ENHANCED APPROACH FOR DETECTING SINGLE AND COOPERATIVE ATTACKS IN MOBILE AD HOC NETWORKS

ABDULRASHID SABO
SPS/14/MCS/00003

A DISSERTATION SUBMITTED TO THE POSTGRADUATE SCHOOL THROUGH THE DEPARTMENT OF COMPUTER SCIENCE, BAYERO UNIVERSITY, KANO IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MSC IN COMPUTER SCIENCE

DECEMBER, 2017

DECLARATION

I hereby declare that this work is a product of my research efforts that was undertaken under the supervision of Dr Abdulwahab Lawan and has not been presented in Bayero University, Kano and elsewhere for the award of Masters of Science in Computer Science. All sources referenced have been duly acknowledged.

Name Abdulrashid Sabo

SPS/14/MCS/00003

Sign: _____ Date: _____

CERTIFICATION

This is to certify that the research work of this dissertation and its subsequent preparation is undertaken by Abdulrashid Sabo (SPS/14/MCS/00003) was carried out under the Supervision of:

Abdulwahab Lawan (PhD)
Department of Information Technology
Faculty of Computer Science and Information Technology
Bayero University, Kano

APPROVAL

This dissertation has been examined and approved for the award of Masters of Science in Computer Science.

Supervisor

Abdulwahab Lawan (PhD)

Sign: _____ Date: _____

Head, Department of Computer Science

Mal. Mansur Babagana,

Sign: _____ Date: _____

Representative of School of Postgraduate Studies

Bashir S. Galadanci, PhD

Sign: _____ Date: _____

ACKNOWLEDGEMENT

I would like to begin by expressing my gratitude to Allah (SWT) for giving me the opportunity to complete this dissertation.

I offer sincere appreciation to my able supervisor Dr. Abdulwahab Lawan for his invaluable support and guidance toward the successful completion of this dissertation.

My special thanks to Malam Mubarak Umar and Malam Auwal Tata for their useful guidance and support that make this work possible.

Special thanks to the entire families of Alh. Sabo Babale, Hajiya Ana and all members of Ambitious Allies for their support, prayers and advices during the period of the research.

I will not forget to express my special thanks to Sadiya Bashir Namalam for her support and tireless prayer.

DEDICATION

I dedicate this research work to my beloved parents, my granny (Hajiya Ana Mai Fura), my brothers and sisters who have encourage me throughout the period of this work.

ABSTRACT

Mobile ad-hoc network is a system of wireless mobile nodes that are dynamically self-organize in arbitrary and temporary topologies, with no fixed set of communication infrastructure and lack centralized administration, where network devices are inter-connected through wireless interface. Mobile nodes in MANETs not only act as a host but as a router or relay stations for forwarding packets from source to destination. The dynamic nature and other characteristics of MANETs such as nodes mobility dynamic and topological changes makes it highly susceptible to various security attacks ranging from collaborative black hole/ grayhole attacks, sink hole attacks to eavesdropping attacks. The mentioned attacks mainly disrupt the routing process by giving false routing information in MANETs, thus finding safe routing path by avoiding malicious nodes is a genuine challenge. The research work aim at in cooperating RSA encryption algorithm to the cooperative bait detection scheme. The proposed work allow the source to use public key crypto system (in this case RSA) to encrypt data before transmitting it to the destination after the initial reverse tracing operations, it eliminate the use threshold value use to indicate the reoccurrence of malicious nodes, it also eliminate the use of confirmation RREQ, since the public key cryptosystem introduce by the is sufficient enough to cover the transmitted data from an unknown attacker. The research work was simulated using network simulator tool NS2 and simulation results shows that the proposed work show and increase in packet delivery ratio, network throughput and also show a remarkable decrease in routing overhead and end to end delay.

Table of Contents

List of Figure.

