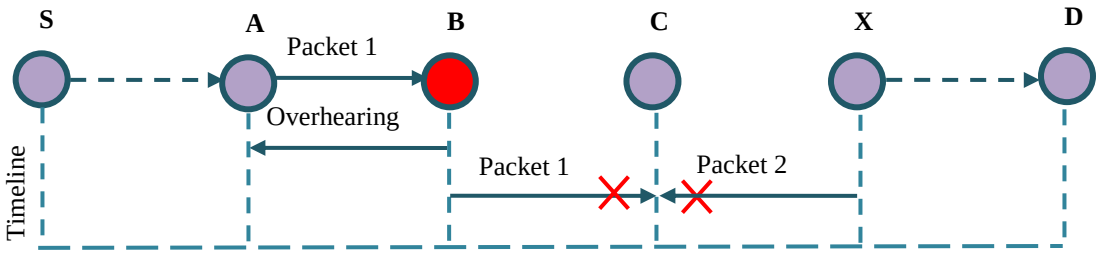

Figure 3-1 : Receiver Collisions problem.

In this case, node B is smart attack who can cheat the monitor node A and intend to do a collision at the next hop node C by sending the packet 1 while the received node C busy with other transmissions from node X.

b) Limited transmission power: In order conserve energy, a misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the previous node, but too weak to be received by the true recipient, such as node B limits its transmission power, so it is strong enough to be overheard by node A but too weak to be received by node C as shown in Figure 3-2.

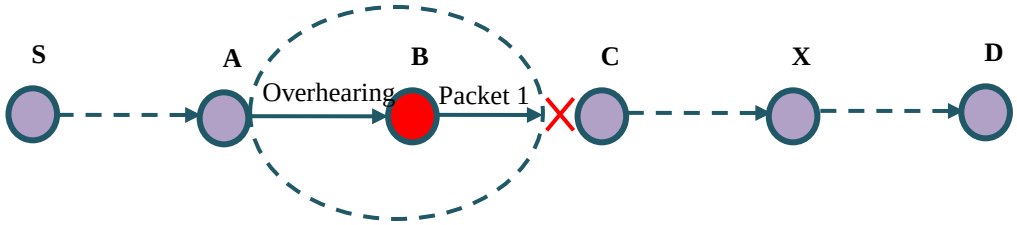

Figure 3-2: Limited Transmission Power problem.

In this case, node B is smart attack that can control its transmission power to let the monitor, node A, overhears its transmission while the next hop node C is out of its range.

c) Collaborative attacks (collusion attacks): Multiple misbehaving nodes in ad-hoc networks cooperate to perform sophisticated attack. In another word, if there are two consecutive collaborative misbehaving nodes in a route path, they are cooperative to drop any data packet. For example, nodes B and C in Figure 3-3 could collude to cause mischief, where node B forwards packet 1 to node C but does not report to node A when node C drops the packet 1, that means node B cooperates with node C to drop packet 1.

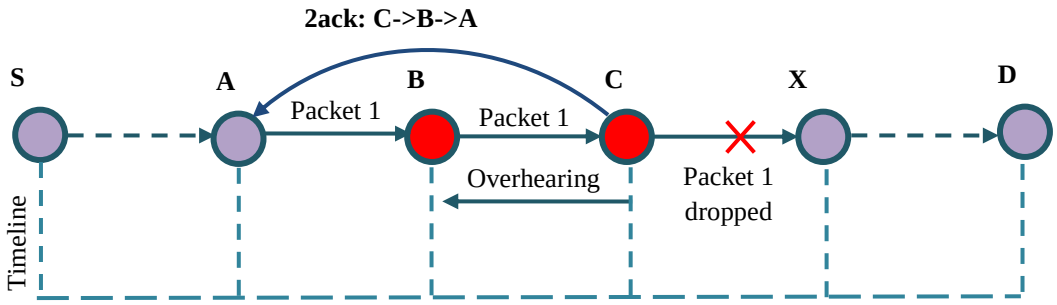

Figure 3-3: Collaborative attacks.

We conclude that the TWOACK and AACK schemes fail to detect two consecutive collaborative misbehaving nodes in a route path because both of them based on send back *2ACK* packet to a sender of a data packet two hops away in opposite direction to verify

packets delivery over every three consecutive node over a path between a source and a destination. However, as in Figure 3-3, two consecutive misbehaving nodes are able to send back 2ACK packet to a sender of a data packet two hops away in opposite direction and drop the data packet as well. In this case the TWOACK and AACK existing schemes are vulnerable to the consecutive collaborative attacks problem.

In this research, we propose a novel IDS technique that is designed mainly for MANETs, which solves all of receiver collision, limited transmission power and collaborative attacks within presence of two consecutive collaborative misbehaving nodes in a route path. It also improved the detection accuracy by doing malicious nodes detection instead of links detection.

3.3. Model Assumptions

The assumptions in this research include:

- Our proposed technique works on any source routing protocol, such as DSR protocol.
- Source and destination cannot be misbehaving nodes.
- We assume each pair of nodes use bi-direction communication.
- We assume that the misbehaving nodes are working as collaborative attacks to drop any data packets if there are two consecutive misbehaving nodes in a route path. Also, we assume that the misbehaving nodes are working as non-collaborative attacks to drop any data packets if they are not consecutive in a route path.

- We assume that the misbehaving nodes are participating to forward control or information packets as well as they are participating in the routing discovery and maintenance.
- We assume that the misbehaving nodes are controlling their transmission power to produce limited transmission problem.
- Finally, we assume that the misbehaving nodes are trying to generate receiver collision at a receiving node by sending packets while the received node busy with other transmissions.

3.4. A3ACKs Scheme Model

In this section, we describe our new proposed scheme models, node models and switching system models as well.

3.4.1. A3ACKs Scheme Description

In this subsection, we describe our proposed scheme in details. As explained in section 3.2, A3ACKs is abbreviation of *A*daptive *Three ACK*nowledgements. It is an extension to AACK scheme, it is designed to complement AACK by solving three weaknesses of Watchdog scheme, namely: limited transmission power, receiver collision and collaborative attacks (collusion attack) especially when there are two consecutive collaborative malicious nodes in a route path. The A3ACKs scheme is a network layer acknowledgement based scheme, which is considered as combination system consists of three major models: End-To-End Acknowledgement (*Aack*) model, Two

Acknowledgement (*Tack*) model and Three Acknowledgment (*Thack*) model. It is built on DSR protocol due to it needs a source route protocol. Details about these models as follow:

3.4.1.1. Aack Model

As discussed previously, *Aack* model is basically End-To-End Acknowledgement model. It works as a part of the hybrid scheme in *A3ACKs technique*. It is the default model of *A3ACKs* mechanism and aims to reduce the routing overhead of networks when there is no misbehaving node detected in an active route path. Figure 3-4 shows the Aack model.

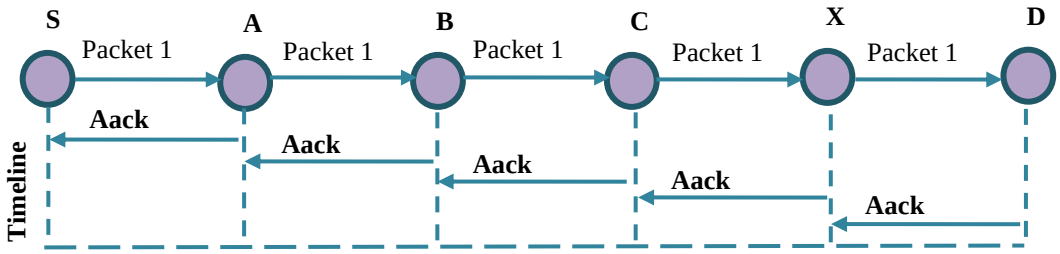

Figure 3-4: Aack Model Procedure of *A3ACKs* Scheme

In *Aack* model, a sender node S starts sending out an *Aack* data packet to a destination node D and stores the ID and sending time of the sending Aack data packet. In this model all intermediate nodes along the active route should cooperative to relay the *Aack* data packet to the destination node D by only forwarding it to next hop without saving the ID or sending time of the sending data packet. If the destination node D successfully received the *Aack* data packet from the source node S, the destination node is required to send back acknowledgement packet (*Aack*) to the source node S within predefined timeout over the same route but in a reverse order. Otherwise, the sender node S has to

switch to *Tack* mode by sending out *Tack* data packet to destination node D to detect if there is a misbehaving node in the active route path.

3.4.1.2. Tack Model

The *Tack* model is enhanced version of TWOACK technique proposed by Liu et al. [11] except that the *Tack* model in *A3ACKs* scheme is able to perform nodes detection instead of links detection. The principle of *Tack* model is to make every three consecutive nodes work together in a group to detect misbehaving nodes in a route path. That means, for every three consecutive nodes in a route path the third node, which is two hops away from the first one, is required to send back acknowledgement packet (*Tack*) to the firs node in that group within predefined timeout. For example, as in Figure 3-5, when node B receives packet 1 from A and forwards to C, node C (two hops away form A) is required to generate an acknowledgement packet (*Tack*), which has reverse route from A to C, and sends the *Tack* packet back to A indicating B has forwarded the packet 1 to C successfully. If A didn't get *Tack* packet from C within predefined time period, node A reports node B as malicious node. The same process is carried out by every three consecutive nodes along rest of the route path.

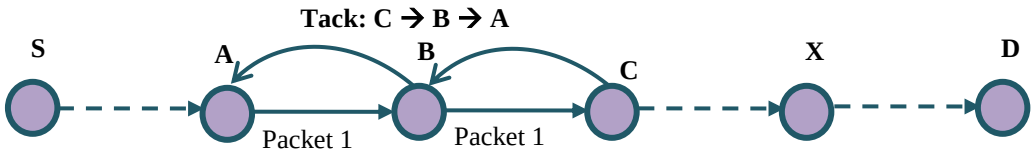

Figure 3-5: Tack Model Procedure of *A3ACKs* Scheme

As a result, the Tack mode, in *A3ACKs technique*, aims to detect misbehaving nodes with the presence of receiver collision and limited transmission power. However, if the source node S still does receive neither acknowledgement packet (*Tack*) nor alarm with a predefined timeout, it has to switch to *Thack* model by sending out *Thack* data packet to detect if there are any two consecutive collaborative misbehaving nodes in the route path as explained in section 3.2.

3.4.1.3. Thack Model

The *Thack* model is not only used to solve the problems of receiver collision and limited transmission power but also to solve the problem of consecutive collaborative attacks within the presence of two consecutive collaborative misbehaving nodes in a route path. The principle of the Thack model is to make every four consecutive nodes work together in a group to detect if there are any two consecutive collaborative misbehaving nodes in a path. That means, for every four consecutive nodes in a path fourth node, which is three hops away from the first one, is required to send back acknowledgement packet (*Thack*) to the firs node in that group within predefined timeout as in shown in Figure 3-6.

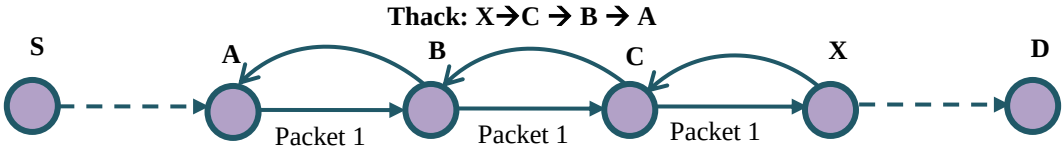

Figure 3-6: Thack Model Procedure of *A3ACKs* Scheme

For example, when node C receives packet 1 from B and forwards to X, node X (three hops away form A) is required to generate an acknowledgement packet (*Thack*), which

has reverse route from A to X, and sends it back to A indicating B and C have forwarded packet 1 to X successfully. If A didn't get the *Thack* packet from X within predefined time period, node A reports nodes B and C as malicious nodes. The same process is carried out by every four consecutive nodes along rest of the route path.

By adaption these three models, the new *A3ACKs* technique solves all of receiver collision, limited transmission power and also consecutive collaborative attacks problems within the presence of two consecutive collaborative misbehaving nodes in a route path as explained in section 3.2.

3.4.2. Node Models

In this subsection, we discussed two types of nodes that are used in our implementation of the *A3ACKs* mechanism, named, *regular nodes* and *misbehaving nodes*.

