بسم الله الرحمن الرحيم

Sudan University of Science and Technology College of Graduate Studies

Detecting and Isolating of Misbehaving Nodes in MANETs

اكتشاف وعزل العقد سيئة السلوك في شبكات الجوال المخصصة

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Computer Science

By :

Omer Humed Osman Mohamed

Supervised by:

Dr. Faisal Mohamed Abdallah

April 2021

Dedications

This research is dedicated :

To the sake of Allah, my Creator and my Master my

great teacher and messenger Mohammed

(may Allah blessand grant him) who

taught us the purpose of life

To my great parents who never stop giving of

themselves in countless ways

To my beloved brothers and sisters

To all my family, the symbol of love and giving

To my dear friends who encourage and support me

To All the people in my life

To my Teachers at Sudan University of Science and

Technology .

Acknowledgement

In the Name of Allah, the Most Merciful, the Most Merciful and prayers and peace be upon Mohamed His servant and messenger. First and foremost, I must acknowledge my limitless thanks to Allah, the ever Magnificent. I owe a deep of gratitude to Sudan University of Science and Technology for giving me an opportunity to complete this research. I wish to acknowledge the great assistance and fruitful guidance offered by my supervisor Dr. Faisal Mohamed Abdullah ,who has been always generous during all phases of the research. I would like to take this opportunity to convey warm thanks to all my beloved friends ,who have been so supportive along the way of writing my thesis. I also would also like to express my wholehearted thanks to my family for their generous support they provided me throughout my entire life and particularly through the process of pursuing the master degree, and for their unconditional love and prayers.

.

Abstract

Mobile Ad-hoc Networks are wireless networks without infrastructure consisting of wireless mobile devices with self-configuration and self-organization. As a result of the lack of centralized management, these nodes cooperate with each other to send data packets. Most network protocols assume a cooperative environment between the nodes in the network. Moreover these types of networks are prone to many types of attacks because the nodes change their positions quickly and randomly. So there is a need for techniques to detect misbehaving nodes. This research presents a solution for identifying misbehavior using techniques to solve receiver collisions, limited transition power and collaborative misbehaving nodes using Ad hoc On-demand Distance Vector (AODV). The protocol has been implemented using network simulator NS2. Result show that the problem of collaborative misbehaving nodes has been solved taking into account the routing overhead and the misbehaving nodes were detected and isolated from the route.

المستخلص

شبكات الجوال المخصصة هي شبكات لاسلكية بدون بنية تحتية. تتكون من أجهزة الموبايل اللاسلكية وهي ذاتية التكوين وذاتية التنظيم . نتيجة لعدم وجود إدارة مركزية ، تتعاون هذه العقد مع بعضها البعض لإرسال حزمة البيانات. تفترض معظم بروتوكولات الشبكة هذه البيئة التعاونية بين العقد في الشبكة. علاوة على ذلك ، فإن هذا النوع من الشبكات عرضة لأنواع متعددة من الهجمات بسبب العقد التي تغير مواقعها بسرعة وبشكل عشوائي. لذلك هناك حاجة لتقنيات لاكتشاف العقد سيئة السلوك. يقدم هذا البحث حلاً لتوجيه السلوك الخاطئ باستخدام تقنيات لحل تصادم أجهزة الاستقبال وقوة الانتقال المحدودة والعقد التعاونية سيئة السلوك ، تم استخدام محاكي الشبكات NS2 لتتطبيق بروتوكول متجه المسافة المخصص حسب الطلب (AODV) اظهرت النتائج انه تم التغلب على مشكلة العقد التعاونية سيئة السلوك وتمت مراعاة الحمل الزائد على التوجيه وتم كشف العقد سيئة السلوك وعزلها عن المسار.

Table of Contents

Contents	Page No.

List of Figures

List of Tables

List of Abbreviation

Abbreviation	Meaning
MANET	Mobile Ad-hoc Networks
AODV	Ad hoc On-Demand Distance Vector
NS	Network Simulator
DOS	Denial Of Service
WPAN	Wireless Personal-Area Networks
WLAN	Wireless Local-Area Network
WMAN	Wireless Metropolitan-Area Networks
WWAN	Wireless Wide-Area Network
CPU	Central Processing Unit
IEEE	Institute of Electrical and Electronics Engineers
VANET	Vehicular Ad hoc Network
IMANET	Internet Based Mobile Ad hoc Networks
INVANET	Intelligent Vehicular Ad hoc Networks
FANET	Flying Ad hoc Network
DSDV	Destination Sequenced Distance Vector
CSGR	Cluster Switch Gateway Routing
OLSR	Optimized Link State Routing
STAR	Structured Transparent Accessible and Reproducible
WRP	*Wireless Routing Protoco*l
FSR	Fisheye State Routing
GSR	Global State Routing

DSR	Dynamic Source Routing
TORA	Temporally Ordered Routing Algorithm

Abbreviation	**Meaning**
ABR	Auditory Brainstem Response
LMR	Land Mobile Radio
ZRP	*Zone Routing Protocol*
ZHLS	Zone-based Hierarchical Link State
SHRP	Strategic Highway Research Program
WARP	Wireless Augmented Reality Prototype
RERR	Route Error
RREQ	Route Request
RREP	Route Reply
TCL	Tool Command Language
I-2ACK	Improve Tow Acknowledge
AACK	Adaptive Acknowledge
E-TWOACK	Enhanced Two Acknowledge
AMD	Audit-Based Misbehavior Detection
EAACK	Enhanced Adaptive Acknowledge
MRA	Misbehavior Report Authentication
A 3ACK	Adaptive Three Acknowledge
IA-ACK	Improve Adaptive Acknowledge
CBR	Constant Bit Rate
RTS	Request To Send
CTS	Clear To Send

CHAPTER ONE

INTRODUCTION

CHAPTER ONE

INTRODUCTION

1.1 Background

The world has embarked on the study and development of wireless networks for their convenience and coverage. There is also a widespread and acceptance of wireless networks that are autonomous and self-configured. The most popular are mobile ad-hoc networks 'MANETs', which are dynamic wireless networks that operate without infrastructure and are fully cooperative in routing and sharing resources. It is known that the ad hoc network does not contain static routers which means that all nodes are able to move dynamically and are connected in a random manner. These nodes can operate as a final system and a router at the same time. The transmission capacity of the nodes and the location of the network are important factors on which the assigned network topology depends and may change over time. Since mobile ad hoc networks change their topology frequently, routing in these networks is a challenging task. Due to the lack of a fixed infrastructure in the nature of mobile wireless networks, there is a need for routing protocols that direct the packet to its correct path.

1.2 Problem Statement

Malicious nodes trigger Denial Of Service (DOS) attacks. They prevent cooperation with the rest of the nodes in sharing resources. This is called directive misbehavior.

1.3 Proposed Solution

This research is focused on detecting and mitigating the influence of misbehaving nodes in mobile ad-hoc networks. This is achieved by locating and isolating misbehaving nodes. The result is finding a path through which the message can safely be sent from the source to the destination.

1.4 Methodology

Use simulator2 "NS2" to calculate the impact of misbehavior on MANETs network.

1.5 Research objectives

The objectives of this research are to:

1- Identify and understand the techniques for detecting misbehavior.

2- Detect and isolate misbehaving nodes in the network.

3- Increase network reliability by securely sending the packets from sender to receiver.

1.6 Research scope

This research examines mobile ad-hoc networks (MANETs) through the routing protocols, specifically the AODV protocol, as well as the directive misbehavior node and discusses techniques for detecting and minimizing the impact of misbehavior.

1.7 Thesis Layout

This thesis consists of four further chapters, following this introduction.

Chapter 2: Literature Review contains of Classification of wireless networks, Mobile Ad Hoc Networks (MANETs) explaining their characteristics, advantages, applications, and challenges and its types in addition to the Classification of Security Attacks facing this network. It also explains Routing Protocols and its types Specifically, DSR and AODV protocols. In addition, it overviews Previous studies related to the area.

Chapter 3: Methodology explains the IA-ACK Technical Methodology and illustrates a flowchart that explains the steps of this technique. In addition this chapter explains the rules of detecting a malicious node that modifies and drops data and using RREQ and RREP.

Chapter 4: Implementation illustrates the results of this research in the form of tables to displays Node locations and Routes, Times, and Packets that were sent, as well as flow diagrams for the packets sent from the source to the destination with an explanation of the delay, throughput and jitter by using the AODV protocol. In addition the result compare between the proposed technique and other techniques.

Chapter 5: Conclusion and Recommendation provides and discusses an overview of progress and results obtained from this research. A number of recommendations for future work are listed at the end of this chapter.

CHAPTER TWO

LITERATURE REVIEW

CHAPTER TWO

LITERATURE REVIEW

2.1 Background

Wireless networks use a type of radio waves in the air to send and receive data instead of using wires. This network also reduces the cost of maintenance and wiring. The wireless network provides access to information, whether in the office or at home, and the setup of this network is easy and fast and limits wires through walls, and it can extend to locations that cannot use the wired network, and the network is highly flexible. This network may be subject to interference from weather, radio waves from other devices, or obstacles such as walls, etc. The throughput of this network is affected by the presence of many connections.

Wireless networks work similarly to wired networks, but they convert information signals into a form suitable for transmission through the air. It is used in many cases including providing access to corporate data from remote sites. It also allows connection to remote devices without difficulty, but is vulnerable to interference. For this reason, all countries need regulations that define the frequency bands and transmission power for each permitted technology. Also, electromagnetic waves cannot be easily confined to a limited geographical area. So, a hacker can easily listen to the network if the data sent is not encrypted. To ensure the privacy of data sent over wireless networks, all necessary steps must be taken.

2.2 Classification of wireless networks

Wireless networks are classified based on

2.1.1Based on size

Networks are classified according to the geographic areas they cover.

Figure (2.1) below shows a breakdown of networks covering different areas

.

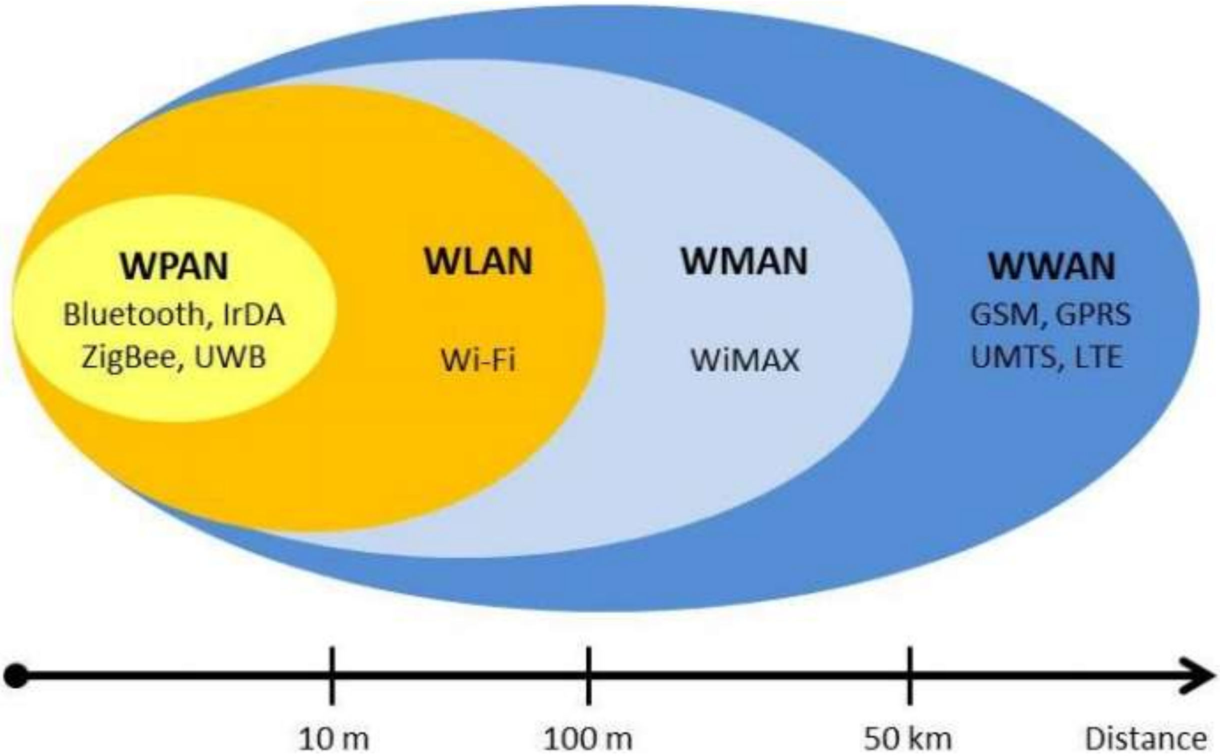

Figure 2.1 classification of wireless networks based on size [1].