List of Tables

List of Abbreviations

MANETs Mobile Ad hoc Networks

CBDS Cooperative Bait Detection Scheme

ESCBDA Enhanced Secured Cooperative Bait Detection Approach

DSR Dynamic Source Routing

AODV Ad hoc On-Demand Distance Vector Routing protocol

OLSR Optimize Link State Routing Protocol

DSDV Destination Distance Vector Routing Protocol

FSR

WRP Wireless Routing Protocol

CGSR

TORA Temporally Ordered Routing Protocol

ABR Associativity Based Routing Protocol

GSR Global State Routing Protocol

STAR Source Tree Adaptive Routing Protocol

HSR Hierarchical State Routing Protocol

MAC Medium Access Control

RREQ Route Request

RREP Route Reply

RERR Route Error

TTL Time to Live

UDP User Datagram Protocol

CBR Constant Bit Rate

TV True Value

MAODV Modified Ad Hoc On-Demand Distance Vector Routing Protocol

ECBDS Enhance Cooperative Bait Detection Scheme

NHN Next Hop Neighbor

IN Intermediate Node

SN Source Node

FRq Further Route Request

DRI Data Routing Information Table

RTT Round Trip Time

TOR the Onion Routing

BFTR Best Effort Fault Tolerant Routing

SRR_REQ Secured Reliable Route Request

SRD_REP Secured Reliable Route Discovery Reply

RL Reliability List

EMAODV Enhanced Modified Ad Hoc On-Demand Distance Vector

RIP Restricted IP

BBN Backbone Node

PDR Packet Delivery Ratio

UID Unique Identification

CHAPTER 1

INTRODUCTION

1.1 PREAMBLE

This chapter consists of a Background of the study, its importance and applications, problem statements, aim and objectives of the study; the scope and limitation of the study; it also includes the significance and motivation of the study.

1.2 BACKGROUND OF THE STUDY

Past few years have witnessed rapid growth in the area of mobile computing due to proliferation of inexpensive widely available wireless devices, this has opened opportunity for researchers to work on wireless mobile ad-hoc networks MANETs [1]. Mobile ad-hoc network is a system of wireless mobile nodes that are dynamically self-organize in arbitrary and temporary topologies where nodes are free to join and leave the network dynamically without fixed set of communication infrastructure and lacks centralized administration [31]. In MANETs mobile host also act as routers or relay station to forward data from source to destination, thus animals, sensors and vehicles can be interconnected in areas with-out pre-existing communication infrastructure.

MANETs can be applied in many areas where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use or is completely damage due to natural disaster. Since MANETs allow mobile nodes or wireless devices to maintain connections to the networks as well as easily adding or removing devices to and from the network, it can be applied in different aspect in our lives where conventional networking cannot be applied. Some application areas of MANETs includes sensor networks for detection of different number of environmental properties such as pressure, temperature, pollution and toxins, military field for relaying information related to situation awareness in the battle field among group of soldiers, search and rescue operations for disaster relief and in universities for campus settings of virtual class rooms, lectures and meeting rooms [32].

1.3 STATEMENT OF THE PROBLEM

In mobile ad-hoc networks, the most important thing is to establish connections between nodes and that node should cooperate with each other in transmitting packets from source to destination and throughout the entire life time of the network. MANETs routing protocols enable nodes to be connected with one another through hop-by-hop manner, so every individual node in MANETs takes route decision to forward packet from source to destination or to its neighbor through intermediary nodes and then to the destination, this make it easier for a malicious node to attack this kind of networks or a legitimate node refuse to forward packet thus acting as a malicious node.

In [1] due to the vulnerabilities of MANETs a malicious node known as black hole node uses the routing protocol especially DSR and AODV to send fake routing information in the network to claim that it has an optimum route to the destination node, causing other legitimate nodes to route data packet through the malicious node. In the case of cooperative black hole nodes, multiple malicious node collide to launch cooperative attack in order to disrupt the routing process of the network by dropping all packets that come across the malicious node. Though [1] attempt to address the problem of cooperative black hole attacks using cooperative bait detection scheme in which the source node uses the address of its neighbor as bait destination address to bait malicious node send fake route reply and uses the reverse tracing algorithm to track and eliminate malicious nodes from the network, the scheme lacks message encryption security scheme that make data to be transmitted with security by encrypting and hiding its content from malicious nodes. It doesn't also address other types of security attacks in MANETs such as the eavesdropping attacks, a situation where a malicious node intercept and read messages or conversation between source and destination by using an RSA encryption algorithm where the eavesdropper node would only see the encrypted message which is not readable and cannot be decrypted by it, and sinkhole attacks a situation where a malicious node advertises wrong routing information to produce itself as a specific node and receive whole network traffic after which it will modifies the secret

information by making changes to the data content or drop them to make the network more complicated [31].

This research work is an attempt to address the issue of insecurity during data transmission, found in the reviewed literatures by in-cooperating a well-known powerful message passing security scheme, in this case an RSA encryption algorithm is chosen to encrypt data using the public key of the destination node before it is transmitted and be decrypted at the destination node using its private key, this makes data to be sent with security across the routing path and the network, since only legitimate node can decrypt and know data contents. Thus the research work can address other types of security attacks such as the eavesdropping and sinkhole attacks since these attacks are perform only when the attack have access to the content of data packet.