3.4.2.1. Regular Node Model

As discussed, we have implemented the *A3ACKs* mechanism over DSR protocol using NS2 simulator, and regular nodes have modified to work within *A3ACKs* mechanism in proper behavior. Regard NS2, the regular nodes are classified into three types based on node's event or action: *source node, forward node* and *destination node*. In this research, we have modified the functionality of the regular nodes to work properly with the *A3ACKs* mechanism as follow:

1. **Source node**, which represents the initiator source of sent packets. We have modified source nodes to work properly in the mentioned three models (Aack, Tack, and Thack) of the *A3ACKs* mechanism. The source nodes are responsible to switch between these three models based on switch system procedure as will be discussed in

next section. In addition, they are responsible to select a suitable route path to destination. Finally, they are responsible to change the route path if there is a problem and select another one that does not pass through detected malicious nodes.

2. **Forward node**, represents the intermediate node between source and destination that receives sent packets from source and forwards them to destination. There may be more than one forward node along a route path between source and destination. We have modified the forward or intermediate nodes to perform different functions according to the used model (Aack, Tack, or Thack) of the *A3ACKs* mechanism. Thus, if the *A3ACKs* mechanism works in the default *Aack* model, the forward nodes have to work only as regular nodes with basic function of DSR protocol by forwarding the received packets to next hop in an active route path. However, if the *A3ACKs* mechanism works in Tack model, they have to work according to the *Tack* model where every three consecutive nodes in a route path work together as group and the third node which is two hops away from the first one is required to send back acknowledgement packet (*Tack*) to the firs node in that group within predefined timeout as explained in section 3.4.1.2. On the other hand, if the *A3ACKs* mechanism works in Thack model, the forward nodes have to work according to the Thack model where every four consecutive nodes in a route path work together as group and the fourth node which is three hops away from the first one is required to send back acknowledgment packet (*Thack*) to the first node in that group with predefined timeout as explained in section 3.4.1.3.

We conclude that the *A3ACKs* mechanism works most of the time in the *Aack* default model and forward nodes work only as regular DSR protocol nodes by

forwarding received packets to next hop. As a result, the *A3ACKs* mechanism saves energy consumption, which is significant factor in MANETs. It saves memory space as well because there is no need to save packet ID and sending time at every intermediate node along a route path when the *A3ACKs* mechanism works in the Aack default model as explained in section 3.4.1.1. Figure 3-7 shows the forward or intermediate node activity or function in the A3ACKs mechanism.

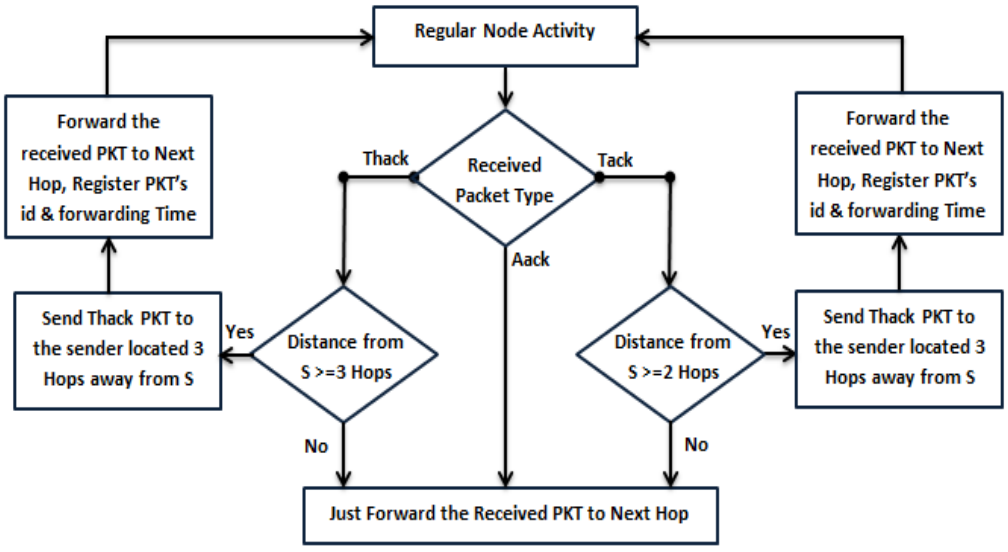

Figure 3-7: Forward Node activity.

3. **Destination node**, which represents the final destination of received packets. We also have modified the destination nodes to perform different functions according to the used model (Aack, Tack, or Thack) of the *A3ACKs* mechanism. Thus, if the *A3ACKs* mechanism works in the default *Aack* model, the destination nodes have to send back only acknowledgement packet (*Aack*) over the active route path in opposite direction to the source of received data. However, the destination node works as forward node, when the *A3ACKs* mechanism works in Tack, or Thack models as discussed, except

that the destination node will not saving the ID and sending time of received data packet since it is the final target of that data packet. In addition, the destination node has to send a switch packet to the source node to change its model to default Aack model. Details about the switch packet will discuss in next section. Figure 3-8 shows destination node activity or function, in the *A3ACKs* mechanism, when it receives data packet from a source node.

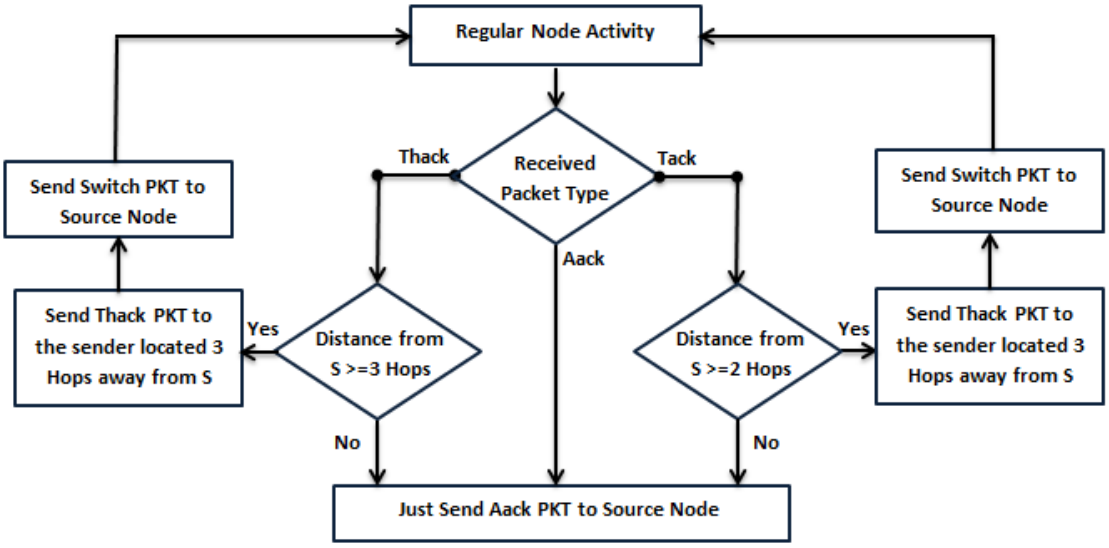

Figure 3-8: Destination Node Activity.

3.4.2.2. Misbehaving Nodes Model

4. In this research, we use the terminology misbehaving nodes to represent both selfish and malicious nodes because both of them drop all data packets that pass through. However, they work as regular nodes by exchanging routing or information packets with their neighbors. Also, they cooperative with other nodes in route discovery or route maintenance of DSR protocol. That means, misbehaving nodes drop all data

packets that pass through but they forward all routing or information packets in a route path. Figure 3-9 shows misbehaving node activity or function, in the *A3ACKs* mechanism, when it receives data packet or routing packet from a regular node in active route path. More details about misbehaving nodes configuration or implementation in our simulation environment will be explained later in our methodology.

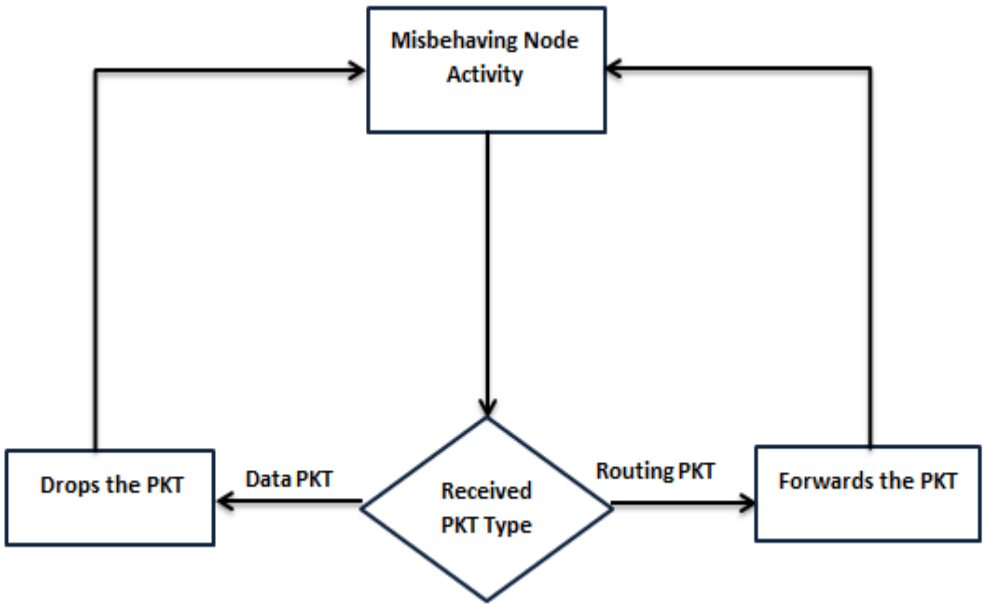

Figure 3-9: Misbehaving Node Activity

3.4.3. Switching System Model

As discussed in section 3.4.1, the *A3ACKs* mechanism is a hybrid system consists of three models (Aack, Tack and Thack) and it needs a dynamic technique to switch between these three models. Thus, we proposed dynamic switch system that enables source node to switch between these three models. Regards the Internet draft of DSR

protocol [37], there is a six bits reserved in the DSR fixed portion header as shown in Figure 3-10. The fixed portion of the DSR header is used to carry information that must be present in any DSR header. In *A3ACKs* mechanism, we use 2 bits from these 6 bits in order to classify different packet types for the three models of *A3ACKs* scheme.

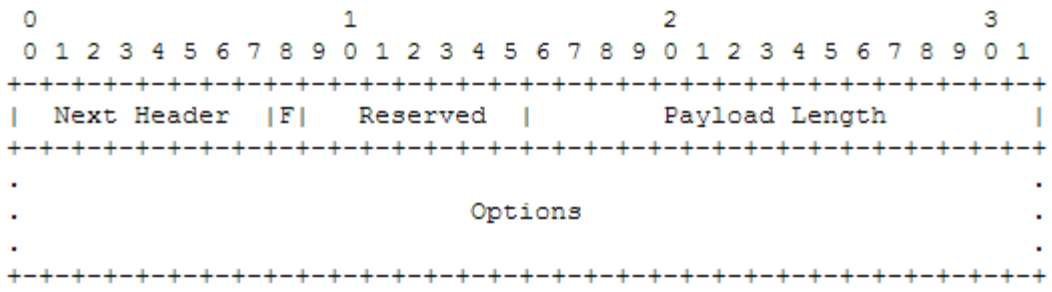

Figure 3-10: Internet Draft of DSR Protocol Header Format [37]

Table 3-1 shows details about different flag packet types for the three models in the proposed *A3ACKs* mechanism.

Packet Type	Aack Packet	Tack Packet	Thack Packet
Packet Flag	01	10	11

Table 3-1: Packet Type Indicators of A3ACKs scheme

The sender node specifies packet type depending on active model as well as it is responsible to switch between these models according to dynamic switching system procedure as shown in Figure 3-11.