- Wireless Personal-Area Networks (WPAN) are based on IEEE 802.15 standards They allow communication in a very short range, of about 10 meters and composed of computers and telephones can be used to connect between the personal devices e.g (Bluetooth).
- Wireless Local-Area Network (WLAN) are based on IEEE 802.11standards and composed of computers in a limited area typical range up to 100 meters such as a home, school or office building, and does not require expensive communication lines e.g (Wi-Fi network).

- Wireless Metropolitan-Area Networks (WMAN) are based on IEEE 802.16 standards and composed of computers within a large area and may cover a whole city e.g (community wireless network).
- Wireless Wide-Area Network (WWAN) Is a wireless network that covers a large area of more than 50 kilometers and connects networks across regional boundaries such as cities or countries and needs the cost of communications lines e.g(cellular network) [1] .

2.2.2 Based on mobility

- static wireless network
- Mobile wireless networks

2.2.3 Based on Infrastructure

- infrastructure
- infrastructure less

2.3 Mobile Ad Hoc Networks (MANETs)

Mobile ad hoc networks (MANETs) is an infrastructure-less , dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack.

2.3.1 Characteristics

- Distributed operation: Protocols must be distributed in the network and do not rely on a centralized node that controls the network. And that the node in the network can enter and leave the network with ease. The nodes involved in a MANET should cooperate with each other and communicate among themselves.
- Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

- Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time.
- Autonomous terminal: In MANET, each mobile node is an independent node.
- Light-weight terminals: The nodes move with less CPU capacity, less storage power, and smaller memory size.
- Shared Physical Medium: The wireless communication medium is accessible to any entity. Accordingly, access to the channel cannot be restricted [2].

2.3.2 Advantages of MANET

- provide access to information and services regardless of geographic position Do not rely on a central server, self-configuring, nodes act as a router
- Scalable.
- Improved Flexibility .
- Robust due to decentralize administration.
- The network can be set up at any place and time.
- Less expensive as compared to wired network [3] .

2.3.3 MANETs Challenges

- Dynamic topology membership may disturb the trust relationship among nodes possibly packet losses.
- Limited bandwidth wireless link continue to have significantly lower capacity than infrastructured networks and The nodes has a limited capacity that allows only access to nodes that are close to one another and thus lose their useful capacity.

- Routing Overhead nodes often change their location within network. So some stale routes are generated in the routing table which leads to unnecessary routing overhead.
- Hidden terminal problem: refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes.
- Packet losses due to transmission errors due to factors such as increased collisions and interference.
- Mobility-induced route changes: ad hoc wireless network is highly dynamic.This situation often leads to frequent route changes.
- Battery constraints Devices used in these networks have restrictions on the power source so the node in this network may act selfishly when you find that there is only a binding control supply.
- Security threats wireless mobile ad hoc nature of MANETs brings new security challenges [4] .

2.3.4. Applications

- Military battlefield
- Collaborative work
- Local level
- Personal area network and Bluetooth
- Commercial Sector
- Intelligent Transportation System
- Wild life monitoring
- Smart Agriculture [5] .

2.4. Types of MANET

2.4.1 Vehicular Ad hoc Network (VANET) They are created through a MANETs application that provides effective communication with another vehicle or helps to communicate with equipment on the side of the road.

2.4.2 Internet Based Mobile Ad hoc Networks (IMANET) Supports Internet protocols and uses network layer routing protocols to connect mobile nodes and create routes automatically.

2.4.3 Intelligent Vehicular Ad hoc Networks (INVANET) Use artificial intelligence to handle unexpected situations such as accidents.

2.4.4 Flying Ad hoc Network (FANET) Consisting of an unmanned aerial vehicle and transporting communications to remote areas [6] .

2.5 Classification of Security Attacks

2.5.1 Passive attacks Does not disrupt the operation of a routing protocol and does not alter the data but attempts to discover the important information from routed traffic.

2.5.2 Active attacks Is very severe attacks on the network prevent the transmission of messages between nodes. These attacks are divided into two parts.

- Active external attacks Can be executed from external nodes do not exist in network.
- Active internal attacks Implemented through malicious nodes that are part of the network, these attacks are more severe and harder to detect than external attacks.

These attacks generate unauthorized access to the network that helps the attacker to make changes such as packet modification and these active attacks are classified into four groups.

- Dropping Attacks.
- Modification Attacks.
- Fabrication Attacks.

- Timing Attacks [7] .

2.6 Routing Protocols

There are a number of routing protocols currently available in adhoc networks. These protocols can be divided into three categories of proactive protocols (Table-driven), Reactive (On-demand) protocols and hybrid protocols.

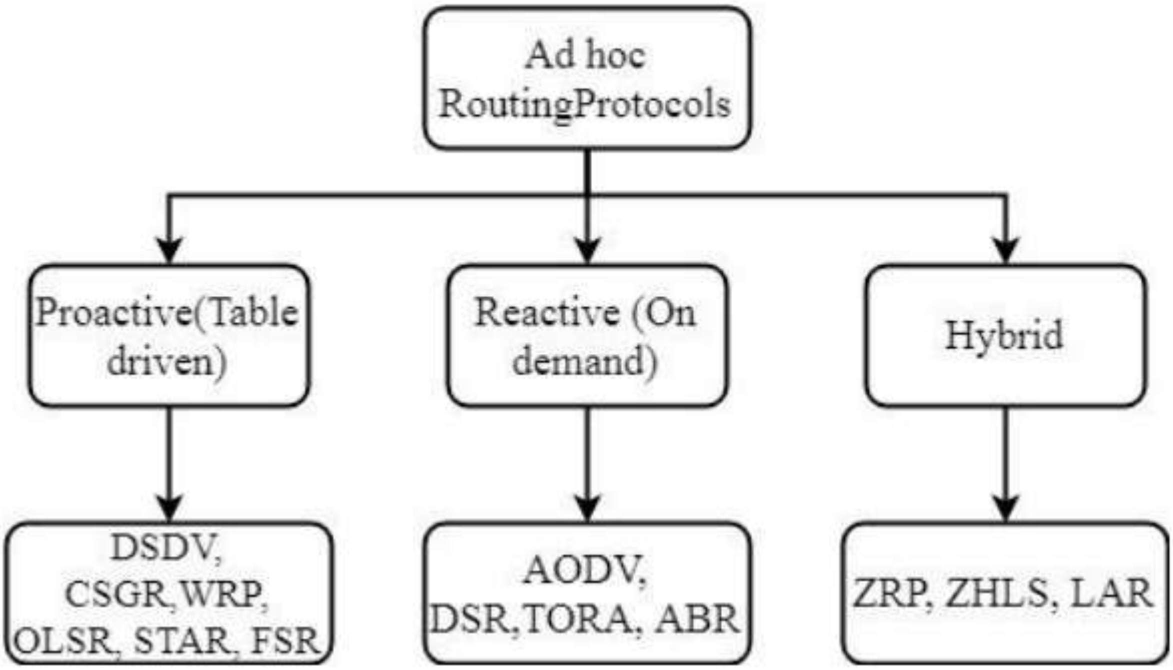

Figure 2.2 classification of routing protocols in MANET [8]

.

2.6.1 Proactive protocols(Table-driven) Also known as table-based routing protocols. Any node maintains a routing table that contains information about the network topology, but this feature consumes power and the routing tables are updated periodically whenever the network topology changes. These protocols are not suitable for large networks because they need to keep node entries for each node in the routing table , Examples of these protocols are DSDV, CSGR, OLSR STAR, WRP, FSR, GSR etc

2.6.2 Reactive protocols(On-demand) Are also known as ondemand routing protocols. This type of routing protocol does not save routing information to reduce overheads. If the node wants to send the packet to another node, this protocol looks for the on-demand manner and establishes a connection to send and receive the packet. The route discovery is always when a request route occurs over the network ,Examples of these protocols are AODV, DSR, TORA, ABR, LMR etc.

2.6.3 Hybrid routing protocols Is a combination of both proactive and interactive routing protocol to make the routing process more efficient and overcome their problems and reduce the pressure on the track. It use Proactive to collect routing information completely and then uses Reactive to retain routing information when a change occurs in the network structure. These protocols are suitable for large networks .Examples of these protocols are ZRP, ZHLS, SHRP, WARP etc [8] .

2.7 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is one of the more generally accepted on demand routing protocols. It is natural to consider the DSR protocol with multiple routes since they may be built during the route discovery by flooding. The Dynamic Source Routing (DSR) protocol also has an option of maintaining multiple routes, so that an alternate route can be used upon failure of the primary one. But in DSR, too many routes are maintained in a trivial manner, without any regard to their ultimate usefulness. The performance study of DSR protocols has not been conducted.

Develop a comprehensive analytic model for the performance study of the multiple route DSR protocol for MANET. At first, introduce two performance metrics. The first metric is the probability that the lifetime of multiple routes is larger than the lifetime of a data transmission.

Note that in the multiple route DSR protocol, the lifetime of multiple routes for a source S to destination D may be longer than the time interval between two data transmission.

2.7.1 The Protocol consists of two main mechanisms

Route Discovery and Route Maintenance, which work together to allow the node to detect and maintain erroneous routes in private mobile networks, and allow multiple routes for any destination and any sender to choose and control the routes used to send the packet.

2.7.1.1 Discover Route Discovery Path discovery is used whenever the source node wants to route the packet to the destination where the source node searches the route cache to verify whether it contains the destination path. If the source node finds a valid path to the destination, you use this path to send its data.

If the node does not have a valid path to the destination, you start the process of discovering a second path by transmitting a route request message that contains the source, destination, and ID address, the intermediate node that received the path request message looking at route cache from the path to Destination. If you do not find the path, this node inserts its address into the message send log and sends the message to the neighboring node. The message propagates over the network until you reach either the destination or the argument node with a path to the destination.

Then there is the route reply message containing a series of nodes to reach the destination where this message is generated and returned to the source.