1.4 AIM AND OBJECTIVES

The research aim to in-cooperate RSA encryption scheme to the cooperative bait detection scheme in order to detect and prevent malicious nodes from intercepting, modifying and unauthorized reading of transmitted information and launching of single and cooperative attacks in MANETS by malicious nodes.

The objectives are:

I. To identify malicious nodes in mobile ad hoc network in order to improve the reliability of the routing process through simulation
II. To prevent single and cooperative black hole attacks in MANETs
III. To introduce an encryption scheme to the CBDS (substitute the transposition encryption scheme in SCBDA) in order to hide data content from the malicious node there by improving security.
IV. To find a more secured routing path from source node to destination node avoiding the black hole nodes.

1.5 SCOPE AND LIMITATIONOF THE STUDY

The scope of this research work is to explore the cooperative bait detection scheme and implement public key crypto system as a tool for preventing the reoccurrence of

cooperative black hole attacks in MANETs. To simulate the scenario of the mobile ad-hoc network nodes using network simulator tool NS2 which record the simulated data in a simulation file. The simulated data is analyzed using network animator tool NAM and Xgraph. The data used in the research are generated by the CBR source selected by the user.

The proposed research work have the following limitations

I. The process of the RSA cryptosystem key generation is assumed throughout the simulation scenarios

II.

The next chapter discussed literatures related to the research work and the operational mechanism of the proposed work.

1.6 RESEARCH MOTIVATION

1.7 SIGNIFICANCE OF THE RESEARCH WORK

CHAPTER 2

LITERATURE REVIEW

2.1 PREAMBLE

This chapter consists of a brief introduction of mobile ad-hoc routing protocols, then review some literatures related to the research work and closes with the discussion on the operational mechanisms of the proposed work.

2.2 MOBILE AD-HOC NETWORKS ROUTING PROTOCOLS

Communication between source and destination in mobile ad hoc networks occur through wireless links, when the two are within communication range they communicate directly else, an intermediate node(s) help forwards packet to the designated node. To make communication easier and more effective routing protocols are required to established routes between participating nodes, conventional routing protocols used in infrastructure based networks, based on distance vector or link state algorithms cannot be applied here due to limited transmission range, multiple network hop may be needed to enable communication between two nodes in the network and the frequent unpredictable dynamical topological changes of mobile ad hoc networks [27].

Routing protocols in MANET play important role in finding routes for data transmission, according to [25] the classification of routing protocol in MANETs can be done in many ways, but most of these are done depending on the routing strategy which consist of proactive and reactive routing protocols and depending on the network structure which include flat hierarchical and the geographic position assisted routing protocols, both table-driven (proactive) and on-demand (reactive) routing protocol falls under flat routing protocol, figure1.1 shows the classification of routing protocol in MANETs.

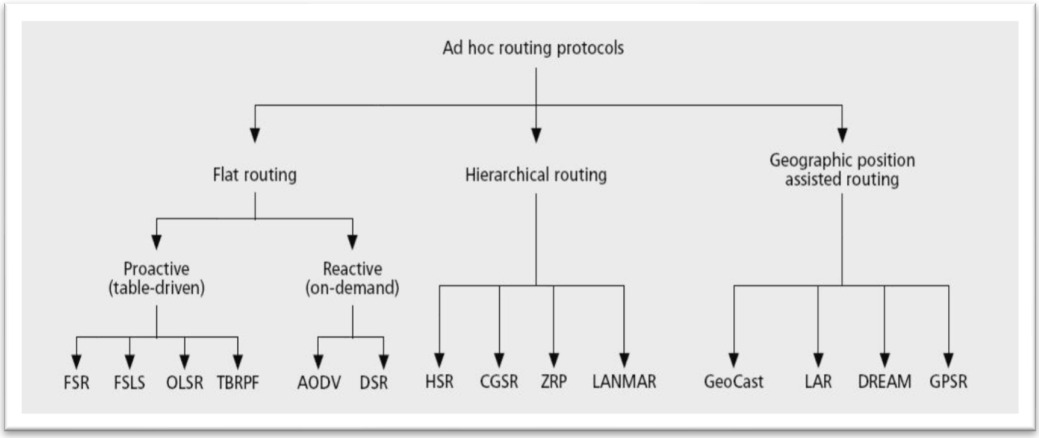

Figure 1.1 Classification of ad-hoc routing protocols [25]

In table driven protocols, each node in the network contain one or more routing tables which are updated regularly, each node sends a broadcast message to the entire network, if there is a change in the network topology [24], example include DSDV, OLSR STAR and GSR. While according to [23] reactive protocols are bandwidth efficient on-demand protocols for MANETs, they comprises of two main functions of route discovery which is responsible for the discovery of new routes and the route maintenance function responsible for the detection of link breakage and repair of an existing route. Examples include DSR, AODV, and TORA.