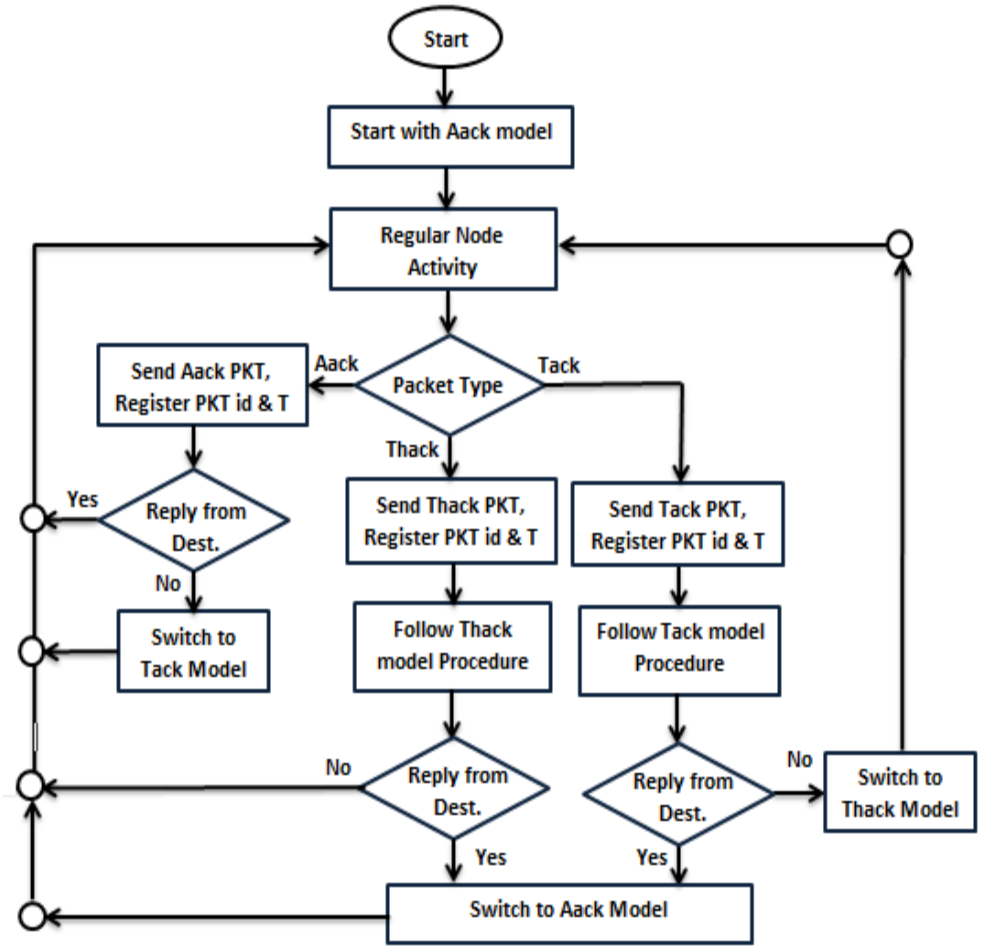

Figure 3-11: Dynamic Switch System Procedure of *A3ACKs* scheme.

In *A3ACKs* technique, each node in the network operates in three models, named, Aack, Tack and Thack as disused before. Therefore, switching system is used to enable the source node to switch between these three models. However, the default model is the Aack mode; that means the source node starts working in Aack model to reduce network routing overhead until it faces timeout event. Then, it switches to Tack model to detect if there are any misbehaving nodes in active route path. It continue works in Tack model until it receives either acknowledgment packet (Tack) or alarm then it switches to Aack model again. Otherwise, the source node has to switch to Thack model to detect if there

are any consecutive collaborative misbehaving nodes in active roué path. Also, it continues working in Thack model until it receives either acknowledge-ment packet (Thack) or alarm then it switches to Aack model again.

By using the switching system, the intermediate nodes can be known what the flow model is. That means, the intermediate nodes can decide whether they have to just forward the packet (in case of Aack model) or they have to send Tack packet to the previous two haps node (in case of Tack model) , or they have to send Thack packet to the previous three hops node (in case of Thack model). Details about switch system procedure of the A3ACKs technique are presented in the above Figure 3-11.

3.4.4. Timeout Threshold

Timeout threshold is a very significant element and its value affects the accuracy of the used detection system. So if it is too large, the misbehaving nodes will have more chance to drop more packets. However, if it is too small, it could reduce network performance sharply due to increase the false alarms inside the network. In this research, we compare our new technique *A3ACKs* with the existing *AACK* technique. So, we need to evaluate both of the existing AACK and the new A3ACKs techniques. The AACK technique consists of two models: the first model is TWOACK model, which is similar to TWOACK technique where the third node must send back an acknowledgement packet to the first node in every three consecutive nodes along the path. The second model is End-To-End model (AAck) where the destination node must send back an acknowledgement packet to the source node that sent the received data packet. As a result, the AACK technique has two timeout thresholds: one for first model and another

for second model. The timeout threshold of the first model is identical to timeout threshold of TWOACK technique ($TAck_{Tout}$), which it is defined as the period of time from sending a data packet to receiving the acknowledgment of the same data packet. This timeout was calculated by Al-Rouby [29] experimentally and the average value is taken. It was set to $TAck_{Tout}$ = 0.2 second. However, the timeout threshold in second model, named $AAck_{Tout,}$ is a variable depends on the number of hops in a path from source to destination. It was calculated by Al-Robai [29] according to equation 3-1:

$$\boldsymbol{AAck_{Tout} = \frac{TAck_{Tout}}{2} \times Number\ of\ Hops} \text{ ..... (3-1)}$$

On the other hand, the *A3ACKs* technique has three models: End-To-End Acknowledgement model (Aack), two acknowledgement model (Tack) and three Acknowledgement model (Thack) as discussed. The procedures for both Aack and Tack models are similar as the End-To-End model and TWOACK model respectively in the AACK technique. Thus; the timeout thresholds of the Aack model and Tack models in the A3ACKs scheme are same as the timeout thresholds in the AACK technique. As a result, Tack model timeout threshold of A3ACKs scheme is set to 0.2 second and Aack model timeout threshold of A3ACKs scheme is calculated according to equation 3-2:

$$\boldsymbol{Aack_{Tout} = \frac{TAck_{Tout}}{2} \times Number\ of\ Hops} \text{ ..... (3-2)}$$

However, the procedure in Thack model of A3ACKsscheme works as follow: the fourth node must send back an acknowledgement packet to the first node in every four consecutive nodes along a route path. Therefore, the timeout threshold of Thack model in A3ACKs technique can be calculated according to equation 3-3:

$$\boldsymbol{Thack_{Tout} = \frac{TAck_{Tout}}{2} \times 3} \text{ ..... } \textit{(3-3)}$$

Where 3 represents the number of hops in Thack model over it the acknowledgement packet is sent back by fourth node in ever four consecutive nodes along a route path in the *A3ACKs* technique.

CHAPTER 4

METHODOLOGY AND PERFORMANCE EVALUATION

This chapter discusses our simulation environment including simulator description, simulation methodology and simulation configuration as well. In addition, it presents the used metrics to evaluate our network performance. Moreover, it shows details about our simulation results and discussion. Lastly, conclusion and future work are presented at the end of this chapter.

4.1. Simulation Environment

In this section, we describe the simulator tool, simulation methodology and simulation configuration as well.

4.1.1. Simulator Description

To demonstrate the feasibility of our proposed system, we implemented it using Network Simulator-2 (NS-2) version 2.34. NS-2 is a flexible, open source, and free simulator tool. It is a good simulation tool for researchers and the most common simulator used for MANETs [39]. The simulator is written in C++; it uses OTcl as a command and configuration interface. NS v2 has three substantial changes from NS v1 as follow: (1) the more complex objects in NS v1 have been moved into simpler

components for greater flexibility and compensability; (2) the configuration interface is now OTcl, an object oriented version of Tcl; and (3) the interface code to the OTcl interpreter is separate from the main simulator. The benefits of this design come from the execution speed of the C++ compiled network objects and rapid reconfigure-ability of interpreted OTcl configuration objects. As a result, it is convenient to have a fast reconfigurable simulator as the foundation for using the dual interpreter/compiled class hierarchy. If there are changes in OTcl simulation parameters, there are no need to recompile; thus, a researcher can run large sets of simulation with a one-time compilation of the C++ network objects. Moreover, the control parameters and functions of the C++ compiled objects are exposed to the OTcl interpreter through OTcl linkage. Furthermore, for every OTcl object invoked in the interpreter hierarchy there is a mirrored object created in the C++ hierarchy. Lastly, NS-2 simulator can be downloaded directly from NS-2 website. More details about NS-2 can be found NS-2 documentation [39]. Figure 4-1 shows a survey of simulation-based papers in ACM's international Symposium on Mobile Ad Hoc networking and computing conference 2000-2005 [38].

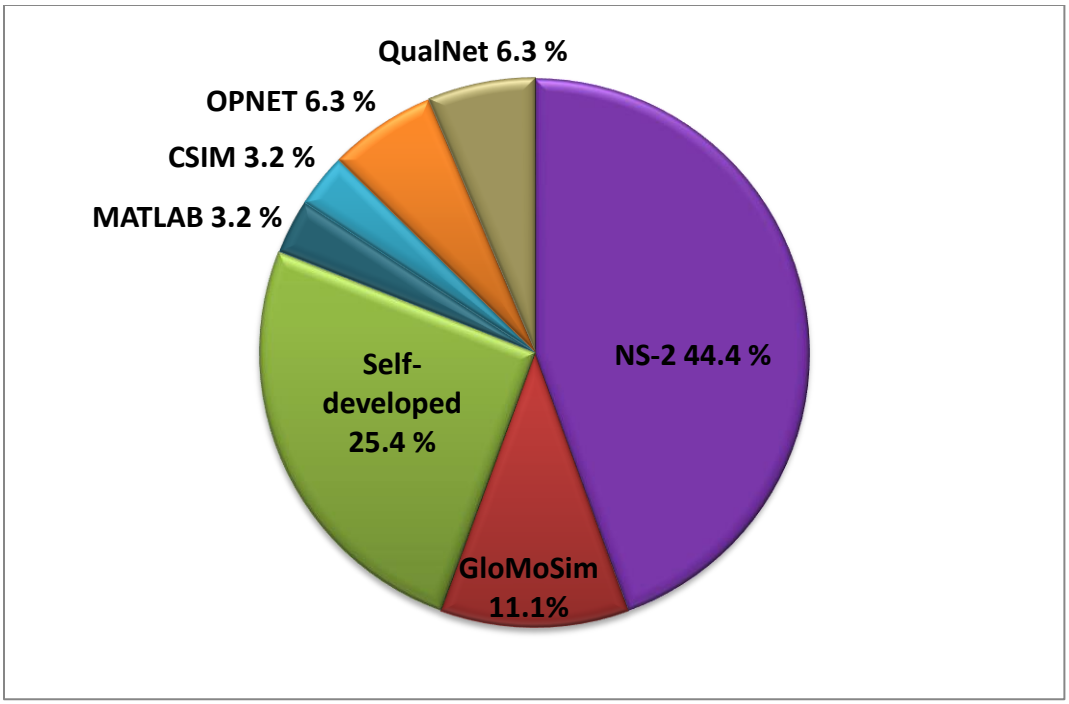

Figure 4-1: Simulator usage survey of simulation-based papers [38].

4.1.2. Simulation Methodology

In order to evaluate and compare the performance of the *A3ACKs* technique under different types of attacks, we test the *A3ACKS* under two types of networks: low speed and high speed networks. The low speed network represents the pedestrian where the specified speed of mobile nodes inside network is 1 meter per second. However, the high speed network represents the car motion where the specified speed of mobile nodes inside network is 20 meter per second. Lastly, we implemented two scenarios settings in each network (low speed network and high speed network) to simulate different types of misbehaving nodes in our simulation environment.

- ***First Scenario***: In this scenario, we simulate a basic packet dropping attacks, where misbehaving nodes drop all data packets they receive. The goal of this scenario is to show the principle actions of *A3ACKs* technique. This scenario also tests the performance of our *A3ACKs* IDS technique against receiver collision and limited transmission power weaknesses of Watchdog IDS, without the presence of collaborative attacks.
- ***Second Scenario****:* In this scenario, we simulate smart collaborative packet dropping attacks, where misbehaving nodes cooperate to drop data packets they receive. And also send back acknowledgement (Tack packet) to sender that is two hops away from them in opposite direction to route path, whenever it is possible. The purpose of this scenario is to test the performance of the *A3ACKs* IDS technique against the three weaknesses of watchdog IDS including receiver collision, limited transmission power and collaborative attacks within the presence of two consecutive misbehaving nodes in a route path.