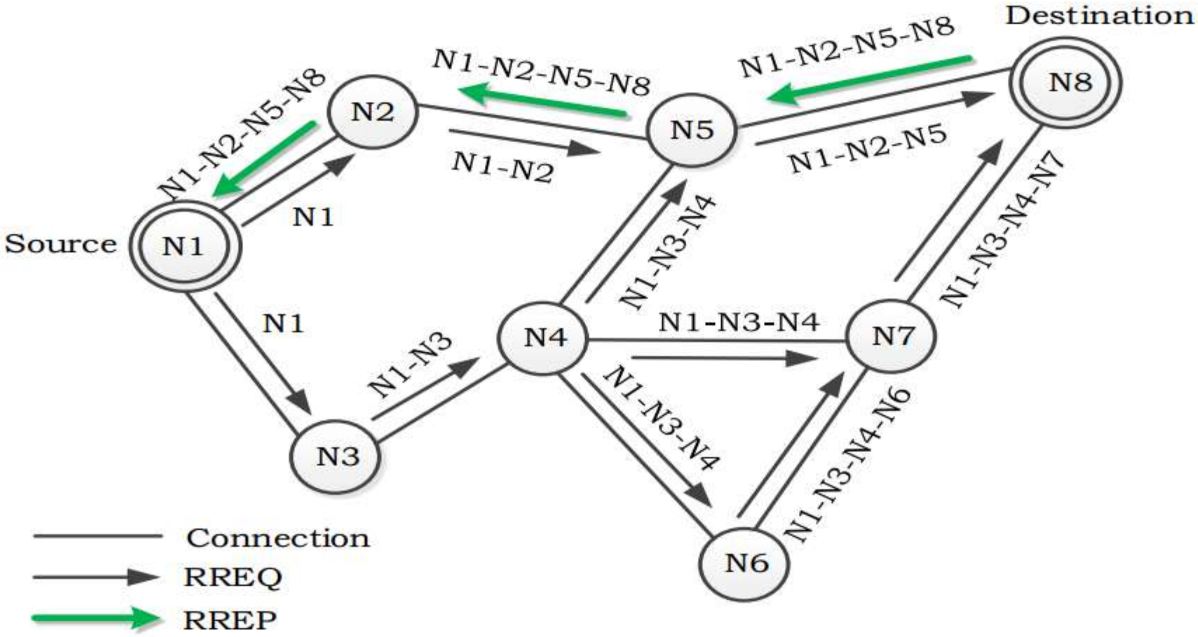

Figure 2.3 Route Discovery Mechanism of DSR [9].

2.7.1.2 Route maintenance Track maintenance is used to deal with path problems. When the node encounters a transport problem in the data transfer layer, it clears the path from its route cache and generates a RERR error message. This message is sent to each node that sent the packet addressed through this disabled path. When you receive the error message (RERR) node, you clear the node that caused the fault from the route cache and send a notification message to be used to verify the correct operation of the path links [9] .

2.8 Ad Hoc On-Demand Distance Vector Routing (AODV)

It is one of the most important types of interactive routing protocol widely used on demand that forms a path from the source node to the destination node at the request of the source node. It means that when the node starts sending data from source to destination, it will start discovering the path between source and destination. For example, if there is a node that needs to send data between the source and destination node, then the node must find the way to its destination [10].

Uses an on-demand-based protocol to discover the desired route and builds route between nodes only at the request of the source nodes. It maintains these routes as long as they are needed by the sources. It is loop-free and self-starting. AODV uses the destination broadcast ID number because the intermediary nodes only forward the first copy of the same request packet , the destination sequence number is created by the destination for any route information that it sends to the request nodes, and it also ensures the freshness of each route created. The route is updated if a new reply is received with the parent destination sequence or the same destination sequence number but the route has fewer hops. Therefore, this protocol will select the freshest and shortest route at any time.

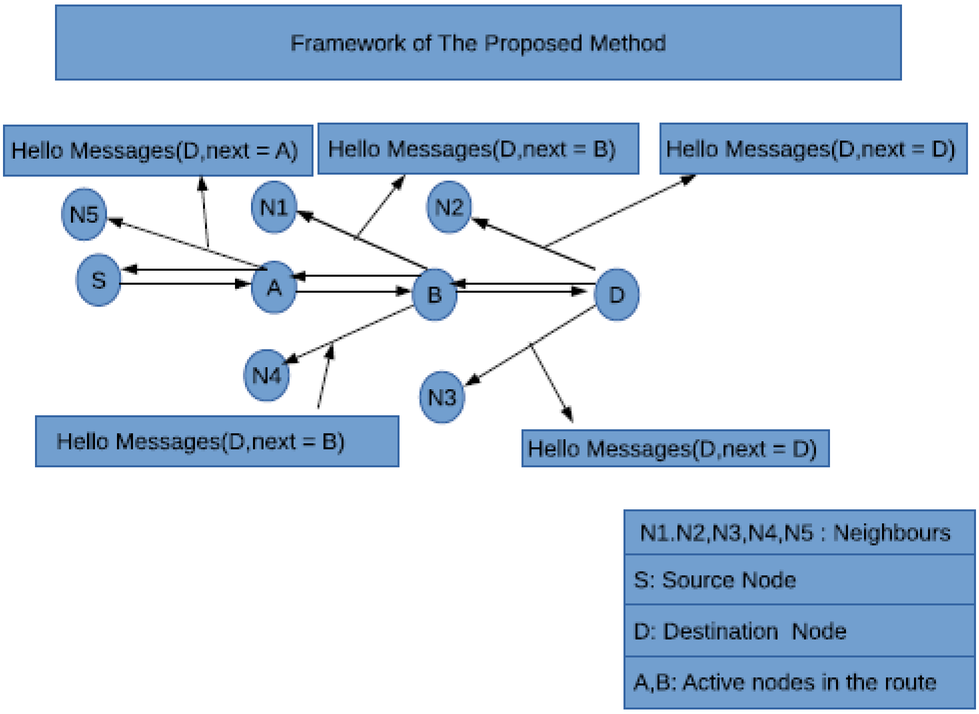

Figure 2.4 The AODV protocol working [11].

2.8.1 The Protocol consists of three main mechanisms

In AODV, there are three types of messages that will govern the working process. They are Route Request (RREQ) , Route Reply (RREP), Route Error Message (RERR) messages. Which is done through two main processes.

2.8.1.1 Route Discovery

If a node needs to send a packet from the source to the destination, it first checks which path is currently available to the destination. If available, it redirects the packet to the Direct Neighborhood node (next step). Else, the path detection mechanism starts. The first purpose of the route discovery process is to create a route request packet (RREQ) that is generated by the source node itself. RREQ packet contains the source address, source sequence number, destination address, destination sequence number, and broadcast ID.

If the node receives RREQ, then it will build a backward path in the routing table for the node from which it received RREQ. The reverse route contains the IP address of the source, sequence number of the source nod , hops count to source, IP address of RREQ received node and lifetime field. The main use of a reverse route is to send a RREP packet to the source as confirmation if the RREQ reaches the destination and if the RREQ IP address matches the destination IP address, the destination node will respond to the RREQ packet by sending an RREP (Route Reply) packet to the source node through Reverse path (unicasting transmission).

The route reply (RREP) packet is which is used for replying for the route request packet sent from the source end . If the node has an exact route to the defined destination, then the destination node will send the route reply packet (RREP) in response to the route request packet (RREQ) This is done because the source must know route for sending the packets to the destination and also not to waste time by searching for alternate route. This packet will contain source address, destination address, destination sequence number, hop count and lifetime fields.

2.8.1.2 Route Maintenance

During the process of sending the packets, all the nodes be active and each and node be monitoring its neighbors. This is done to check whether the nodes nearby are active or not. Also, not all the nodes will be performing better in the network There are cases where the contract fails due to some reason. In AODV, if any node in the active route gets failed, then the Route Error Message (RERR) will be generated . The RERR message is very useful in identifying the nodes that are not contributing for the routing process. This message is generated to inform the neighbor nodes about the link failure [12].

2.9 Types of malicious nodes that infect the MANET network

The misbehavior of the node can consist of selfish or malicious nodes.

2.9.1 Selfish nodes are those nodes which misbehave to save their energy or power and can't share bandwidth**.**

2.9.2 Malicious nodes disturb normal operations of routing protocol by its malicious activities. These nodes may participate in the route discovery and route maintenance phases and transmit control packets which can benefit itself. Attacks of such type are fall into following categories :-

- Denial of Service(DoS) Are production of malicious work with the help of malicious nodes that pose security risks.
- Attacks on Network integrity There are many threats that exploit the routing protocol to provide erroneous routing information.

- Misdirecting traffic The malicious node declares erroneous routing information to obtain secure data before the actual path. The malicious node may declare a wrong path request to send the other nodes replies to that wrong path.
- Attacking neighbor sensing protocols Declares malicious nodes for fake error messages which may result in low network transfer rate and quality of service.

2.9.3 Traffic Analysis Traffic analysis in ad hoc networks may detect following type of information.

- Location of nodes.
- Network topology used for communication.
- Roles played by nodes.
- Available source an destination nodes [13] .

2.10 CYGWIN

‘ Cygwin is a distribution of popular GNU and other Open Source tools running on Microsoft Windows. The core part is the Cygwin library which provides the POSIX system calls and environment these programs expect {Cygwin, 2007 #24} .

The CYGWIN can only do as much as the underlying OS supports. Because of this, CYGWIN will behave differently, and exhibit different limitations, on the various versions of Windows .It flexible and easy to use. You can pick and choose the packets you wish to install, and update them individually. Full source code is available for all packets and tools.

CYGWIN is designed to be interactive, but there are a few different ways to represent this. If you are publishing on multiple systems, the best approach is to run the complete install once, saving all of your entire downloaded packets.

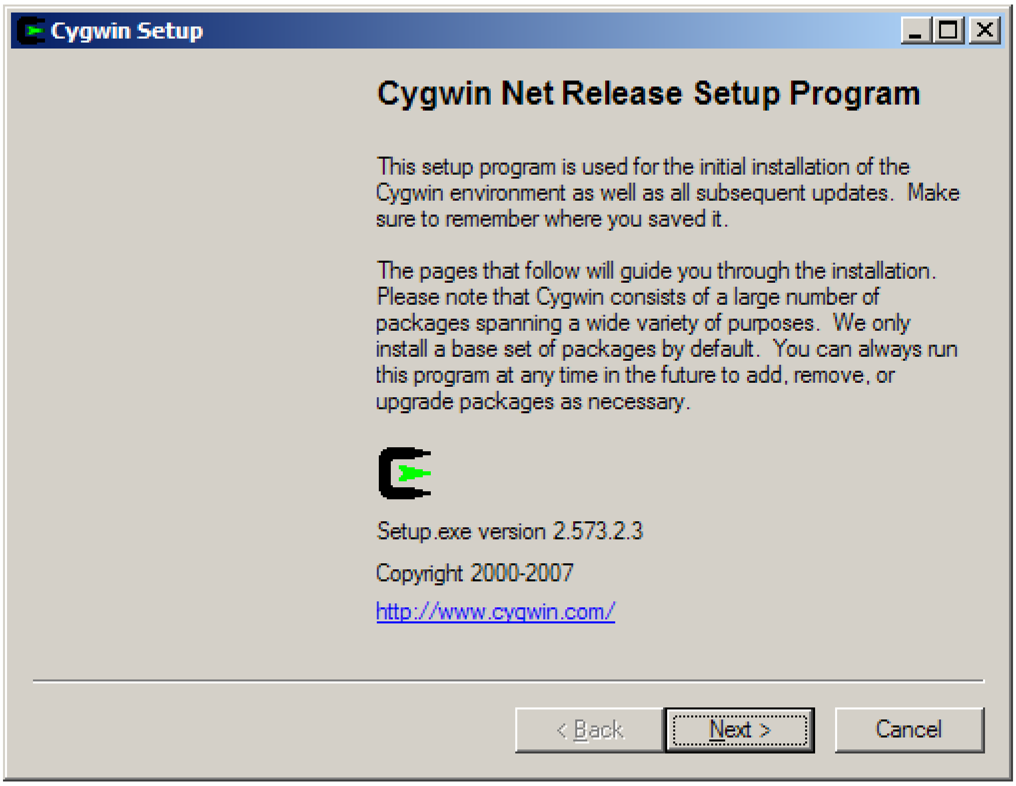

Figure 2.5 first screen starting to install.