Security is a challenging issue in MANET because of its characteristics like dynamic varying network topology, imprecise state information, lack of central coordination, hidden node problems, limited resources and insecure transmission medium [18]. MANETs are vulnerable to various security attacks ranging from passive and active attacks to internal and external attacks, such attacks can be black hole, gray hole, cooperative black hole, eavesdropping, sinkhole, jelly fish, spoofing attack and rushing attacks. Hence finding a secured and trustworthy end-to-end connectivity in MANET is a genuine challenge [2].

In the route discovery function of on-demand routing protocols, a malicious node uses the routing protocol to advertises itself as having the shortest and fresh route to the destination node whose packet it want to drop/replay, when the malicious node receive a route request RREQ packet, it then create and send a corresponding fake

route reply RREP where an extremely shortest route is advertised [31]. Once this RREP reaches the source node before any RREP from a legitimate node, then a forged route has been created and the malicious node is capable of dropping all packets passing through it. This kind of attack is called black hole attack while in a situation where more than one malicious node cooperate to form this kind of attack in order to disrupt the routing process and the whole network is referred as cooperative black hole attack [27].

The research work is an attempt, to fill in the gaps found in the reviewed literatures related it, by in-cooperating an RSA encryption algorithm to the cooperative bait detection scheme (also known as Enhanced Approach for detecting single and collaborative attacks in mobile ad-hoc networks) in order to prevent MANETs from cooperative black hole attacks.

2.3 REVIEW OF RELATED LITERATURE

In an attempt to find a better solution to the security challenges in mobile ad hoc network, various researchers have proposed different solutions for various security issues in MANETs. However, most of these techniques and methods need to cost much time and resources in order to avoid, detect and prevent cooperative malicious nodes (cooperative black hole/gray hole), attacks. A number of research for the detection prevention and avoidance of cooperative black hole/grayhole attacks are given below:

An algorithm to prevent the cooperative black hole attacks in mobile ad hoc networks was presented in [15], the algorithm is based on a trust relationship between nodes and hence it cannot tackle grayhole attacks. Besides due to intensive cross-checking, the algorithm takes more time to complete, even if the network is not under attack.it also lack a security scheme that will prevent attacks by legitimate intermediate nodes when they turn to be malicious since the cross checking technique is based on trust relationship. In [9] an approach for detecting collaborative black hole attacks by enhancing the features of ad hoc on-demand distance vector routing protocol AODV was presented, by adding to control packets, a secured reliable route request SRR_REQ and a secured reliable route reply

SRR_REP with a reliability list RL and a threshold value TV as routing entries to the traditional AODV. This scheme is only suitable for 15-45 nodes and the routing overhead increases with increase in MANET's size. In [14] a mechanism for tackling cooperative malicious nodes attacks was presented, the mechanism combine the features of both proactive and reactive defense architecture, it implement a reverse tracing algorithm used to locate malicious nodes. It also uses the onion routing (TOR) protocol which encapsulate data in multiple layers and then send it with security. Though the mechanism send data with security by encapsulating it in to multiple layers, this encapsulated data can be compromised using brute force when it get to the malicious nodes, thus using a better encryption scheme can prevent it from malicious nodes and may address other types of security attacks in MANETs.

A scheme designed to tackle malevolent nodes launching cooperative attacks on MANETs was proposed in [8], it uses CBDS with dynamic source routing as the protocol for route discovery and maintenance, it also combine the advantages of both reactive and proactive defense scheme, the CBDS implement a reverse tracing technique with an additional function of hello message as used in AODV to keep track of source neighbor nodes that help in detecting malicious nodes.. This method prevent the use of reactive defense scheme only as malicious nodes may not be detected at the initial stage of the network, so using reactive defense scheme only to secure mobile ad hoc network skip the detection of malicious node, thus exposing the network to security threat at the initial stage. In [11] a scheme that uses a circular ring of tokens generated to bait selfish and malicious nodes was presented. Once token neighboring nodes are received to simulate bait RREQ to all other nodes with bait tokens, all other nodes including selfish and malicious nodes send to replies corresponding source node. Then backtracking is applied to detect the route path from all the nodes. It lacks a message security scheme to send data with security. In [7] an approach that uses the CBDS to detect wormhole attack using a hop latency was proposed, it address wormhole attack apart from cooperative black/grayhole attacks. Inclusion of a better reactive detection scheme can improve its efficiency at real time by monitoring continuously. In [13] a technique for detecting and preventing cooperative black hole/gray hole attacks in MANETs is presented by embedding the features of DSR in AODV protocol, it consist of three stages, the

baiting stage which attract malicious nodes to send RREP by using adjacent node address as bait destination address, the dubious path detection which detect the suspected route of the malicious node RREP and the confirmation request with the RREP where the destination node request its neighbors to confirm the route given as secured. Using better reactive detection scheme may improve its efficiency, also detection and prevention from other type of security attacks can be done with some modification to this techniques. Thus adding an encryption algorithm to it may increases the versatility to detect and prevent two to three types of attacks.