4.1.3. Simulation Configuration

The simulation environment is created using Network Simulator (NS2), version 2.34 on Ubuntu 10.10 operating system. This system run on laptop with Core 2Duo CPU and 4GB-RAM. We adopted the default scenario setting in NS 2.34 to compare our simulation results with other existing research works. We configured our NS2 2.34 simulation environment to contain 50 nodes scattered on a flat area with size of 900 x 900 m. Physical layer and 802.11 MAC layer are also included in the wireless extension of NS2. The mobility mode is Random Waypoint with pause time equal zero. There are two

Moving speeds: one for low speed network and another for high speed network. In low speed network, the moving speed of mobile node is 1 m/s, but in high speed network the moving speed is 20m/s. User Datagram Protocol (UDP) traffic with Constant Bit Rate (CBR) of 4 packets per second is used with a packet size equals to 512 Byte. In each technique and for every network scenario, we run the NS simulation ten times with fixed simulation time equals to 900s with different seed numbers from 1 to 10. Then, we calculated the average value. The misbehaving nodes generated and scattered randomly from 0% to 40% with 10% scale increments. Details about simulation's parameters are shown in Table 4-1.

Parameter	**Value**
Number of nodes	50 nodes
Simulation area	900 meter X 900 meter
Simulation time	900 second
Mobility model	Random waypoint with pause time 0
Maximum speed (mobility speed)	1m/s for low speed network and 20m/s for high speed network
Traffic type	CBR (Constant Bit Rate)
Packet size	512 bytes
Packet rate	4 packets per second

Maximum connections	10
Propagation model	Two-ray ground model
Antenna model	Omni-directional
Transmission range	250 meter
MAC protocol	802.11 CSMA/CA
Link Bandwidth	2 Mbps
Routing protocol	Dynamic Source Routing (DSR)

Table 4-1: Details of Simulation Parameters.

4.2. Performance Metrics

In order to evaluate and compare simulation performance of the *A3ACKs* IDS, we use the two metrics [12, 16]:

- ***Packet Delivery Ratio* (*PDR*)**: It defines the ratio of the number of received packets at destination node to the number of sent packets by the source node as shown in equation 4-1.

$$\boldsymbol{Packet\ Delivery\ Ratio(PDR)} = \frac{\sum \textbf{Received packets at destinations}}{\sum \textbf{Sent packets by sources}} \ldots\ldots 4\text{-}1)$$

- ***Routing Overhead* (*RO*):** It defines the ratio of routing related packets [Route Request (RREQ), Route Reply (RREP), Route Error (RERR), Aack, Tack, Thack,

alarm and switch] in bytes to the total routing and data transmissions in bytes as shown in equation 4-2.

$$\boldsymbol{Routing\ Overhead(RoH)} = \frac{\sum \boldsymbol{Routing\ Messages}}{\sum \boldsymbol{Data\ \ transmissions} + \sum \boldsymbol{Routing\ transmissions}} \quad \ldots (4\text{-}2)$$

That means, network routing overhead includes: Route Request (RREQ) packet which is a broadcast packet sent by a source node to all the neighbors within its communication range. Route Reply (RREP) packet which is an unicast packet sent by the target destination node to the source node that sent the RREQ packet when the destination node receives the RREQ packet. Route Error (RERR), which is a packet sent to the source node that sent the RREQ packet when a failed node is detected due to broken link in DSR routing protocol. Aack packet which is a packet sent by destination node to the source node in End to End mode of *A3ACK* and *AACK* schemes. Tack packet which is a packet sent by a third node that is two hops away from the source node in every three consecutive nodes in *A3ACK* and AACK schemes. Thack packet which is a packet sent by a fourth node that is three hops away from the source node in every four consecutive nodes in *A3ACK* scheme. Alarm packet which is a packet generated by DSR protocol generally indicates detection of misbehaving node in a route path. Finally, switch packet which is a packet sent by destination node to a source node telling him to switch to Aack mode in A3ACKs scheme.

4.3. Simulation Results and Discussion

To evaluate the results of the new *A3ACKS* IDS technique and provide the readers with more clarifications on our simulation's results as well as to show the effect of

collaborative attacks on MANETs' performance, we compare the performance of the *A3ACKs* scheme against the AACK existing IDS technique for both low speed and high speed networks. Lastly, we end this section with comparison between the results of low and high speed networks to see the effect of mobility changing on our new IDS technique comparing with other existing IDSs, i.e. AACK.

4.3.1. Low Speed Network Simulation Results

The low speed network represents the pedestrian where the specified speed of mobile node is 1 meter per second. The simulation results of low speed network for both scenarios, as explained in our methodology, are presented in Table 4-2 where MN refers to misbehaving nodes.

Low Mobility- Scenario 1 (Single attack) : Packet Delivery Ratio (PDR)					
	0%	10%	20%	30%	40%
AACK without collaborative attacks	0.9942614	0.8829214	0.8317173	0.735389	0.696997
A3ACKs without collaborative attacks	0.9942614	0.8773666	0.8348631	0.7529527	0.7019225
Low Mobility- Scenario 1 (Single attack) : Routing Overhead (RoH)					
	0%	10%	20%	30%	40%
AACK without collaborative attacks	0.11158755	0.13990378	0.14474138	0.17392723	0.19624141
A3ACKs without collaborative attacks	0.115063848	0.14233643	0.14862111	0.16760948	0.20164842
Low Mobility - Scenario 2 (Collaborative attacks) : Packet Delivery Ratio (PDR)					
	0%	10%	20%	30%	40%
AACK with collaborative attacks	**0.9942614**	**0.9296658**	**0.9006466**	**0.8287053**	**0.8151953**
A3ACKs with collaborative attacks	**0.9942614**	**0.9696658**	**0.9406466**	**0.9287053**	**0.9351953**
Low Mobility - Scenario 2 (Collaborative attacks): Routing Overhead (RoH)					
	0%	10%	20%	30%	40%
AACK with collaborative attacks	**0.14797643**	**0.15769441**	**0.16341925**	**0.18487654**	**0.18003621**
A3ACKs with collaborative attacks	**0.14508353**	**0.17418731**	**0.17050975**	**0.18574344**	**0.20303621**

Table 4-2: Details of Low Speed Network Simulation's results

***Low Speed Network Scenario 1*: Simulation Results**

In this scenario, as discussed, misbehaving nodes drop all data packets they received. The goal of this scenario is to prove the principle of how the new A3ACKs IDS technique works against the receiver collision and limited transmission power problems and compare the results with existing AACK technique. Figure 4-2 shows the results of network performance of packets delivery ratio (PDR) vs. misbehaving nodes (MN) ratio.

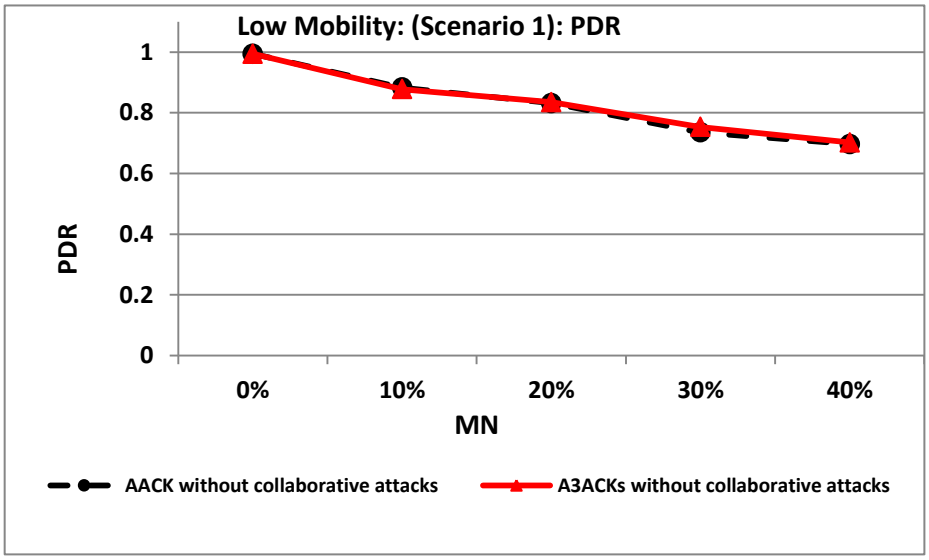

Figure 4-2: Comparison PDR vs. MN ratio in Low Speed Networks for scenario 1

We observe that packets delivery ratio of AACK and A3ACKs schemes almost the same. It decreases as the ratio of misbehaving nodes increases; because both of AACK and A3ACKs use the same mechanism to deal with no collaborative attacks (single attack). As a result, we conclude that both of the AACK and A3ACKs schemes are able to detect misbehaving nodes against the receiver collision and limited transmission.

The results of network routing overhead (RoH) vs. misbehavior nodes ratio in scenario 1 are shown in Figure 4-3. In general, we observe that the routing overhead ratio of AACK

and A3ACKs schemes almost close together and it increases with the increase of the ratio of misbehaving nodes. This is again because both of the techniques use the same mechanism to deal with a single misbehaving node in a route path.

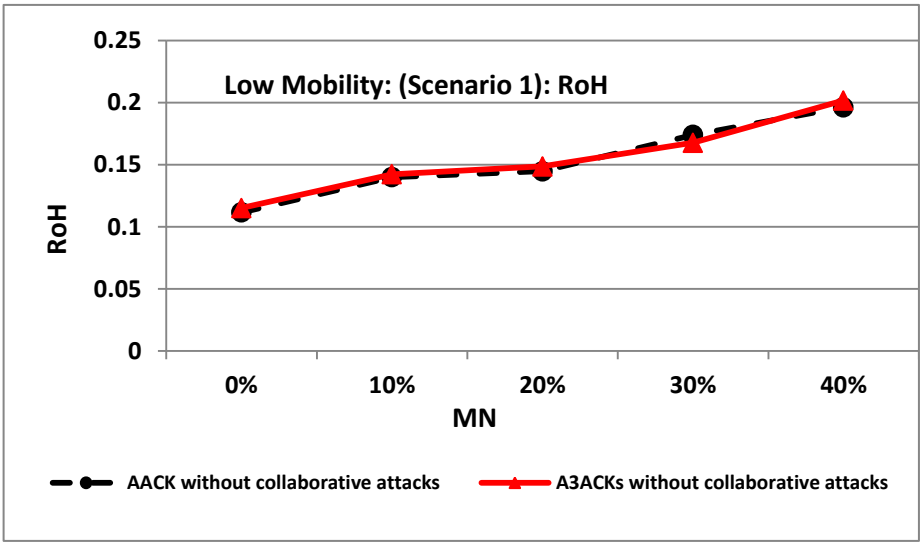

Figure 4-3: Comparison RoH vs. MN ratio in Low Speed Networks for scenario 1

***Low Speed Network Scenario 2*: Simulation Results**

In this scenario, as discussed, smart collaborative misbehaving nodes cooperate with each other to drop data packets they receive and send back acknowledgement (Tack) packet to the senders that are two hops away from them, in an opposite path direction, whenever it is possible. The purpose of this scenario is to test the performance of the A3ACKs IDS technique against the receiver collision, limited transmission power as well as the collaborative attacks, within the presence of two consecutive misbehaving nodes in a path. And then, compare the achieved results with an existing AACK technique. Figure 4-4 shows the results of network performance of packets delivery ratio (PDR) vs. misbehaving nodes ratio for scenario 2.