Figure 2.6 first screen starting to install.

Then write the following codes in the figure 2.6

Ns .bashrc Startx;

2.11 X-Windows Server

The X-Windows Server is a program that acts as an interface between graphical UNIX applications and the graphics subsystem of the computer. will be setting up an X-Windows Server using Cygwin .

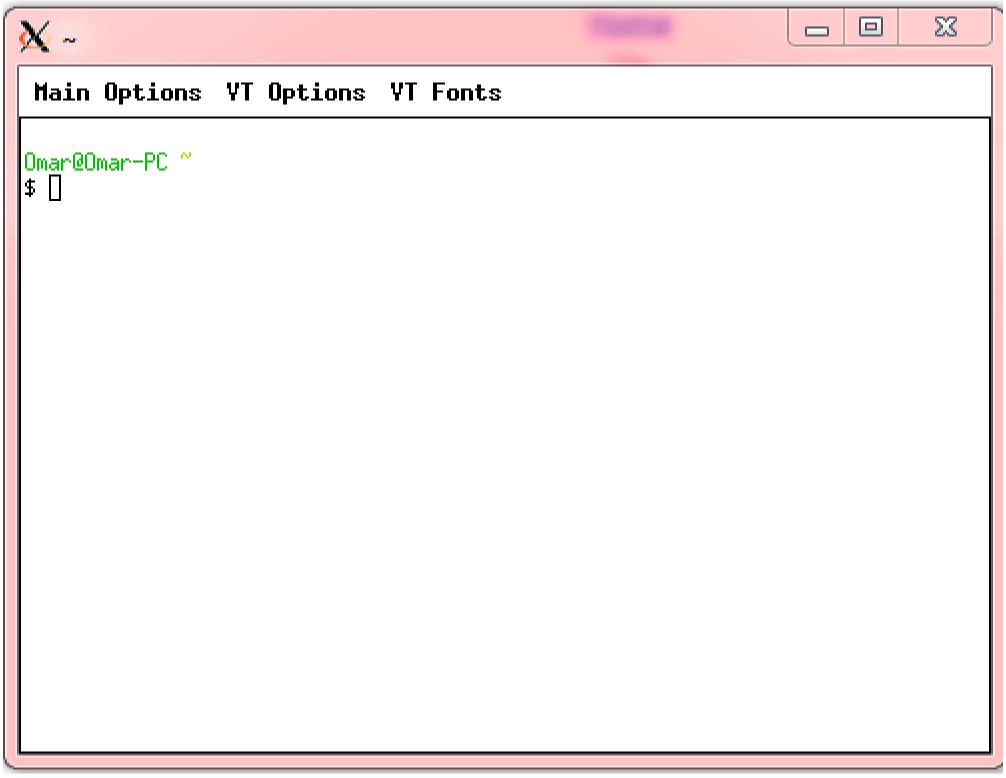

Figure 2.7 screen X-Windows Server

In figure 2.7 execute the simulation program and display the end screen of the MANET networks called Network Animator NAM.

Nam is a TCL /TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools.

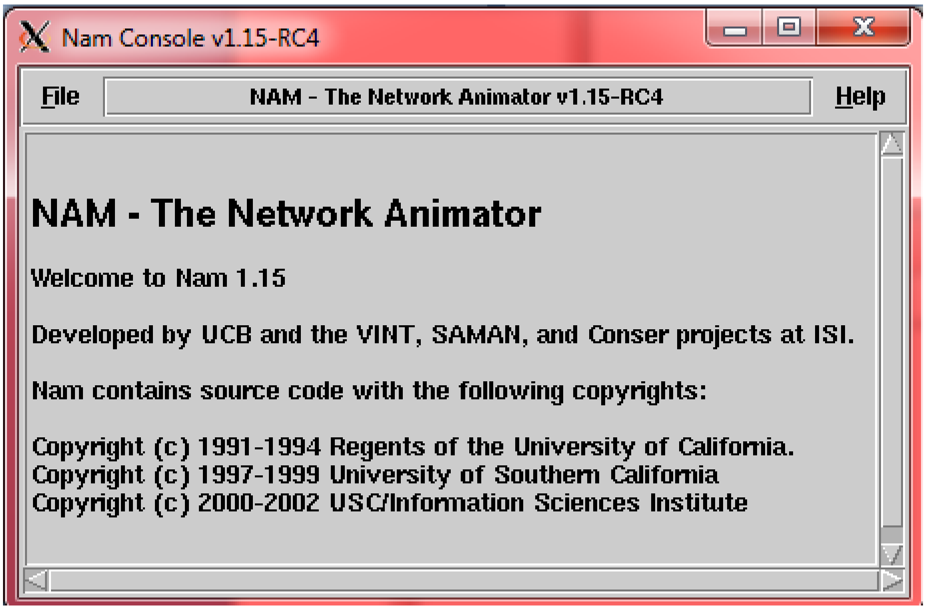

Figure 2.8 screen NAM.

2.12 Network Simulator NS2

Is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks . Due to its flexibility, modular nature, and ease of handling, the NS2 is becoming more widely used in the network research community.

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTCL).

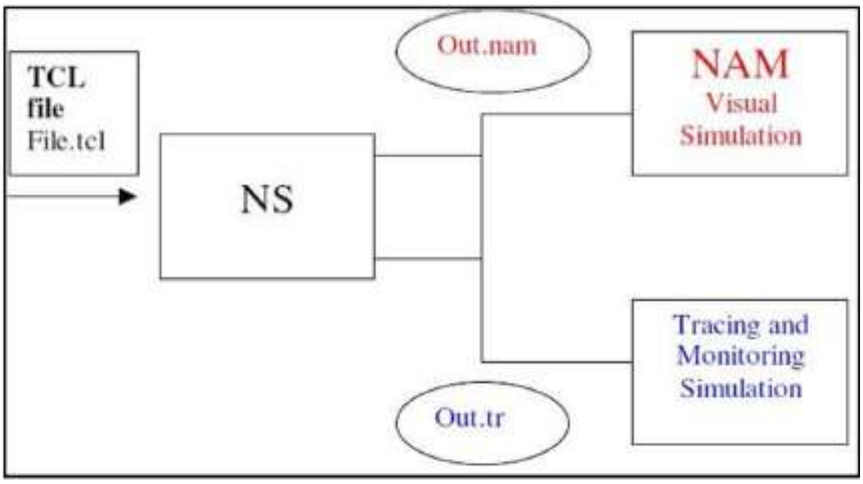

Figure 2.9simplified users view of NS-2 {Pant, #23}

2.13 Tool Command Language TCL

It is a combination of a scripting language and its own interpreter that gets embedded to the application. Its main objective is to provide the ability for the programs to interact with other programs and also to act as an embedded translator.

2.13.1 Features of Tcl

- Reduces development time.
- It runs on Windows, Mac OS X, and almost every Unix platform.
- Extremely simple that it can be learned in a few hours or days.
- Embedded in C, C ++, Java, or vice versa.
- It has a powerful set of networking functions.
- It is open source and free and can be used for commercial applications without any limit.

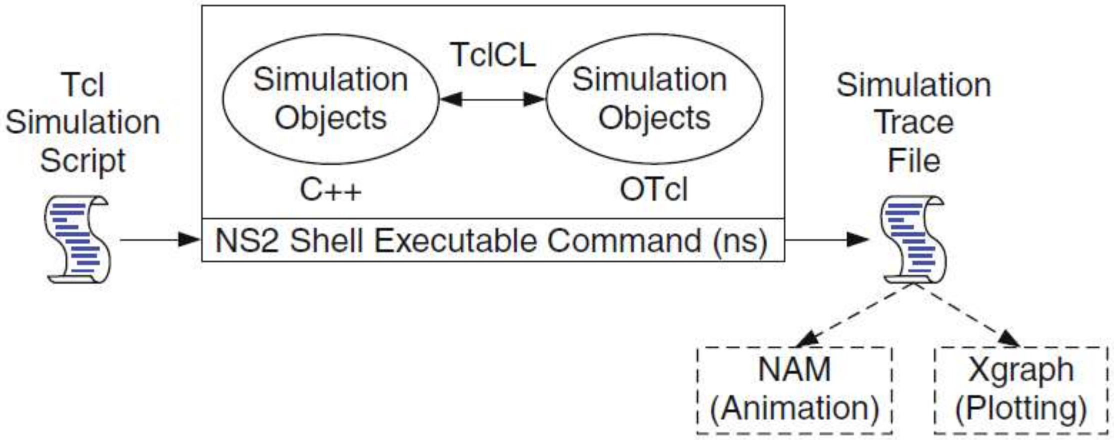

Figure 2.10 Flow of events for a TCL file run in NS {Issariyakul, 2009 #22}.

2.14 Previous studies

2.14.1 I-2ACK Technique

I-2ACK is designed for detection and isolation of misbehaving nodes. I-2ACK is based on sending acknowledgement packets for reception of data packets and using simple rating mechanism for counting the number of data packet such that it overcomes the problem of misbehaving nodes. includes following three steps:-

1. Detection of malicious group

2. Identification of particular misbehaving node

3. Isolation and mitigation of misbehaving node

One of its advantages is its best performance in the presence of misbehaving nodes. Also it is proved that I-2ACK has lesser routing overhead and requires less number of acknowledgement packet transmission [14] .

2.14.2 AACK Technique

One of the Acknowledgment-based schemas and my abbreviation Adaptive Acknowledgment scheme that operates only under the DSR protocol because it needs to know the full path the packet uses to reach its destination. End-to-end is used as a default node mode to reduce the overhead and also develops a node detection algorithm to increase TOWACK detection efficiency

2.14.2.1 Combines two main technique

- First: Enhanced TWOACK (E-TWOACK)

Sunilkumar and manvi used 2ACK technique is technique used to detect and mitigate misbehavior, and also to verify the confidentiality of data transmission in MANET by using a new acknowledgment packet. The receiving node sends a acknowledgment called 2ACK for the sent node indicating that the data was received successfully, One of the advantages of this technique is that it detects misbehavior at the link and its disadvantages are overhead and do not detect the false misbehavior and collaboration node [15] .

Is a technology that improves the technique of TWOACK by adding a mechanism that detects misbehavior at the contract level instead of the connector level because link level detection allows the bad node behavior more than an opportunity to drop more data packets while node level detection identifies the misbehavior node exactly.

- Second: end-to end acknowledgment scheme

One of the advantages of this technology is that all intermediate nodes operate on a regular basis without changing their functions, thus allowing not to consume power and memory. In this technique, the source and destination work together to ensure delivery of data packets and sends the acknowledgment after receiving all data packets

2.14.2.2 Switching Schema

Each node sent in the network operates in two modes, end-to-end acknowledgment mode and E-TWOACK mode, so the switching system is used to enable the node to operate in both modes. The default mode is end-to-end acknowledgment mode, and the sender works in this mode until an encounter occurs a timeout event, uses one bit in the DSR Header field to classify data packets to an end-to-end acknowledgment packet or an E-TWOACK packet.

Its advantages are solving two problems: limited transmission power and the receiver collision [16] .

2.14.3 AMD Technique

This approach is based on the usage of two techniques which will be used in parallel in such a way that the results generated by one of them are further processed by the other to finally generate the list of misbehaving nodes. The first part detects the misbehaving links using the 2ACK technique and this information is fed into the second part which uses the principle of conservation of flow (PFC) technique to detect the misbehaving node. The problem with the 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving. Hence we use the principle of conservation of flow, PFC for the second part which detects the misbehaving nodes associated with that of the misbehaving link.

One of its advantages is to avoid misbehaving nodes successfully, even when a large part of the network is refused to redirect the packet and can operate in multi-channel networks and in network with Directional antennas.