A mechanism named cooperative bait detection scheme CBDS based on DSR routing protocol for detecting and preventing collaborative black hole and grayhole attacks in MANETs was presented in [1]. It allows the source node to use the address of its neighbor as bait destination address to bait malicious node replies with fake routing information and implement a reverse tracing algorithm to detect them. The scheme can be enhanced by integrating it with a well-known message security scheme to construct a secured routing frame work to prevent MANETs against malicious nodes. In [3] cooperative bait detection scheme that use DSR as routing protocol to detect malicious nodes launching cooperative attacks in MANETs was proposed. It in cooperate the proactive and reactive defense architecture and randomly collaborate with a stochastic adjacent node. The address of an adjacent as bait address to attract malicious nodes to transmit a reply message and detect strange node with reverse tracing technique to prevent and ensure security in MANETs. Though it reduces waste of resource by using both reactive and proactive measures employing message encryption scheme to transmit data with security will be of great advantage to the system. A method for detecting and preventing cooperative black hole attacks in mobile ad hoc networks by thresholding the route reply sequence number was introduced in [16], it is implemented using an ad hoc on demand distance vector AODV routing protocol. The route request and route reply RREQ-RREP messages of the AODV routing protocol are used in real-time, if any detection rule is violated, the black hole attack is said to be detected and the malicious node is isolated and added to the black hole list. A static threshold value T is set, and the AODV RREP sequence number is overlook to see if it is greater than the threshold value, if it is, the node is suspected to be a malicious and is added to the black hole

list, such node will be blocked. The detection of all the remaining nodes is done in this way for the whole network. It also introduce a new control packet that alert all neighbors about the malicious node and has a blacklist nodes as parameter, and the neighboring nodes will know all the malicious nodes and ignore any RREP from the.it. This method can be extended suitably to deal with other types of attacks in mobile ad hoc network. In [12] an enhanced cooperative bait detection scheme for preventing collaborative black hole attacks in mobile ad hoc network was proposed, it embed the features of dynamic source routing, 2ACK protocols and merges the proactive and reactive defense architecture. To ensure secure data transmission a key distribution scheme shuffling algorithm is used, route reply RREP is modified to reserve a field used to record addresses which enables the method to trace malicious node on sending RREP, and the route request RREQ packet is also modified to have a virtual non-existent address as its target address. At the initial stage route discovery is initiated with the source sending RREQ to all nearby nodes, the target address of the RREQ is a fake ID, on receiving the RREQ malicious nodes replies itself as the shortest path to the destination and the suspected path detection uses the RREP received from the malicious node and check the record field, so that source knows which node among the RREP recorded addresses is the malicious node and remove it from the network. To make data transmission secure after detection of cooperative black hole attack, the key distribution center provides key shared between source and destination in order to encrypt data before it is sent to the destination by the source and decrypt it at the destination upon reception. The proposed technique reduces resource wastage and performs well in terms of routing overhead and throughput over DSR and 2ACK, and offer a greater packet delivery ratio. The encryption key may be compromised when the key distribution center transmit a key to one of the node, thus using symmetric encryption to secure data before transmission is sometimes vulnerable.

A technique that use a unique protocol for identifying and removal of cooperative black hole and grayhole nodes in mobile ad hoc networks, with the help of a backbone network of trusted nodes for restricted IP (RIP) addresses was proposed in [10]. The scheme lacks message security scheme, so it can’t tackle eavesdropping attacks

2.4 SUMMARY OF THE LITERATURE REVIEW

Table 2.1 show the summery of the literature reviewed related to the research work.