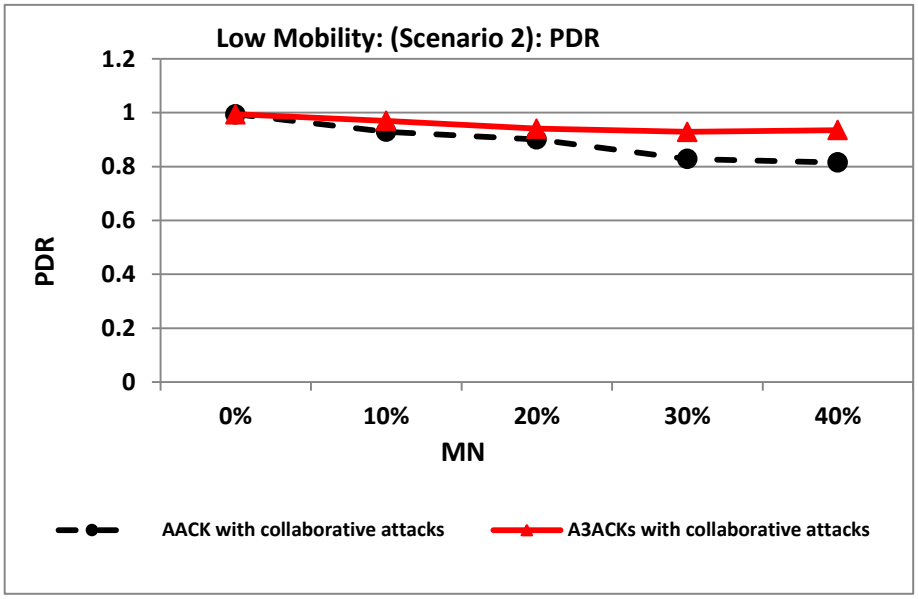

Figure 4-4: Comparison PDR vs. MN ratio in Low Speed Networks for scenario 2

We observe that the packets delivery ratio of the A3ACKs scheme slightly outperforms the AACK scheme when the percentage of the misbehaving nodes is small (i.e., 10% and 20%). Whereas, the packets delivery ratio of the A3ACKs scheme is better than the AACK scheme by approximately 11% and 12% especially when the percentage of the misbehaving nodes are 30% and 40% respectively. As a result, we conclude that only A3ACKs scheme is able to detect misbehaving nodes against receiver collision, limited transmission and collaborative attacks within the presence of two consecutive misbehaving nodes in a route path, unlike AACK scheme.

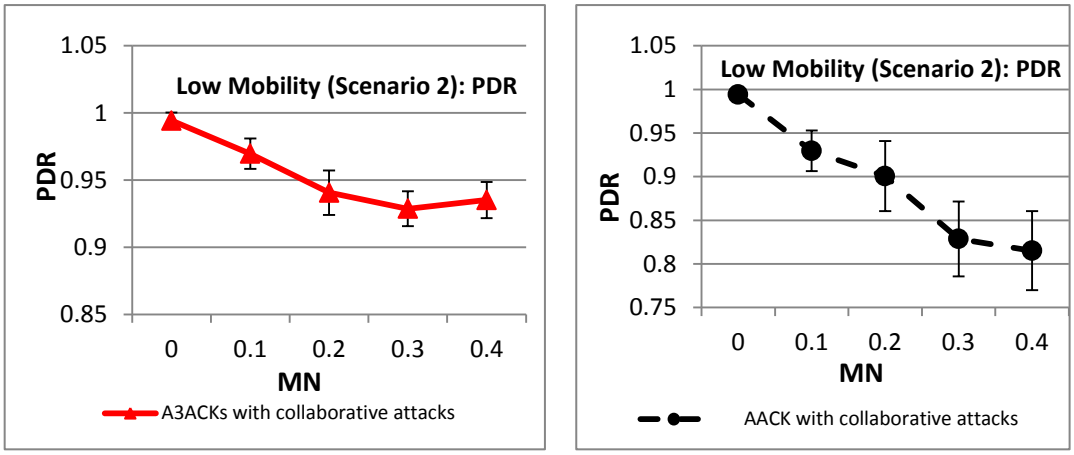

Figure 4-5: Confidence Interval for PDR vs. M N ratio in Low Speed Networks for scenario 2

Figure 4-5 compares the confidence interval of the A3ACKs and the AACK schemes for PDR with 95% confidence. It clear from the figure that the values of confidence interval are more accurate when the ratio of MNs decreases. Because of packets dropping decreases when MNs ratio decreases.

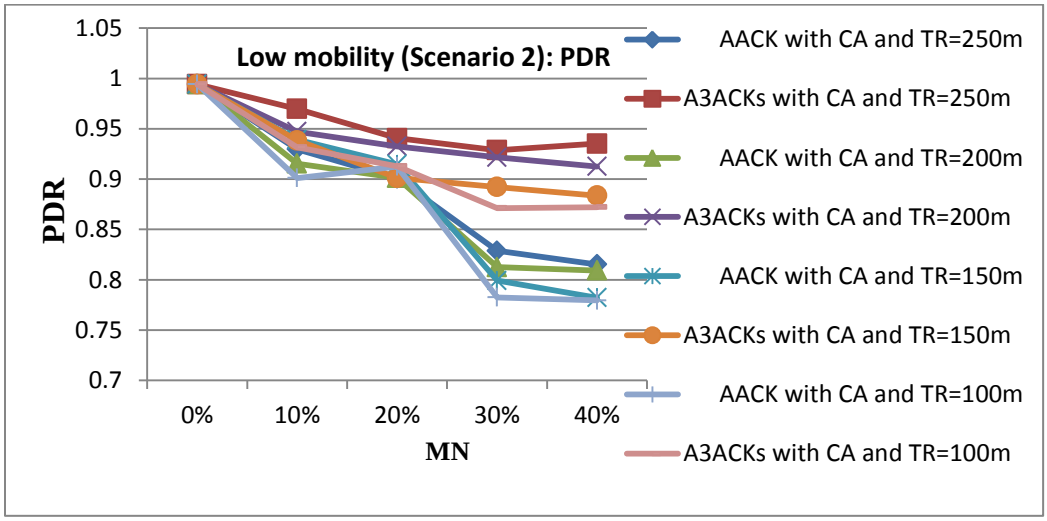

Figure 4-6: PDR vs. MN ratio in Low Speed Networks for Scenario 2 with Different Transmission Range

Figure 4-6 shows that the PDR of the A3ACKs and AACK schemes increases when the value of transmission range increases. It could be as result of greater transmission range leads to greater transmission distances can be achieved. As a result, more packets will be delivered because mobile nodes can communicate within large transmission range.

The results of network routing overhead (RoH) vs. misbehavior ratio in scenario 2 are shown in Figure 4-7. In general, the routing overhead of the AACK and A3ACK schemes are increased by increasing the percentage of misbehaving nodes. However, we observe that the routing overhead ratio of the A3ACKs scheme is higher than the AACK scheme, especially when the percentage of the misbehaving nodes is at 40%. We generalize that as result of introduction of the Thack mode in A3ACKs technique. That means, the A3ACKs scheme switches to Thack mode to detect collaborative misbehaving nodes in a route path and this leads to increase its overhead more than AACK scheme.

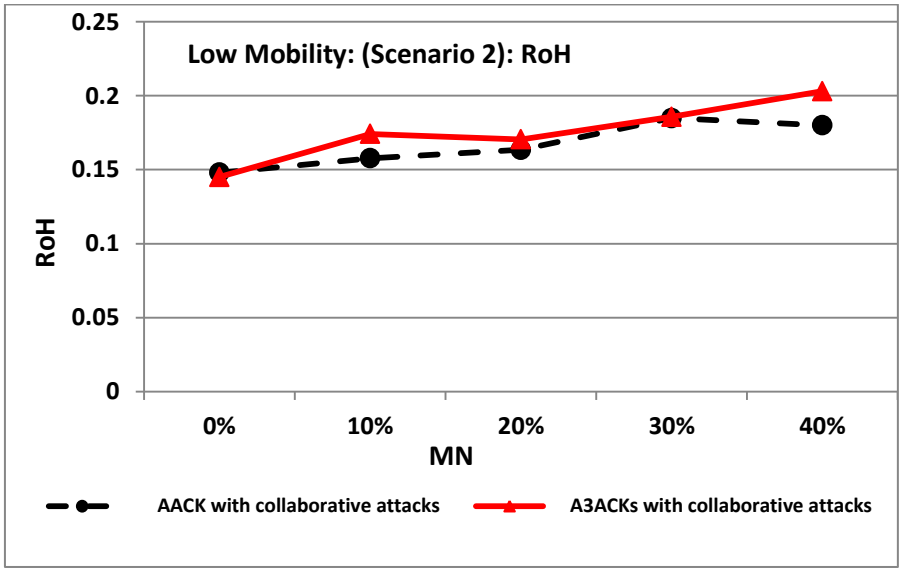

Figure 4-7: Comparison RoH vs. MN ratio in Low Speed Networks for scenario 2

Figure 4-8 compares the confidence interval of the A3ACKs and the AACK schemes for routing overhead with 95% confidence. We observe that the values of confidence interval are more accurate when the ratio of MNs decreases. Because there is more RoH produced when MNs ratio increases.

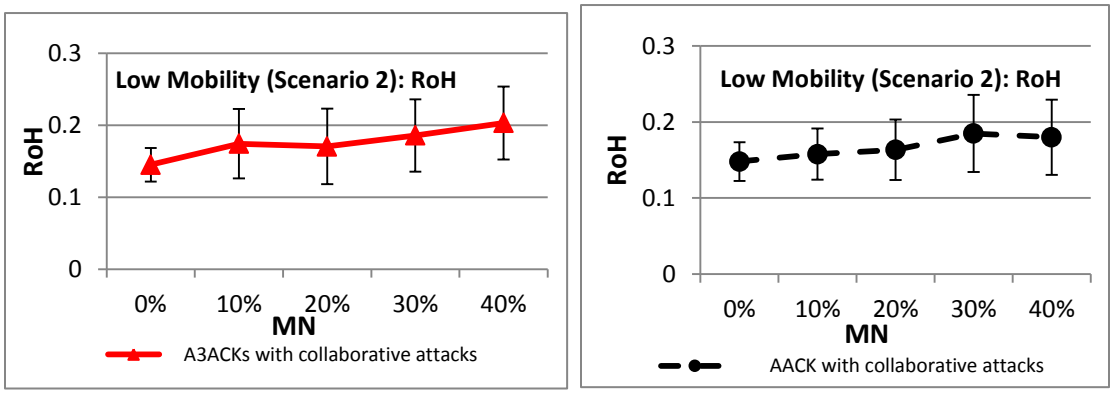

Figure 4-8: Confidence Interval for RoH vs. MN ratio in Low Speed Networks for scenario 2

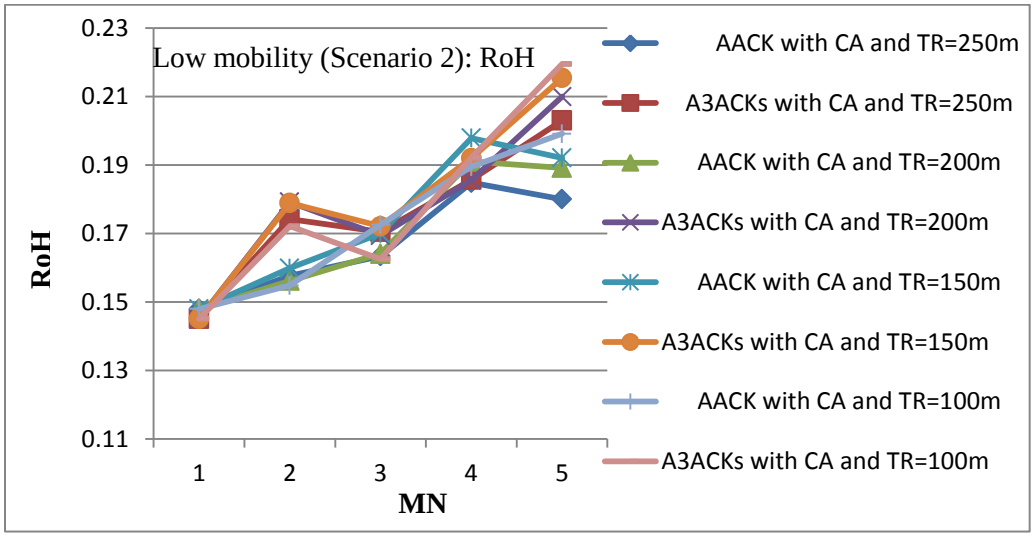

Figure 4-9: RoH vs. MN ratio in Low Speed Networks for Scenario 2 with Different Transmission Range

Figure 4-9 shows that the RoH of the A3ACKs and the AACK schemes increases when the value of transmission range decreases. It could be as result of less transmission range leads to less transmission distances can be achieved. As a result, more packets dropped and more routing overhead produced.

4.3.2. High Speed Network Simulation Results

The high speed network represents car motion where the specified speed is 20 meter per second. The simulation results of high speed network for both scenarios, as explained in our methodology, are presented in Table 4-3 where MN refers to misbehaving nodes.