One of disadvantages are sometimes a large part of the network refuses to forward the packet [17] .

2.14.4 Exwatchdog Technique

In his approach an author proposed an improved watchdog mechanism and more powerful in detecting the selfish node and we studied effective trust management system and the combination of trust deriving from network and traditional quality of service (Qo S) trust. The main goal of ExWatchdog is to increase the precision over detection and reduce the detection time in the network.

Improved ExWatchdog protocol is proposed with some modifications to overcome the problem related to the Watchdog protocol.

This Ex Watchdog protocol is very efficient to detect the actual reason for the packet loss. The trust management protocol contains QoS trust with some social trust. ExWatchdog has performed very well in detecting the selfish nodes in the MANET [18] .

Sergio Marti Proposed a watchdog method to detect the misbehaving contract. It is suggested that the path between the transmitter and the receiver has three intermediate nodes A, B, C. A node does not send the entire packet to node C, but sends one packet and then listens to the transmission traffic on node B For example, if node A sends a to node B to resend it to node C, node A often learns whether node B retransmitted to node C or not, by listening to the transmission traffic on node B, the features of this technique reveal the misconduct Redirect level, not just link level. It cannot detect misconduct in the cases:

- ambiguous collision
- receiver collisions
- limited transition power
- limited transition power
- false misbehavior
- collision
- partial dropping [19] .

Khatawkar Added a path rater to Watchdog to work on each node in the network, collects information about the bad node "misbehavior node" and uses documented data to choose the most documented destination. Each node saves the other nodes on the network and calculates the path scale by means of an average calculation The path rater allows the shortest path algorithm to be simulated when unregistered information is collected, but if multiple paths exist for the same face, we choose the path with the largest scale [20] .

Gomathy and Dineshkumar have proposed the E2ACK technique, which is used to improve the 2ACK scheme to detect misbehavior at the link or node level. Its features reduce the number of ACK and reduce the overhead and detect the misbehavior node exactly and also detect the false misbehavior and its disadvantages are collaborative node [21] .

Chinthanai and others have introduced the EAACK technology proposal are designed for receiver collision and false misbehavior, consisting of two main sections misbehavior report authentication (MRA) and Secure ACK (S-ACK) and use digital signature to prevent attackers of forgery packets, but does not discover the cooperative node [22].

Abdulsalam, Tarek, and Elhadi used A 3ACK technique are an acknowledgment-based scheme based on the DSR protocol , designed to handle receiver collision, limit transition power, and detection collaborative node. and its disadvantages do not Collaborating node for more than four consecutive nodes [23] .

Prof. Poonam Gupta , Sarita Chopde used improved 2ACK technique are uses the concept of 2ACK scheme as it is based on it. The improved 2 ACK scheme is used for detecting misbehaving link or node in triplet , designed to reduce number of ACK and detecting which node or link is exactly misbehaved in triplet and handle receiver collision, limit transition power, Limited Overhearing Range ,Routing Overhead. and its disadvantages which hampers the receiver collisions performance and disturbs other packets performance in acknowledging.[24]

A Al-Roubaiey, T. Sheltami ,A. Mahmoud , E. Shakshuki and H. Mouftah used AACK technique It aims to improve the performance of TWOACK scheme and reduces the routing overhead of TWOACK while maintaining better performance and increases its detection efficiency by applying node detection instead of link detection. The AACK scheme benefits are apparent if the number of hops in the path more than 2 hops [25].

CHAPTER THREE

METHODOLOGY

CHAPTER THREE

METHODOLOGY

3.1 Background

The previous chapter discussed the techniques presented by researchers in to solve the problem of monitoring misconduct in the MANETs network by comparing path-level or node detection, routing loading, faulty detection, and preventing bad collaborating nodes.

After studying several papers in this field and using the experimental method, The AODV protocol was used to detect and isolate the malicious nodes it was implemented using NS2 simulator.

This chapter explains the methodology of the AODV protocol and how it works.

3.2 IA-ACK Technical Methodology

This technique applies a method to solve the problem of cooperative contract malpractice and reduce the output overhead of acknowledgments by combining two technologies, AACK and I-2ACK.

The AACK is initiated as a default mode, which is end to end acknowledgment based scheme that sends a packet of type AACK and records the packet number pkt ID and transmission time (T), if the received node receives a packet of type AACK that returns acknowledgment within the specified time period and continue in this scheme otherwise changes the schema mode to the I-2ACK schema.

This I-2ACK scheme starts by sending an I-2ACK packet and records the packet number pkt ID and the send time (T), and then performs the following steps:-

1) The first step is detecting the co-operative groups on misbehavior were nodes are classified into the active routing path (logically divided) for a number of sets (eg S1- S3- S3).

a. Each of these sets consists of three nodes. The first node is referred to as (Lnode), the second node is (Mnode) and the third as (Rnode). The last group of these groups may consist of three nodes as other groups or may include two nodes referred to as (Lnode) and (Rnode), or may contain one node referred to as (Rnode).

b. The (Rnode) node in each group sends two acknowledgments, one to the (Lnode) node in the same group (N) called Ack-1 and the other to (Lnode) in the previous group (N-1) called Ack-2 .

c. Each (Lnode) of each group make sure that it sent packets are waiting for acknowledgment packets.

d. If a group does not receive the Ack-1 packet within the T1 period and the Ack-2 packet within the T2 period then that group is considered a Malicious Group.

2) The second step is to define the specific misbehaving node.

a. If the (Lnode) node receives an Ack-1 packet within the T1 period, it waits for the Ack-2 packet and monitor the number of lost packets on the (Mnode) node.

b. If the specified amount exceeds (Thresholde TS), the (Lnode) node declares that the node (Mnode) is misbehaving.

c. If does not specified amount exceeds (Thresholde TS), the (Lnode) node declares that the (Rnode) node is a misbehaving, and then propagates the information.

d. If the (Lnode) node does not receive the Ack-2 packet within the T2 time period, the (Mnode) node sets a time period T3 for the next group.
e. If the number of lost packets exceedes the specified amount within TS ,the (Mnode) node includes the (Rnode) node in the same group (N) as a misbehaving node, otherwise it classifies the (Lnode) node from the following set (N + 1) as a misbehaving node, and publishes bad nodes information on the network, and so on.

3) The third step is to isolate and reduce the misbehaving node.

a. Each node in the network maintains a list of bad nodes and updates this list to avoid using the misbehaving node for a time period T4.
b. Delete all nodes from the lists to give them another chance to use the network again and avoid being with the bad nodes.
c. If the same node misbehaves for certain number of times, this node is isolated from the network.
d. The chart mode returns to the AACK scheme.

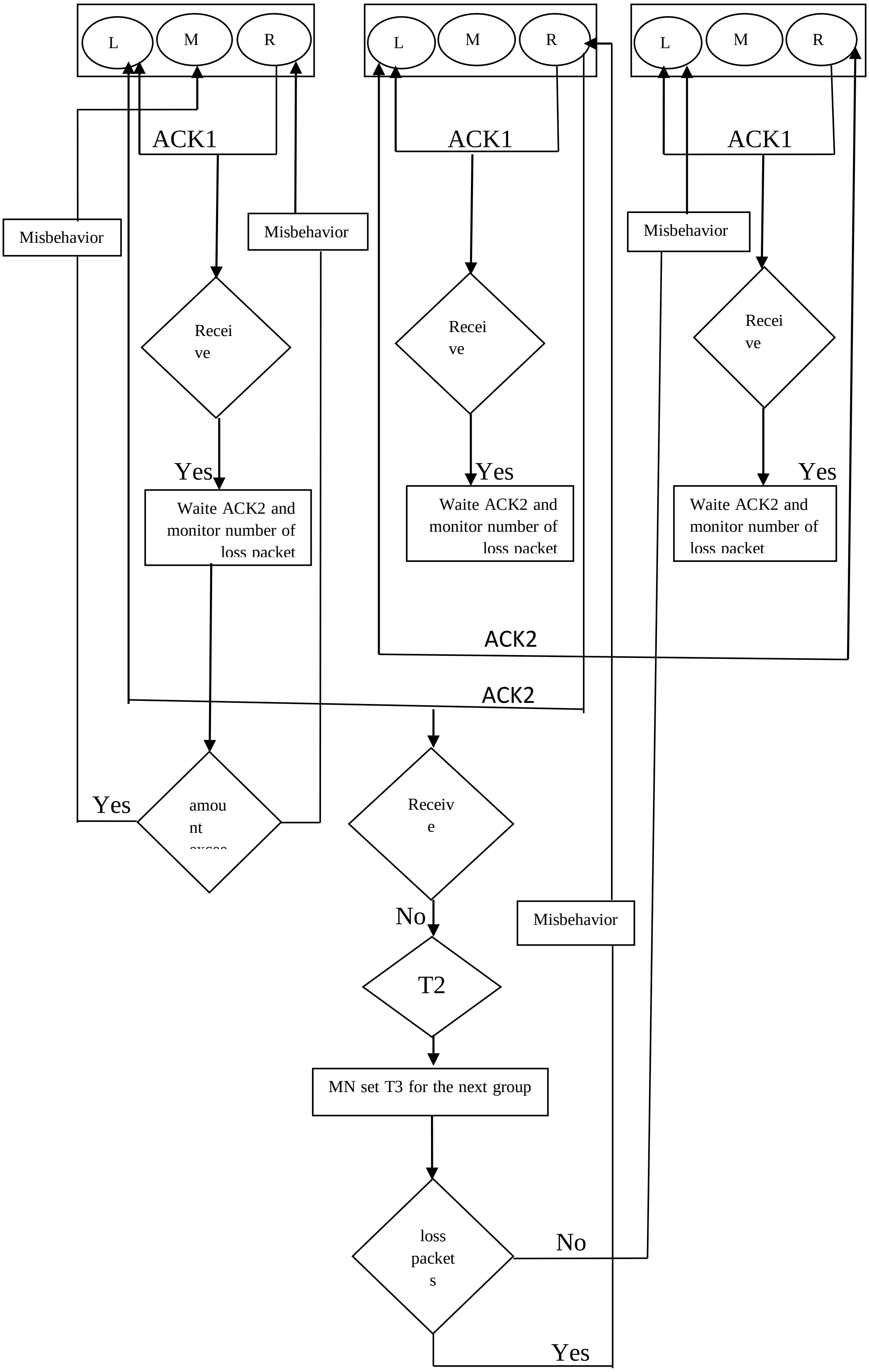

Figure 3.1 Flowchart to explain these steps

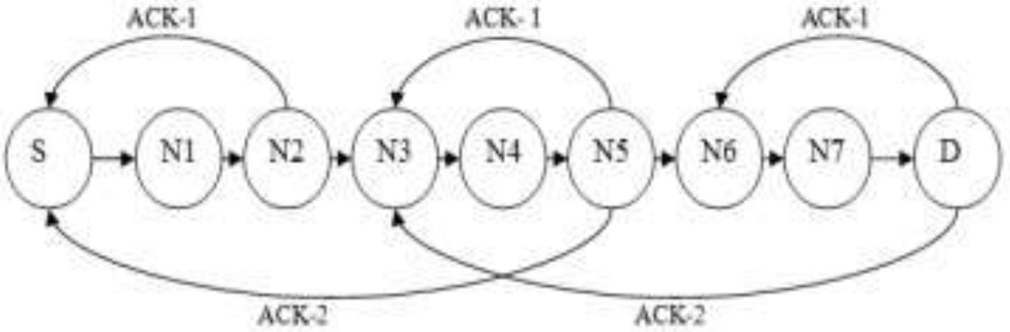

Figure3.2 division of active path nodes into groups and returns of acknowledgment packets [14].