S/N	Author	Title	Strength	Weakness	Remark
1	Ramaswamy et al. (2016)	Prevention of cooperative Black hole Attacks in Wireless MANETs	Crosschecking technique use for detecting malicious nodes	Takes longer time and the use of trust relationship so can't treat grayhole attacks	Adjusting the approach to minimize its trust relationship to address other attacks (grayhole)
2	S. Abiramy et al. (2016)	Defending Malicious nodes In MANETs Using CBDS with Onion Routing	The use of the Onion routing to encapsulate data in to multiple layers	Encapsulation key is required	
3	Musthafa et al. (2016)	Token Ring Based CBDS for Both Selfish and Malicious Nodes Attack in MANETs	Tokens used in baiting both selfish and blackhole nodes and then the use of the CBDS to detect them.	transmitted data may be known by an eavesdropper	Modifying the scheme to include a public key cryptosystem may improve its security
4	Newlin et al. (2016)	Detection of Wormhole attacks Using CBDS	Use of hope latency to detect and prevent Wormhole attacks	Private information can be known by an attacker.	Better reactive detection scheme may improve its efficiency at real time by monitoring continuously
5	Priya C. et al. (2016)	An Efficient Approach For Detecting Malevolent Nodes in MANETs Using CBDS	Combine the advantages of both reactive and proactive defense scheme	Can't treat wormhole attack	Adding public key cryptosystem may improve the scheme to treat wormhole attacks
6	Anuj	EMAODV:	The use of	It is only suitable	Adjusting the

	et.al (2015)	Technique to Prevent Collaborative Attacks in MANETs	SRR_REQ, SRR_REP, RL and TV to detect and prevent malicious nodes attacks	for small number of nodes and produce high overhead	scheme to cover large number of nodes and also reduce the overhead
9	Hedges and Uvraj et al. (2015)	Enhanced Bait Approach to Defend Against Collaborative Attacks in MANETs	Combine the features of DSR and AODV protocols to prevent packet loss	Treat only collaborative black hole attacks	Modifying the scheme may address more than one type of collaborative attack
10	Chang et al. (2014)	Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach	The use of reverse tracing technique to trace and detect malicious nodes	Lacks message security scheme	In-cooperating the scheme with a message security scheme may improve its performance and the feasibility of addressing other types of attacks
11	Olushola and K. Suresh (2014)	Cooperative Bait Detection Scheme to Avoid the Collaborative Attacks in MANETs	Utilizes both reactive and proactive defense architecture	Transmitted data is sent openly (i.e. no data hidden techniques is employed)	Adjusting the scheme to address other types of attacks
12	HireMath and Anuradha T. (2014)	Detection and Prevention of Collaborative attacks in MANETs	Thresholding the RREP sequence number	Produce high overhead	
13	Vishnu K and J Paul. ()	Detection and Removal of Cooperative Blackhole/Grayhoel Attacks in	Uses backbone network of nodes to assign RIP that aid the detection	Once the backbone nodes are compromised the whole network is in	Introducing message security scheme may improve its performance

		MANETs		danger	

2.5 WORKING MECHANISM OF THE PROPOSE WORK

2.5.1 Dynamic Source Routing (DSR) Protocol

Dynamic source routing is a uni-path routing protocol specifically design for use in multi-hop networks consisting of mobile nodes [20]. DSR forms an on-demand route, no prior configuration and or organization of network is required, since ad hoc network is an infrastructure less network which is manage independently, where nodes cooperate with each other, leave and join the network dynamically, for all these conditions DSR is best suited . In DSR routes are found on-demand so it can work on zero-configuration for sending data from one node to another. In this environment. DSR first uses route discovery process for finding route from source to destination where nodes communicate with each other within communication range and ultimately find route to the destination. Once the route is found route reply is send to the source through the path found.

DSR work on-demand and does not send any periodic message of any kind which increases network overhead. Next important part of DSR is route maintenance , once route are discovered by the source , it will be kept in the cache of the source and the source can send the data in the path saved without initiating route discovery process. If while sending the data an intermediary sending node finds that the link is broken, it generate a route error packet and send to the source, each node between the source and the broken link will be updated about the link failure and if there is a node that has an alternative path will send the data along that path. Otherwise source node can invoke the route discovery process again. Both route discovery and route maintenance are invoked on-demand.

2.5.2 Route Discovery Process in DSR

Let a source node want to send a data to a destination, the source will broadcast a route request RREQ packet, which contain a unique RREQ packet id, destination address, and source address. When a node receives the RREQ packet it will first compare the packet destination address to its own address and:-

a) If node is not the destination node
   - It will check whether it has seen the packet already, if it has it will discard the packet, this will be done by comparing the incoming packet unique RREQ packet _id. Otherwise
   - It will append it's address in the packet and broadcast it again

b) If node is the destination node
   - Node will make a new route reply RREP packet
   - It will copy the route record and RREQ ID found on the RREQ to the RREP packet and also it will append its address in the path field and the node will unicast the packet along the path found.
   - Upon receiving the RREP packet the intermediate node in the path will check the RREP source route and will unicast the packet to the next node in the route. Also when the source node receives the RREP packet it will copy the address in the path field to its address cache and will send the packet in the path found [40].