High Mobility - Scenario 1 (Single attack) : Packet Delivery Ratio (PDR)					
	0%	10%	20%	30%	40%
AACK without collaborative attacks	0.9843134	0.7088881	0.5434132	0.4244745	0.3852435
A3ACKs without collaborative attacks	0.9843134	0.7006484	0.5368222	0.421733	0.3847024
High Mobility - Scenario 1 (Single attack) : Routing Overhead (RoH)					
	0%	10%	20%	30%	40%
AACK without collaborative attacks	0.1293531	0.134682	0.1807414	0.2641265	0.4703682
A3ACKs without collaborative attacks	0.1293531	0.12564157	0.17836331	0.2526122	0.4966829
High Mobility - Scenario 2 (Collaborative attacks) : Packet Delivery Ratio (PDR)					
	0%	10%	20%	30%	40%
AACK with collaborative attacks	0.9843134	0.8285976	0.7063138	0.5947121	0.524068
A3ACKs with collaborative attacks	0.9843134	0.8821178	0.7918064	0.6941413	0.6801401
High Mobility - Scenario 2 (Collaborative attacks): Routing Overhead (RoH)					
	0%	10%	20%	30%	40%
AACK with collaborative attacks	0.1293531	0.1356249	0.1398516	0.1750516	0.2076547
A3ACKs with collaborative attacks	0.1293531	0.1556538	0.146925	0.18918203	0.2550042

Table 4-3: Details of High Speed Network Simulation's Results

High Speed Network Scenario 1: Simulation Results

In this scenario, misbehaving nodes drop all data packets they received. The goal of this scenario is to show the principle of how the new A3ACKs IDS technique works against

the receiver collision and limited transmission power problems and compare the results with the existing AACK technique. Figure 4-9 shows the results of network performance of packets delivery ratio (PDR) vs. misbehaving ratio.

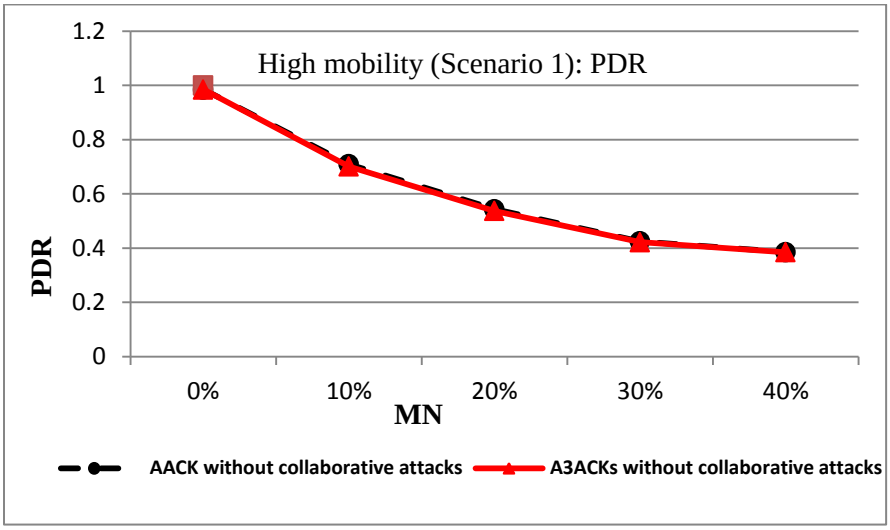

Figure 4-10: Comparison PDR vs. MN ratio in High Speed Networks for scenario 1

We observe that packets delivery ratio of AACK and A3ACKs schemes almost the same. It decreases as the ratio of misbehaving nodes increases; because both of AACK and A3ACKs use the same mechanism to deal with no collaborative attacks (single attack). As a result, we conclude that both of the AACK and A3ACKs schemes are able to detect misbehaving nodes against the receiver collision and limited transmission.

The results of network routing overhead (RoH) vs. misbehavior ratio in scenario 1 are shown in Figure 4-11. In general, we observe that the routing overhead ratio of AACK and A3ACKs schemes almost close together and it increases with the increase of the ratio of misbehaving nodes. This is again because both of the techniques use the same mechanism to deal with a single misbehaving node in a route path. However, the

A3ACKs scheme has more overhead than AACK scheme when the percentage of misbehaving nodes is at 40%. This could be explained as a result of switching overhead in A3ACK given a broken link error.

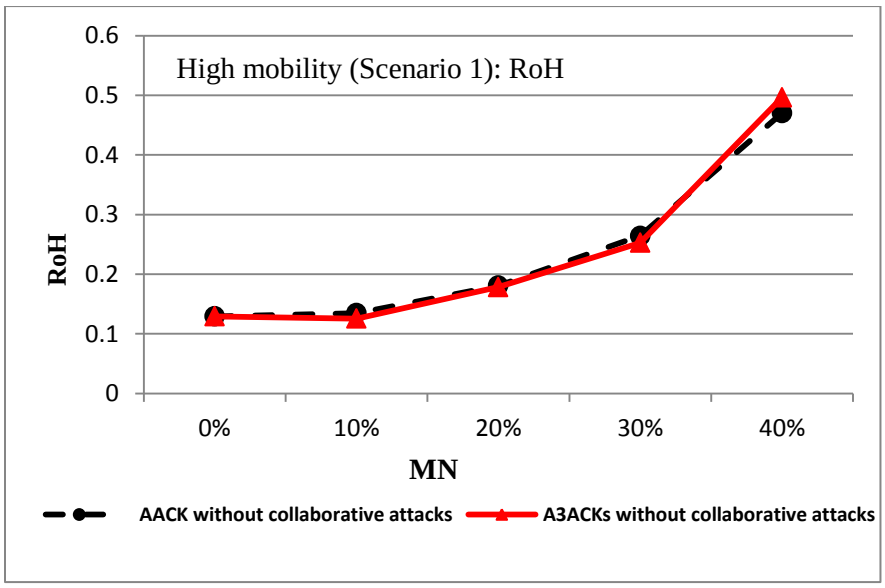

Figure 4-11: Comparison RoH vs. MN ratio in High Speed Networks for scenario 1

High Speed Network Scenario 2*: *Simulation Results

In this scenario, smart collaborative misbehaving nodes cooperate with each other to drop data packets they receive and send back acknowledgement (Tack) packet to the senders that are two hops away from them, in an opposite path direction, whenever it is possible. The purpose of this scenario is to test the performance of the A3ACKs IDS technique against the receiver collision, limited transmission power as well as the collaborative attacks, within the presence of two consecutive misbehaving nodes in a path. And then, compare the achieved results with an existing AACK technique. Figure

4-12 shows the results of network performance of packets delivery ratio (PDR) vs. misbehaving ratio for scenario 2.

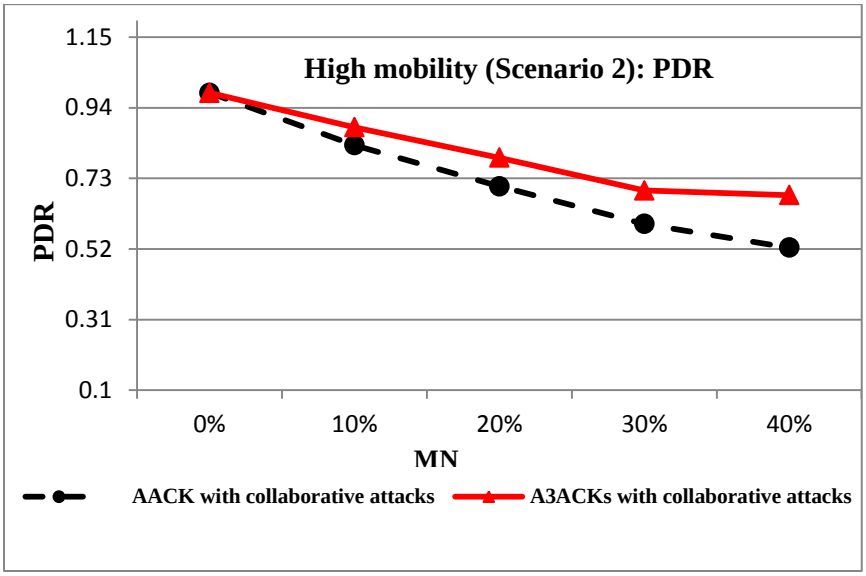

Figure 4-12: Comparison PDR vs. MN ratio in High Speed Networks for scenario 2

We observe that the packets delivery ratio of the A3ACKs scheme slightly outperforms the AACK scheme when the percentage of the misbehaving nodes is small (i.e., 10% and 20%). Whereas, the packets delivery ratio of the A3ACKs scheme is better than the AACK scheme by approximately 10% and 16% especially when the percentage of the misbehaving nodes are 30% and 40% respectively. As a result, we conclude that the A3ACKs is able to detect misbehaving nodes against receiver collision, limited transmission and collaborative attacks within the presence of two consecutive misbehaving nodes in a route path, unlike AACK scheme.

Figure 4-13 shows the confidence interval of the A3ACKs and AACK schemes for PDR with 95% confidence. It clear from the figure that the values of confidence interval are

more accurate when the ratio of MNs ratio decreases. Because of packets dropping decreases when MNs ratio decreases.

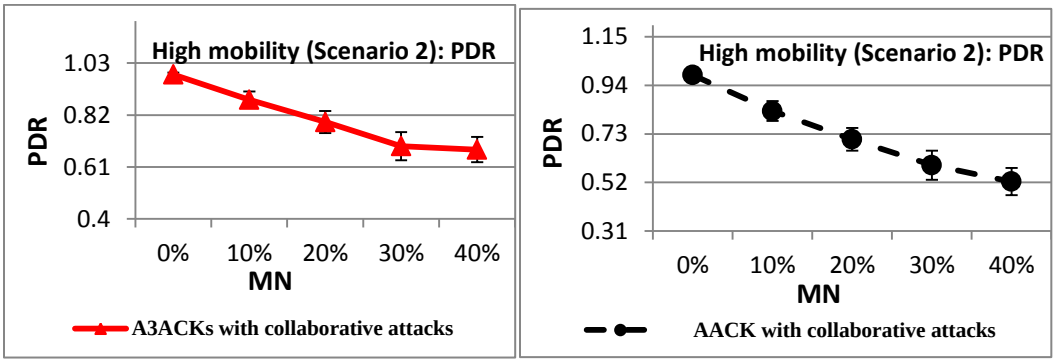

Figure 4-13 : Confidence Interval for PDR vs. MN ratio in High Speed Networks for scenario 2

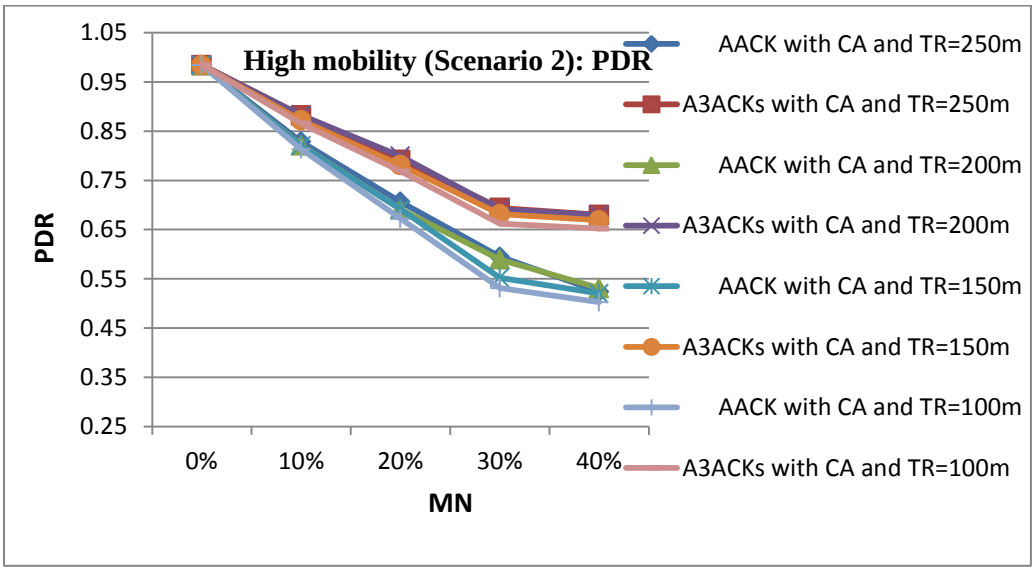

Figure 4-14: PDR vs. MN ratio in Low Speed Networks for Scenario 2 with Different Transmission Range

Figure 4-14 shows that the PDR of both A3ACKs and AACK techniques increases when the value of transmission range increase. It could be as result of greater transmission range leads to greater transmission distances can be achieved. As a result, more packets

will be delivered because mobile nodes can communicate within large transmission range.