3.3 IA-ACK technology algorithm

The Algorithm

1. Start with AAck mode as default schema.

2. Regular Node Activity.

3. If node mode I − 2Ack then go to (7).

4. Send AAck packet and Register PKT ID and the time (T).

5. If the distention receive AAck packet within the time limit then it sends AAck acknowledgement to source and go to (2).

6. Switch the schema mode to I − 2Ack mode.

7. Send I − 2Ack and Register PKT ID and the time (T).

8. Source node S will form N number of nodes into Sets and each set consists of three consecutive nodes (i.e. LNode, MNode and RNode).

9. LNode and RNode of any set act as temporary source and temporary destination and forward data packets to the next hop along the active route.

10. LNode of every group will make an entry of forwarded data packets in the LIST and wait for ACK-1 and ACK-2 packets which are sent from RNode of first set and RNode of second set respectively.

11. If each LNode makes an entry of forwarded data packet in LIST and received two acknowledgement packets (ACK-1, ACK-2) within time T1 and T2 respectively, then go to (2).

12. If any ACK-1 or ACK-2 packet is not received within their time limit T1 and T2 respectively, then mark that group as malicious group.

13. If switch packet is received then switch schema to AAck mode node.

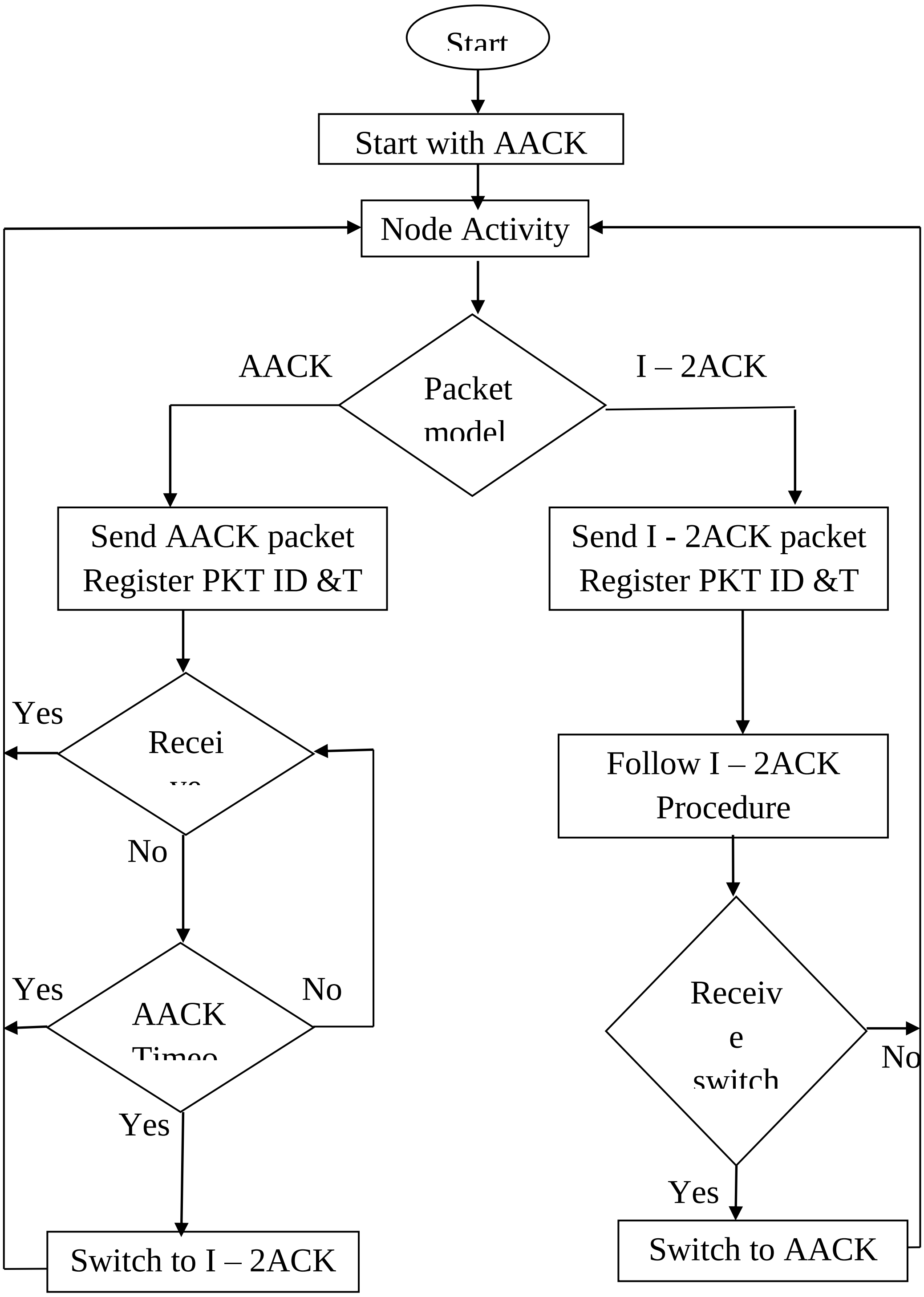

Figure 3.3 flow of steps of the IA-ACK technique

3.4 Detecting malicious node

In AODV routing protocol a malicious node can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DOS) Attack. Also once a route is formed, any node in the route may turn malicious and may refrain from forwarding packets, modify them before forwarding or may even forward to an incorrect intermediate node. Such malicious activities by a misbehaving node can be checked for in AODV protocol. The following rules determine if the node is malicious or not.

Rule 1 If a node delivers many data packets to destinations, it is assumed not to be a malicious node.

Rule 2 If a node receives many packets but does not send the same data packets, it is possible that the current node is a malicious node.

Rule 3 When Rule2 is correct about a node, if the current node has send a number of RREP packets, surely the current node is malicious.

Rule 4 When Rule2 is correct about a node, if the current node has not sent any RREP packets, the current node is a failed node**.**

3.5 Steps to identify malicious nodes by using RREQ and RREP

Step 1 Source node sends the RREQ to the next neighbor node. If the route is found it send a RREP to the source node.

Step 2 If the route is established then source node sends data packet to the next node.

Step 3 If the intermediate node is a malicious node it will drop the packets which it receives from the neighbor node {Sahu, 2013 #2}.

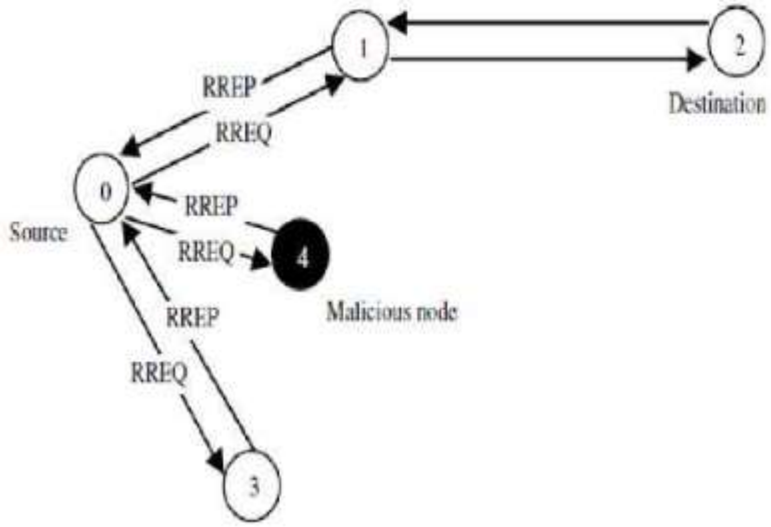

Figure 3.4 RREQ nad RREP in AODV protocol {Patel, 2014 #1}

3.6 Malicious node drops data

Referring to Figure 3.4, when a malicious node C does not transmit data to a destination node D and drops the data, a preceding node B cannot overhear transmission of data of the node C within a predetermined length of time and thus determines that the node C does not transmit data and drops it. Thus, the node B reports the node C as a malicious node.

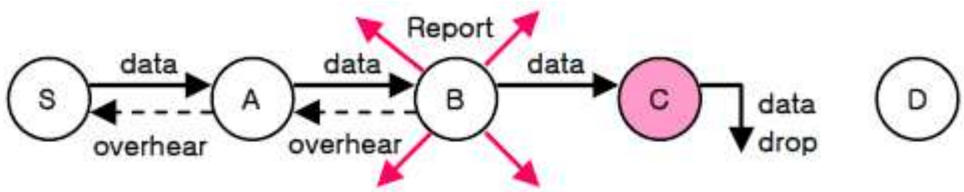

Figure 3.5 Malicious node drops data {Choi, 2005 #3}

3.7 Malicious node modifies data

Referring to Figure 3.5, a malicious node C arbitrarily modifies the content of or a part (or the entire part) of a header of data received from a

node B, and transmits the modified data to a node D. Then, the node B overhears the transmission of the data of the node C and compares the transmitted data with a copy of the data stored in a
buffer of the node B.

When the comparison reveals that the data was arbitrarily changed, the node B considers the node C as a malicious node and reports the node C to a source node S.

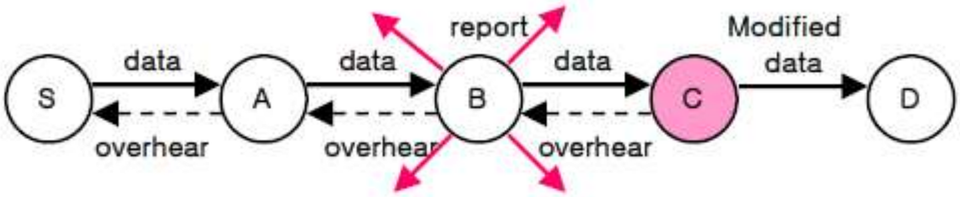

Figure 3.6 When malicious node modifies data{Choi, 2005 #3}.

When the source node S receives the report and does not receive an ACK from the destination node D, the source node S determines that a malicious node is in the current route and sets up a new route.

CHAPTER FOUR

IMPLEMENTATION

CHAPTER FOUR

IMPLEMENTATION

4.1 Background

This chapter displays the implementation of the proposed misbehavior detection and isolation technique. The first section presents the sequence of screens and the function of each screen and its role in detecting and isolating malicious nodes. The second section shows the performance analysis of the packet transmission from the source to the destenation with an explanation of the delay, throughput and jitter by using the AODV protocol and using the CBR protocol in determining the transmission time, the dropped packets, and the path that was followed in sending the packets from the source to the destination.

4.2 Implementation

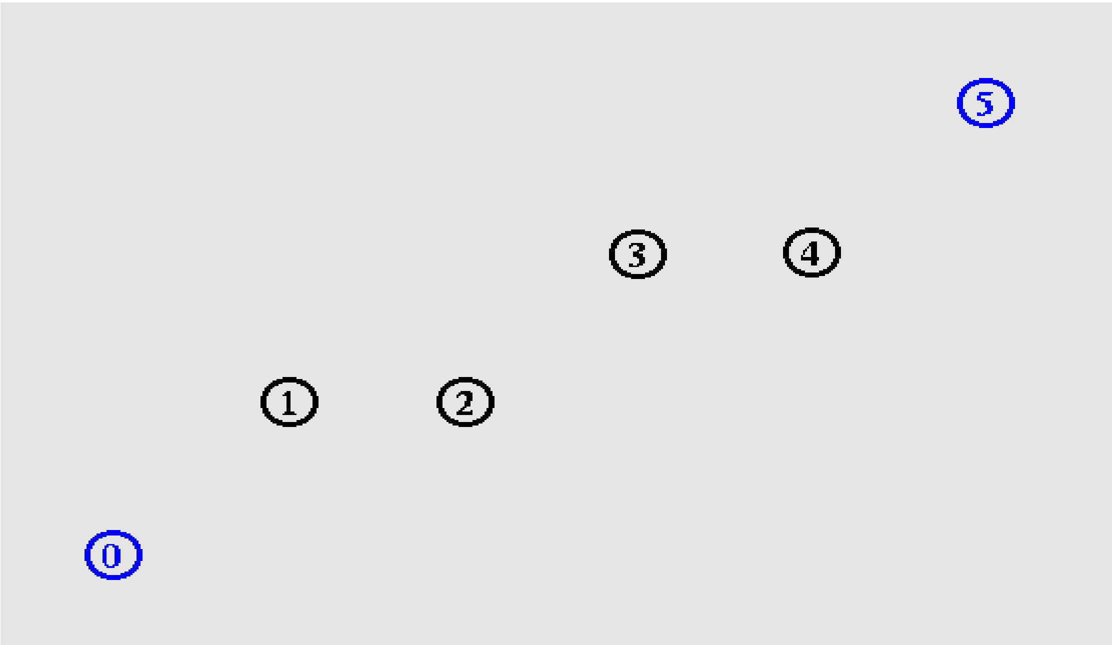

Figure 4.1 Source and destination nodes.