Whenever a source node want to discover route to a destination, it will broadcast RREQ packet, which is then broadcasted by the subsequent nodes until the destination node receive the RREQ packet as described in the route discovery process. Table 2.2 shows RREQ format in DSR.

Table 2.2 Route Request Format[40]

RREQ	**Source IP**	**UID**	**Destination IP**	**Path**

RREQ: packet type

Source IP: Contain the IP address of the source node

UID: Unique packet ID at the source node

Destination IP: Contain the IP address of the destination node

Path: List of IP addresses separated by comma, in order from the source to the destination.

According to [23] as soon as the destination received a RREQ packet, it originates a RREP message and forward it to the source through the path found. Table 2.3 shows RREP packet format.

Table 2.3 Route Reply Format [40]

RREP	**Source IP**	**UID**	**Destination IP**	**Path**
RREP: Packet type				
Source IP: Contain IP address of the original destination node				
UID: Unique packet ID at the original destination node				
Destination IP: contain IP address of the original source node				
Path: List of IP addresses separated by comma, in order from the original source to the original destination.				

Data packet is generated by the source node after it has get the path from the RREP packet, or it had originally in its route cache, the packet contain the message which is intended for the destination . Table 2.4 shows the data packet format in DSR.

Table 2.4 Data Packet Format [40]

DATA	**Source IP**	**UID**	**Destination**	**Message**
DATA: packet type				
UID: Unique packet ID at the original Source node.				
Message: Is the message to be sent as a string.				

2.5.2.1 Route Caching in DSR

In route discovery process, when source receive RREP from the destination, it save the route from the source to the destination in its route cache which it can use immediately and also in future to send data to node which is along the path found [20]. Also when each node sends RREQ packet it also find path from source to itself and it store the path in its cache which it can use when the node need same path to send data in future. The same thing can be done in RREP packet sending [40].

2.5.2.2 Route Maintenance in DSR

After finding the route, source will send data to the destination along the path it has known through route discovery process. The source have to send data for the destination through the intermediate nodes and each time a node send data to its neighbor it will wait for the acknowledgement for the successful delivery of data, suppose if a node does not receive an acknowledgment from its near node that it send data to, it will wait for some predefined amount of time for the acknowledgement to come and if it does not receive the acknowledgement, it will send route error RERR packet to all the nodes in the path from which it receive the packet. All nodes which receive the RERR packet will update their corresponding route cache for that path and remove the path that is broken. If any node of the receiving RERR has alternative path in it route cache it will try to send the data again in that path. If it succeeds the source will update the new path in its cache. Otherwise source node has to initiate route discovery process again [20].

According to [20] RRER packet is generated by the node that found a broken link or doesn't receive an acknowledgement from its neighbor, it simply forward it to the source node informing it about the link failure. Table 2.5 shows RRER packet format in DSR.

Table 2.5 Rout Error Packet Format [40]

RERR	**Source IP**	**UID**	**Destination IP**	**Path**

RERR: packet type

Source IP: contain IP address of the node which initiate the RERR packet

UID: Unique packet ID at the node sending the RERR

Destination IP: contain the IP address of the original source node

Path: contain list of the IP addresses separated by comma, in the order from the original source to the node where RERR packet was initiated

2.5.3 COOPERATIVE BAIT DETECTION SCHEME

In [1] CBDS is a scheme used in to detect cooperative black hole nodes launching single or cooperative attacks in mobile ad hoc networks. The scheme allows source

node to stochastically chose one of its one-hop neighbor nodes address as destination node address to send a bait RREQ packet in order to bait malicious node send fake RREP packet to the source node, on receiving this fake RREP packet, source node will invoke a reverse tracing algorithm that uses the information on the RREP path field to trace and check all nodes present along the path of the RREP packet to identify and detect malicious node and prevent it from participating in the network, normal route discovery process is initiated by the dynamic source routing protocol after the detection mechanism detection of the malicious node, before sending data to the source node this research work uses RSA encryption algorithm to encrypt the data at the source node before sending it to the destination node.

2.5.4 RSA ENCRYPTION SCHEME

Computer cryptography is the study of computer information encryption, decryption and transformation of scientific, inter-disciplinary mathematics and computer [29]. Cryptography is one of the methods used to ensure confidentiality and integrity of information in a communication system. It is the science and art of transforming messages to make them secure and immune to attack [33], cryptography is broadly described as the art and science of scrambling data to prevent unauthorized access over unsecured transmission channel, it works on the principal of mathematics that generate different algorithms known as cryptographic algorithms, which use mathematical function for encryption and decryption to generate cipher text and plain text.