The results of network routing overhead (RoH) vs. misbehavior ratio in scenario 2 are shown in Figure 4-15.

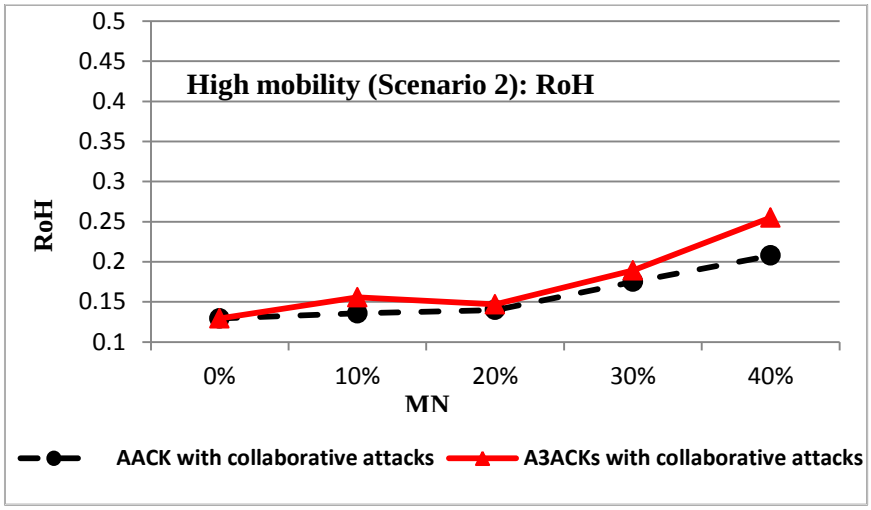

Figure 4-15: Comparison RoH vs. MN ratio in High Speed Networks for scenario 2

In general, the routing overhead of the AACK and A3ACK schemes are increased by increasing the percentage of misbehaving nodes. However, we observe that the routing overhead ratio of the A3ACKs scheme is higher than the AACK scheme, especially when the percentage of the misbehaving nodes is at 40%. We generalize that as result of introduction of the Thack mode in A3ACKs technique. That means, the A3ACKs scheme switches to Thack mode to detect collaborative misbehaving nodes in a route path and this leads to increase its overhead more than AACK scheme.

Figure 4-16 shows the confidence interval of the A3ACKs and the AACK schemes for routing overhead with 95% confidence. We observe that the values of confidence interval

are more accurate when the ratio of MNs decreases. Because there is more RoH produced when MNs ratio increases.

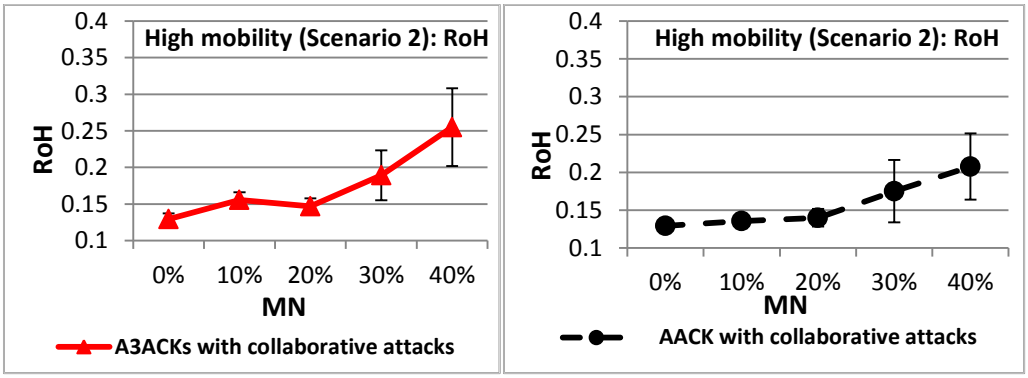

Figure 4-16: Confidence Interval for RoH vs. MN ratio in High Speed Networks for scenario 2

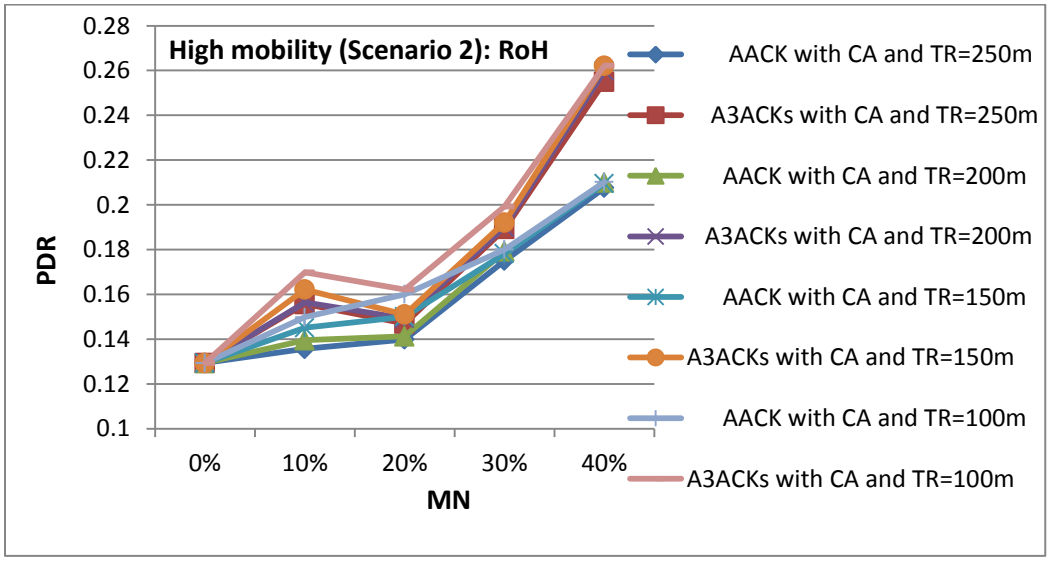

Figure 4-17: RoH vs. MN ratio in Low Speed Networks for Scenario 2 with Different Transmission Range

Figure 4-17 shows that the RoH of both A3ACKs and AACK schemes increases when the value of transmission range decreases. It could be as result of less transmission range leads to less transmission distances can be achieved. As a result, more packets dropped and more routing overhead produced.

4.3.3. Discussion

In this section, we compare the results of low speed and high speed networks to see the effect of mobility on our new *A3ACK* IDS technique comparing with the existing IDSs, i.e. AACK.

In general, both of A3ACK and AACK techniques are acknowledgement based schemes and the results of them in both scenarios are better in case of low speed network than that in case of high speed networks; due to stability of mobile nodes in low speed network than that in high speed network. As a result, low packets dropped and low overhead produced in low speed networks than that in high speed networks. Moreover, the PDR for both scenarios in both low speed network and high speed network is increased when MN ratio increases. However, the RoH for both scenarios in both low speed network and high speed network is inversely proportional to MN ratio, where the RoH is increased when MN ratio decreases.

Figure 4-18 compares the results of packets delivery ratio (PDR) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 1. It is clear that the PDR of AACK and A3ACKs schemes almost the same in scenario 1 for low speed network and as well as for high speed network because both of them use the same mechanism to deal with single attack problem as discussed.

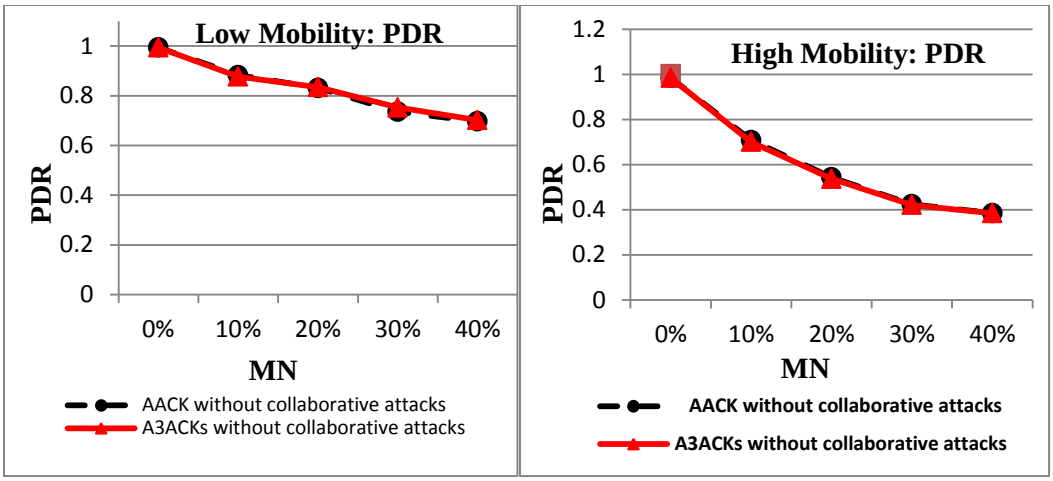

Figure 4-18: Comparison PDR vs. MN in low and high speed networks for scenario 1

Figure 4-19 compares the results of Routing overhead (RoH) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes also for scenario 1. Again it is clear that the RoH of AACK and A3ACKs schemes almost the same in scenario 1 for low speed network and for high speed network for the same reason as mentioned above.

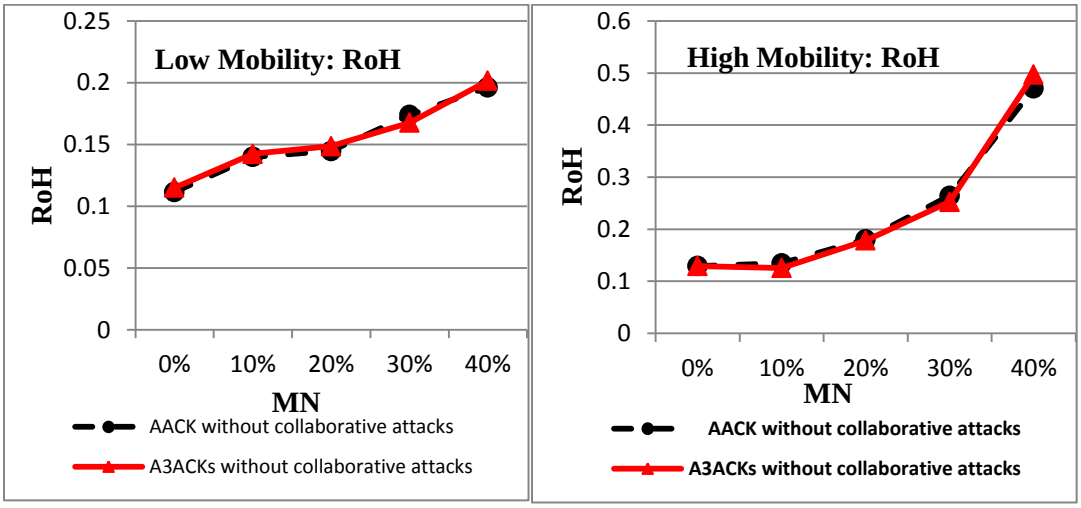

Figure 4-19: Comparison RoH vs. MN in low and high speed networks for scenario 1

Figure 4-20 compares the results of packets delivery ratio (PDR) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 2. For high speed network, A3ACKs slightly tops AACK scheme when MN ratio is between 10% and 20%. Whereas, the PDR of A3ACKs scheme outperforms AACK scheme by approximately 11% to 16% when MN between 30% and 40% respectively. Also, for low speed network, A3ACKs is slightly better than AACK scheme when MN ratio is between 10% and 20%. However, A3ACKs surpasses AACK by about 11% and 13% when MN ratio is between 30% and 40% respectively. The reason behind PDR for both A3ACKs and AACK schemes in low speed network is higher than that in high speed network is that due to the stability of mobile nodes in low speed network.