Figure 4.1 shows the number of nodes and determins the source and destination nodes, as the number of nodes is 6 starting from node 0 to node 5. Node 0 is the source node and node 5 is the destenation node.

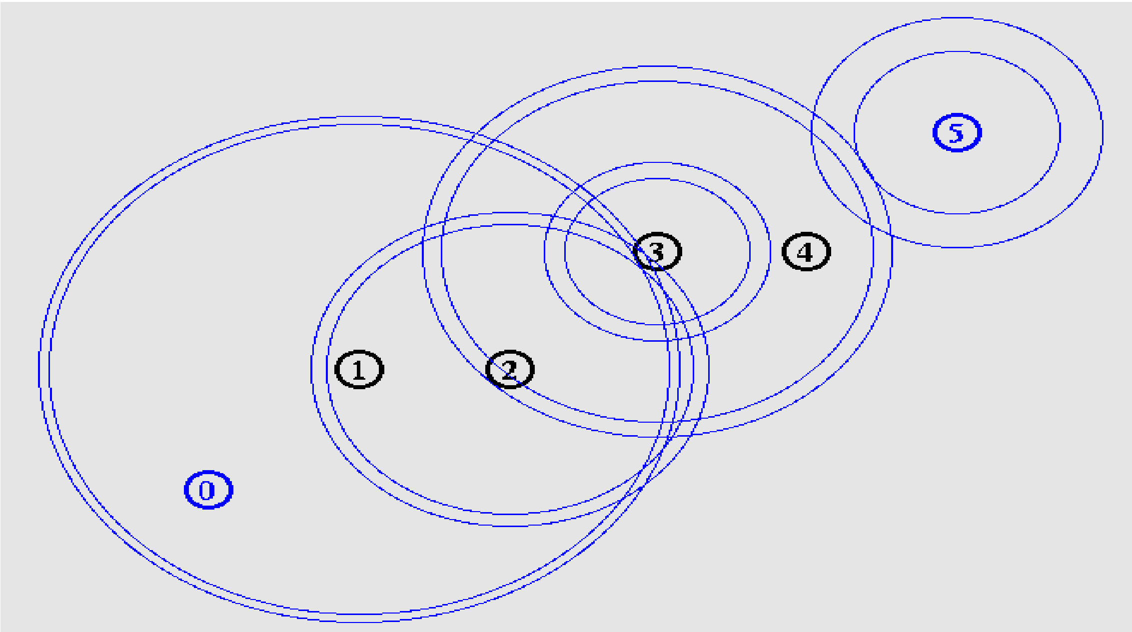

Figure 4.2 broadcasting.

Figure 4.2 shows broadcasting to determine the route between source and destination through which the packet is sent.

Table 4.1 Node locations, CBR and link information.

Node	**Location**	**Link**	**CBR** **N0**→N1→N3→N5	**ACK** N0←N1←N3←N5
N0	(97.5807 , 97.5807)	Between N0 , N1 Bandwidth = 10 Mbits/sec Delay = 10ms	Time = 0.530000 Packets = 1020 byte	Time = 570.6230 Packets =38 byte
N1	(199.404, 199.404)	Between N0 , N1 Bandwidth = 10 Mbits/sec Delay = 10ms	Time = 0.533803 Packets = 1020 byte	Time = 570.6230 Packets =38 byte
N2	(299.538 , 199.692)			
N3	(398.4 , 298.8)	Between N1 , N3 Bandwidth = 10 Mbits/sec Delay = 10ms	Time = 0.544645 Packets = 1078 byte	Time = 0.603475 Packets =38 byte
N4	(499.061 , 299.437)			
N5	(599.942 , 399.961)	Between N3 , N5 Bandwidth = 10 Mbits/sec Delay = 10ms	Time = 0.584788 Packets = 1078 byte	Time = 0.593423 Packets =38 byte

Table 4.1 shows the location, link information and CBR time and packets for each node.

4.3 Performance analysis

The following diagrams illustrate some performance parameters for selected nodes. Figure 4.3 shows the throughput at node 3, Figure 4.4 displays the jitter over time in node 0 and Figure 4.5 shows the delay in node 2.

Table 4.2 shows the routs through which traffic was sent, times packets sent and total packets for each soure-destination.

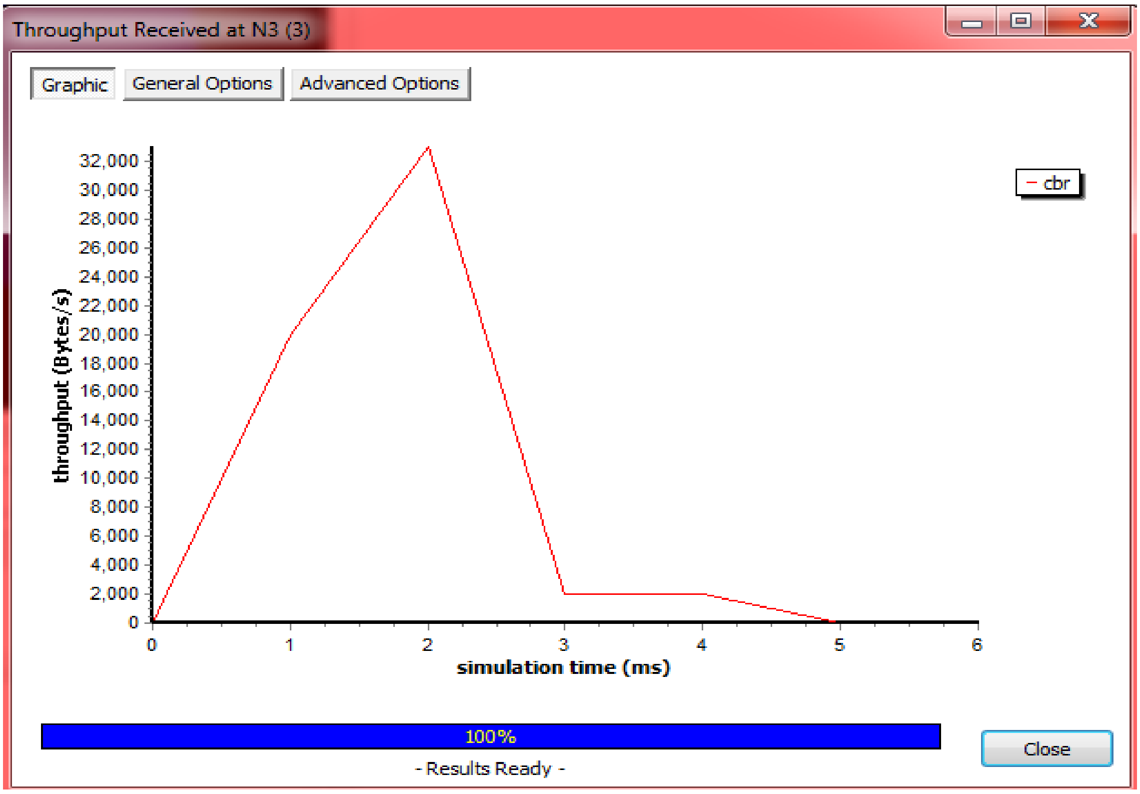

Figure 4.3 Throughput received in Node 3.

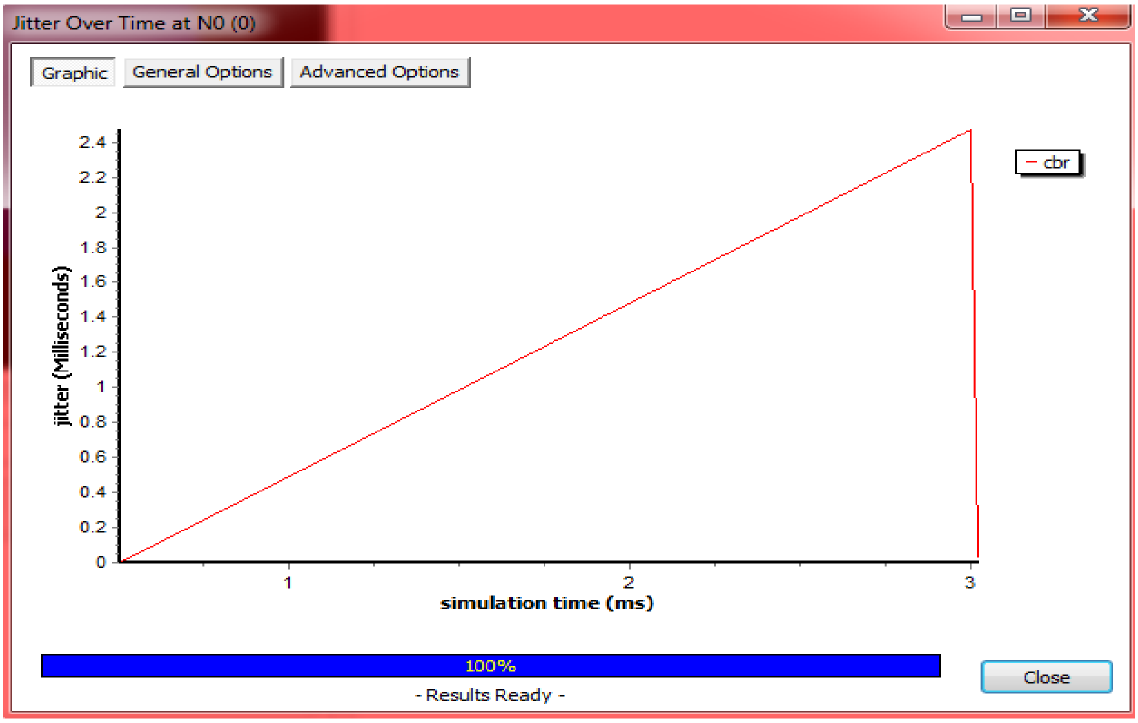

Figure 4.4 Jitter over time in Node 0.