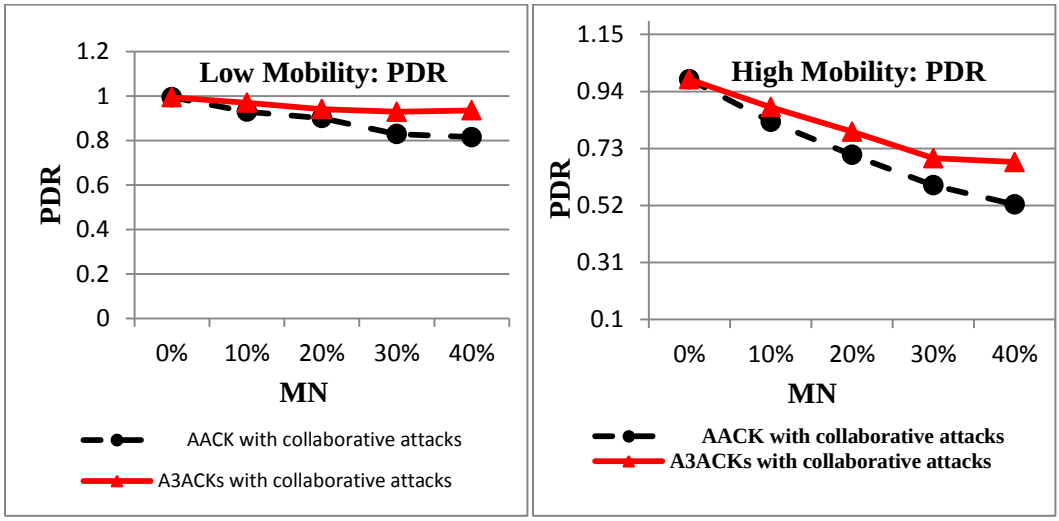

Figure 4-20: Comparison PDR vs. MN in low and high speed networks for scenario 2

Figure 4-21 compares the results of Routing Overhead (RoH) vs. misbehaving nodes ratio (MN) of A3ACKs and AACK schemes for scenario 2. In general, RoH for both AACK and A3ACKs schemes are increased if the MN ratio increases in both high speed network and low speed network. In case of high speed network, it is clear that the RoH of

A3ACKs scheme is higher than AACK scheme especially at 40% MN. This could be as a result of using the Thack model, as previously discussed, in A3ACKs technique to detect collaborative MN in a path when Tack model fails to detect them. As a result, this leads to increase RoH of A3ACKs scheme compared with AACK scheme. However, in case of both low and high speed networks, AACK scheme is slightly better than A3ACKs scheme at 40%.

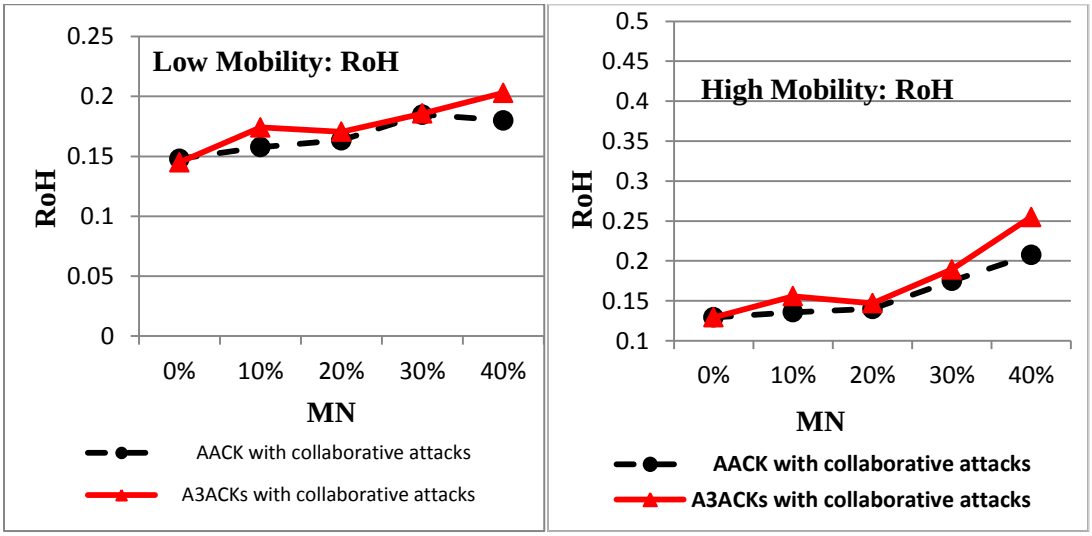

Figure 4-21: Comparison RoH vs. MN in low and high speed networks for scenario 2

4.4. Conclusion and Future Work

Packet dropping attacks could be done by selfish or malicious nodes and it represents major security threats in Mobile Ad hoc Networks (MANETs). This research is devoted to detect and mitigate selfish and malicious nodes by avoiding them in later route transmissions. In this research, we continue improvement of the existing IDSs over MANETs by proposing a novel Adaptive Three Acknowledgements Intrusion Detection System (A3ACKs) scheme. It is designed especially for MANETs and it solves three

significant problems of the Watchdog technique including receiver collision, limited transmission power and collaborative attacks with or without the presence of collaborative misbehaving nodes in a route path. We tested it under both low speed and high speed networks using Dynamic Source Routing (DSR) protocol. We compared the results against the existing AACK IDS scheme under two scenarios using NS2 simulator. While the performance of A3ACKs is comparable with AACK in the case of one misbehaving node, A3ACKs outperforms AACK in the case of collaborative attack. Moreover, the performance of both protocols is better under low speed network than that of high speed network. Although the new A3ACKs IDS has slightly high routing overhead, the network security is more robust and the packets delivery ratio is improved. To the best of our knowledge, this tradeoff is worthwhile when network security has the top priority in MANETs. In conclusion, the results achieved using A3ACKs IDS showed a promising performance especially with the presence of collaborative attacks.

For the future work, we recommend testing A3ACKs under other types of routing protocols in MANETs including reactive, proactive and hybrid protocols. In addition, we would like to improve A3ACKs scheme to solve other weaknesses of the Watchdog IDS, such as misbehaving report and partial drop attacks. Finally, we suggest testing A3ACKs scheme in real networks instead of simulation and comparing the results.

References

[1] Jayakumar, G and Gopinath, G. 2007. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. *In Journal of Computer Science* 3(8): 574-582.

[2] C. E. Perkins, Ad-hoc Networking. Addison Wesley Professional, December 2000.

[3] M. Ilyas, ed., The Handbook of Ad-hoc Wireless Networks. CRC Press, December 2002.

[4] R. Hekmat, Ad-hoc Networks: Fundamental Properties and Network Topologies. Netherlands: Springer , 2006. pp.154. eBook.

[5] M. Barbeau, E. Kranakis, Principles of Ad-hoc Networking. Wiley, 2007.

[6] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," Wireless/Mobile Network Security, 159-180 (2008).

[7] Nandy, Rusha, and Roy Debdutta Barman. "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme." Int. J. Advanced Networking and Applications. 03.01 (May 2011): 1035-1043.

[8] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24-28, 2007, pp. 1154-1159.

[9] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, pp. 393-422, March 2002.

[10] Y. Li, J. Wei. "Guidelines on Selecting Intrusion Detection Methods in MANET", Proceedings of Information Systems Educators (ISECON) 2004, v 21 (Newport): §3233. ISSN: 1542--7382.

[11] Bo Sun, INTRUSION DETECTION IN MOBILE AD-HOC NETWORKS, A Doctor of Philosophy Dissertation, Texas A&M University, May 2004

[12] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM Computer Communication Review, vol. 24, London, UK, pp. 234-244, Oct., 1994.

[13] Royer, E.M.; Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks," Personal Communications, IEEE , vol.6, no.2, pp.46-55, Apr 1999.

[14] C. E. Perkins, and E. M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), New Orleans, LA, pp. 90-100, Feb. 1999.

[15] Park, V.D.; Corson, M.S., "A highly adaptive distributed routing algorithm for mobile wireless networks," INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE , vol.3, no., pp.1405,1413 vol.3, 7-12 Apr 1997

[16] J. Broch, D. Johnson, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks," IETF Internet Draft, Feb. 2002, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt.

[17] Joa-Ng, M.; I-Tai Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," Selected Areas in Communications, IEEE Journal on , vol.17, no.8, pp.1415-1425, Aug 1999

[18] B. Wu, J. Chen, J. Wu and M. Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security, Xiao, Y., Shen, X. and Du, -Z, D. Net. 2006.

[19] Rajni Sharma, Alisha Saini, "A Study of Various Security Attacks and their Countermeasures in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 1 No. 1 December 2011", pp. 01-05.

[20] Monika, Darji, and Trivedi Bhushan. "Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques."International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868. vol. 1.No.3 (February 2012): pp. 38-43.

[21] Aishwarya, Sagar Anand , and Chawla2 Meenu. "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET." IJCSI International Journal of Computer Science Issues. Vol. 7.Issue 4, No 1 (July 2010): pp. 12-17.

[22] Hu Y., Perrig A., Johnson D. (2002) Ariadne: A secure on-demand routing protocol for ad-hoc networks. In Proceedings of the 8th annual international Conference on Mobile Computing and Networking, Sept 2002, pp. 12-23.

[23] Yinan Li; Zhihong Qian, "Mobile Agents-Based Intrusion Detection System for Mobile Ad Hoc Networks," Innovative Computing & Communication, 2010 Intl Conf on and Information Technology & Ocean Engineering, 2010 Asia-Pacific Conf on (CICC-ITOE) , vol., no., pp.145-148, 30-31 Jan. 2010.

[24] S. Axelsson, "Intrusion Detection Systems: A Taxonomy and Survey,"Tech. report no. 99-15, Dept. of Comp. Eng., Chalmers Univ. of Technology, Sweden,Mar. 20, 2003.

[25] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5,pp. 446-556, September 2003.

[26] L. Buttyan and J.P. Hubaux. Security and cooperation in wireless networks. Cambridge University Press, August, 2007.

[27] Tanapat Anusas-amornkul, "ON DETECTION MECHANISMS AND THEIR PERFORMANCE FOR PACKET DROPPING ATTACK IN AD HOC NETWORK," PHD dissertation, university of Pittsburgh, July 24, 2008.

[28] Balakrishnan, Venkatesan, and Vijay Varadharajan. "Packet drop attack: A serious threat to operational mobile ad hoc networks." Networks and Communication Systems. (2005): 18--25. Web. 20 Oct. 2013.

[29] Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634-640, 20-23April2010.

[30] Marti S, Giuli T J, Lai K, Baker M (2000) Mitigating routing misbehaviour in mobile ad hoc networks. In: Proceedings 6th Annu. Int. Conf. Mobile Comput, pp. 255–265.

[31] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.

[32] T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mohmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282. 2009.

[33] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes in MANETs,” in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[34] Parker, J.; Undercoffer, J.; Pinkston, J.; Joshi, A., "On intrusion detection and response for mobile ad-hoc networks," Performance, Computing, and Communications, 2004 IEEE International Conference on , vol., no., pp. 747-752, 2004.

[35] Nasser, N.; Chen, Y., "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks," Communications, 2007. ICC '07. IEEE International Conference on , vol., no., pp.1154-1159, 24-28 June 2007

[36] Nan Kang; Shakshuki, E.M.; Sheltami, T.R., "Detecting Forged Acknowledgements in MANETs," Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on , vol., no., pp.488,494, 22-25 March 2011.

[37] Shakshuki, E.M.; Nan Kang; Sheltami, T.R., "EAACK—A Secure Intrusion-Detection System for MANETs," Industrial Electronics, IEEE Transactions on , vol.60, no.3, pp.1089,1098, March 2013.

[38] S. Kurkowski, T. Camp, and M. Colagrosso. “MANET simulation studies: The current stated and new simulation tools,” Technical report, Department of Math. And Computer Science, Colorado School of Mines, MCS-05-02, February 2005.

[39] Ns documentations: http://www.isi.edu/nsnam/ns/ns-documentation.html

Vitae

Name : Abdulsalam Salem Basabaa.

Nationality : Yemeni.

Date of Birth :7/9/1982

Email : g201002320@kfupm.edu.sa or eng.basabaa@gmail.com

Address : Yemen/Hadhramout/Mukalla

Academic Background : Computer Science

Publications :

[1] Tarek Sheltami, Abdulsalam Basabaa and Elhadi Shakshuki, "A3ACKs: Adaptive Three ACKnowledgments Intrusion Detection System for MANTs," *submitted to Journal of Ambient Intelligence and Humanized Computing, spring, 2014.*

[2] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds," *accepted at the 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), June 2 - 5, 2014, Hasselt, Belgium.*