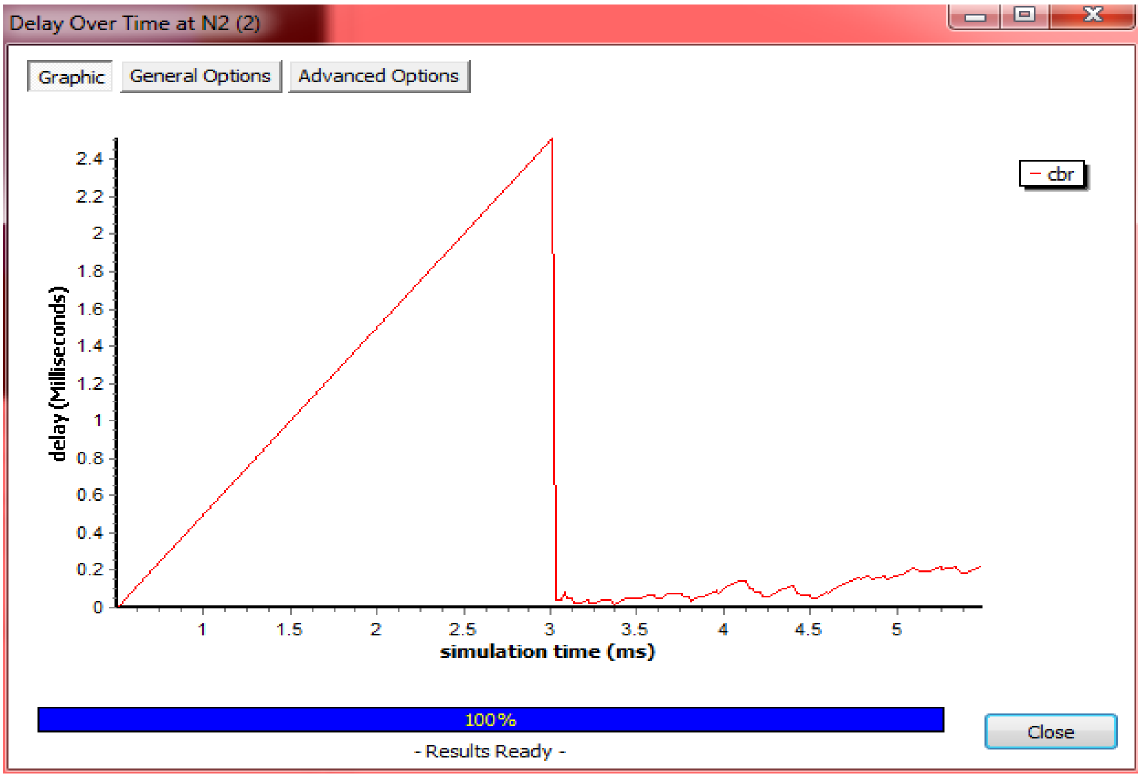

Figure 4.5 Delay over time in Node 2.

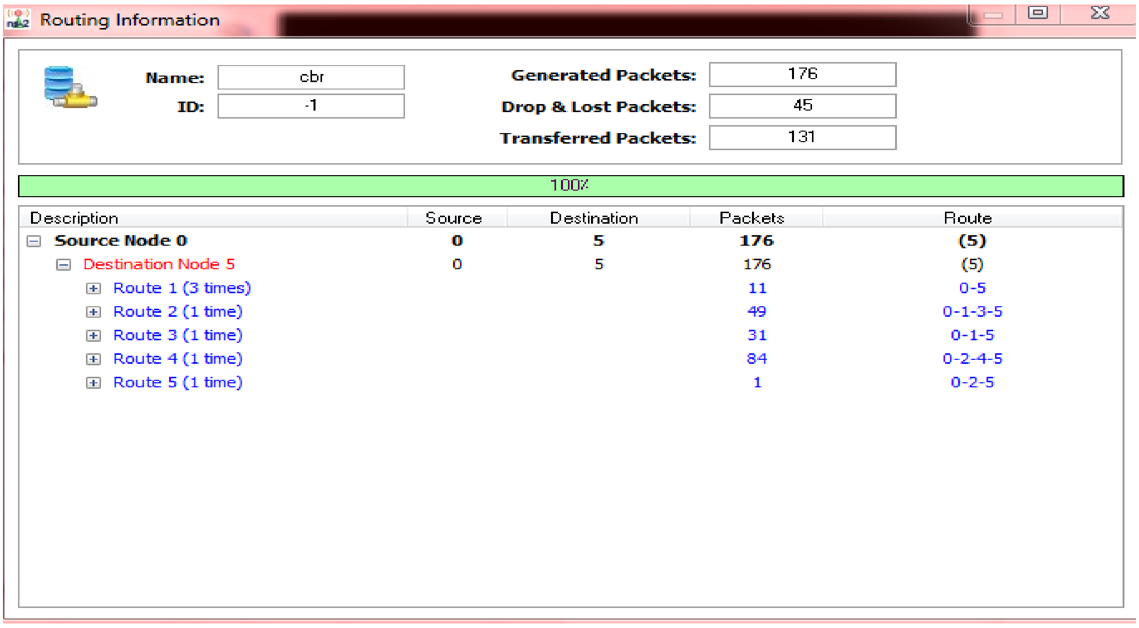

Figure 4.6 Route information between source and destination

Figure 4.6 displays generated, transferred and dropped packets. It also displays source node and destination node, and the route through which packets were sent.

Table 4.2 Routes, Times, and Packets that were sent.

Route	Time1	Time 2	Time 3	Total Packets
Route 1 N0 → N5	T = 0.5000 Packets = 1	T = 2.9300 Packets = 2	T = 5.3000 Packets = 8	11 Packets
Route 2 N0 → N1 → N3 → N5	T = 0.5300 Packets=49			49 Packets
Route 3 N0 → N1 → N5	T= 2.0000 Packets=31			31 Packets
Route 4 N0 → N2 → N4 → N5	T= 2.9900 Packets= 8			84 Packets
Route 5 N0 → N1 → N5	T=5.2700 Packets = 1			1 Packets
All Packets were Sent				176 Packets

4.4 Results

An increase in the number of paths used in the transmission leads to increasing the delay of the transmitted packet, which may lead to a slowdown in the network.

This technique solved problem of cooperative contract malpractice nodes by dividing the nodes into groups and it also reduced the output overhead of acknowledgments by reducing the number of ACK.

Using the AODV protocol reduces space because it uses a single path per destination and better performance compared to DSR protocol, which requires multiple paths for each destination.

Table 4.3 demonstrates that the IA-ACK technique outperforms 2**AC**K and E2ACK techniquesin term of false misbehavior, overhead and node collaboration.

Table 4.3 Comparison between 2**AC**K, E2ACK and IA-ACK techniques.

Technique	**False misbehavior**	**Overhead**	**Collaborative Node**
2ACK	Not detected	Has overhead	Not detected
E2ACK	Detected	Reduces overhead	Not detect**ed**
IA-ACK	Detected	Reduces overhead	Detected

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

Mobile Ad Hoc Networks (MANET) are highly dependent on the cooperation of all its nodes to perform networking functions. This makes it highly vulnerable to selfish nodes. One such misbehavior is routing. When such misbehaving nodes participate in the Route Discovery phase but refuse to forward the data packets, performance may be degraded and less reliable to the end user.

In this research a technique was propose to detect misbehaving nodes and isolate them it from the path and reduce the overhead and also detect misbehaving collaborative nodes by dividing them into groups where that each group consists of three nodes and analyzing and evaluating a technique, called IA-ACK based on AODV protocol. A comprehensive analysis of IA-ACK was performed to assess its performance in detecting and isolating misbehaving nodes.

The results demonstrated positive performances against Watchdog problem and malicious nodes where detected and isolated.

5.2 Recommendations

To improve the current work, the following is recommended.

1. Detect collaborating nodes for more than four consecutive nodes.

2. Using a larger number of paths for transmission, taking into account

reducing delay and increasing productivity.

3. Improving the proposed method to further reduce overhead.

4. Using protocols other than AODV.

Reference

[1] J. Salazar Soler, "Wireless networks," ed: European Virtual Learning Platform for Electrical and Information Engineering, 2017.

[2] A. K. S. Ali and U. Kulkarni, "Characteristics, applications and challenges in mobile Ad-Hoc networks (MANET): overview," *Wireless Networks,* vol. 3, 2015.

[3] R. Jatain, "Review on Congestion Control in MANET," 2018.

[4] S. Agarwal, R. Kaur, and T. Agarwal, "MANET Expansion Security Challenges Attacks and Intriguing future Trends," 2018.

[5] A. Gupta, P. Verma, and R. S. Sambyal, "An Overview of MANET: Features, Challenges and Applications," 2018.

[6] S. Mirza and S. Bakshi, "Introduction to MANET," *International Research Journal of Engineering and Technology,* vol. 5, pp. 17-20, 2018.

[7] D. S. Aarti, "Tyagi,"Study Of Manet: Characteristics, challenges, application and security attacks"," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, pp. 252-257, 2013.

[8] J. Pragati , Akash, Sanghi, "Review of Various Routing Protocols in Mobile Ad-Hoc

Networks (MANETs)," *International Journal of Innovations & Advancement in Computer Science,* vol. 7, p. 10, 2018.

[9] M. Al-Shora, S. Nouh, and A. Khalifa, "PERFORMANCE EVALUATION AND COMPARISON OF DSR, MDSR AND RDSR ROUTING PROTOCOLS," 2018.

[10] A. Kurniawan, P. Kristalina, and M. Z. S. Hadi, "Performance Analysis of Routing Protocols AODV, OLSR and DSDV on MANET using NS3," in *2020 International Electronics Symposium (IES)*, 2020, pp. 199-206.

[11] M. Atto, R. J. Mstafa, and A. Alkhayyat, "Improving AODV Routing Protocol for Image Transmission Over Mobile Video Sensor Networks," *IEEE Access,* vol. 8, pp. 169396-169407, 2020.

[12] S. Deepak and H. Anandakumar, "AODV route discovery and route maintenance in MANETs," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 2019, pp. 1187-1191.

[13] A. Gagandeep and P. Kumar, "Analysis of different security attacks in MANETs on protocol stack A-review," *International Journal of*

Engineering and Advanced Technology (IJEAT), vol. 1, pp. 269-75, 2012.
[14] A. S. A. Ukey, M. Chawla, and V. P. Singh, "I-2ACK: Preventing routing misbehavior in mobile ad hoc networks," *International Journal of Computer Applications,* vol. 62, 2013.
[15] S. S. Manvi, L. B. Bhajantri, and V. K. Vagga, "Routing misbehavior detection in manets using 2ack," *Journal of Telecommunications and Information Technology,* pp. 105-111, 2010.
[16] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, "AACK: Adaptive acknowledgment intrusion detection for MANET with node detection enhancement," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 634-640.
[17] S. Alagumuthukrishnan, K. Geetha, J. B. Achsah, and A. A. Mary, "Monitoring the Misbehaving Nodes in MANET using Audit-Based Misbehaviour Detection (AMD) Method," *Asian Journal of Applied Science and Technology (AJAST),* vol. 1, pp. 185-189, 2017.
[18] M. C. Nimje and P. Junghare, "Detection of node activity, selfish & malicious behavioral patterns using exwatchdog algorithm," *Int J Eng Sci,* vol. 5676, 2017.
[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255-265.
[20] S. Khatawkar, U. Kulkarni, and K. Pandyaji, "Detection of Routing Misbehavior in MANETs," in *International Conference on Computer and Software Modeling IPCSIT*, 2011.
[21] M. P. D. Mrs.K.Gomathy, "Detection Of Routing Misbehavior In Manet By

Enhanced 2ack Scheme Using Dsr Protocol," *International Journal Of Engineering And Computer Science,* vol. 2, 2013.
[22] T. S. K.Chinthanai chelvan, V.Prabakaran,D.Saravanan, "EAACK-A Secure Intrusion Detection System for MANET

" *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, 2014.
[23] A. Basabaa, T. Sheltami, and E. Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds," *Procedia Computer Science,* vol. 32, pp. 571-578, 2014.

[24] P. Gupta and S. Chopde, "Detection of routing misbehavior in MANET using improved 2ACK," *IOSR Journal of Computer Engineering,* vol. 9, pp. 53-60, 2013.

[25] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, "AACK: Adaptive acknowledgment intrusion detection for MANET with node detection enhancement," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 2010, pp. 634-640.