The RSA cryptographic algorithm, is one of the first public key cryptosystems introduced in 1976 [29], by Ron-Rivest, Adi-Shamir and Len-Adleman at MIT and is named after them as the RSA scheme. It is one of the best known public key cryptosystem [33] for key exchange or encryption of blocks of data that uses a pair of related keys, one for encryption and the other for decryption. One key which is called the private key is kept secret and the other one known as public key is disclosed. Message or data packet is encrypted with public key and can only be decrypted by using the private key, so the encrypted data cannot be decrypted by anyone who knows the public key and a secure communication is possible.

The proposed work use the bait phase to bait malicious nodes, then use the reverse tracing technique to identify the malicious nodes and add them to the malicious nodes list (black hole list), broadcast an alarm packet to the nodes in the network to halt all communications with theses nodes and then use the DSR routing algorithm to find route from the source to destination and then use the public key of the destination node to encrypt the message and send the encrypted message to the destination node through the route found during the route discovery process and on reaching the destination, the destination use its private key to decrypt the message received and view its content. This is the typical operation of the proposed system.

2.6 UNIQUENESS OF THE RESEARCH WORK

This section discuss about the research gap found in the reviewed literatures related to the research work.

2.6.1 EXISTING SYSTEM

The existing mechanisms presented in the literature surveyed, detects malicious nodes that attempts to launch grayhole /collaborative black hole attacks. In the schemes, the address of an adjacent node is used as bait destination address to bait malicious nodes to send RREP message and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that are communicating with any node in that list. Though some of the techniques discussed in the literature survey use some form of encryption schemes in their operation such as [12], [9], and [13] but the security mechanisms used by such techniques are based on trust relationships or weak. Thus the encryption technique imposed is weak and can easily be discovered. Unlike other malicious node detection scheme where the merit of the CBDS lies in the fact that it integrate the proactive and reactive defense architecture to achieve its goals.

2.6.2 DISADVANTAGE OF EXISTING SYSTEM

Lack strong data encryption technique that hide data packet content from malicious nodes and do not need secured path for key exchange in order for the destination node to be able to decrypt the encrypted data packet by the source node.
In this regard the effectiveness of these techniques become weak when malicious nodes are aware of the content of the data packet, thus it can be modified or intercepted which may result to more devastating damages to the entire network**.** Also the use of the threshold value to detect the presence of malicious nodes after the initial detection help increase the routing overhead due to their frequent use of routing control packets in the network.

2.6.3 PROPOSED SYSTEM

In the proposed work (system) a public key encryption technique that is RSA encryption algorithm is introduced to the cooperative detection scheme, it encrypt data packet before it is transmitted from the source to the destination after the CBDS detect and remove malicious nodes at the initial stage. Thus data is sent with security since the RSA encryption algorithm is very difficult to be attacked by any of the malicious nodes.

2.6.4 ADVANTAGE OF THE PROPOSED SYSTEM

The research work includes a well-known data encryption technique (Public key cryptosystem) that hide the data packet content from the malicious node, which does not need key distribution center to distribute the encryption key across the network (between source and destination), since the public key cryptosystem employ the use of pair of keys public key for encryption and a private key for decryption. Apart from detecting single and cooperative attack in mobile ad hoc network, the proposed work can also be used to treat eavesdropping and sinkhole attacks which normally launch attacks to the network by monitoring and changing the data packet content. The elimination of the use of threshold value use to recall the reverse tracing

operation by the proposed work help minimized the use of routing control packets which cause increase in overhead.

CHAPTER 3

METHODOLOGY

3.1 PREAMBLE

This chapter consists of the research methodology, simulator and the simulation environment used in the research work, performance metrics and a detailed description of the proposed enhanced approach for detecting and preventing single and collaborative attacks in mobile ad hoc networks.

3.2 METHODOLOGY

An adequate and effective method of gathering the required data and information was used to achieve the in-cooperation of the RSA cryptosystem to the CBDS in order to identify and prevent single and collaborative malicious nodes attacks and also to find a secure routing path in MANETs. In order to achieve these objectives, documentaries and Internet are the main information providing sources used.

Documentary research is one of the method used for data gathering, it includes the logical and systematic examination of documents such as thesis, journals, and eBooks. On the other hand the use of electronic media such as the Internet is also employed by the research work, all for the purpose of obtaining relevant materials or important information for the study to achieve the research work's objectives.

3.2.1 METHODS AND PROCEDURES

The research work used some methods and procedures in order to achieve its aim and objectives, these methods and procedures are discussed below

3.2.1.1 Neighbor Selection Algorithm

In order to use neighbor node as a bait node, the source node need to know all its neighbors in the whole network and randomly select one among them to use it as its baiting node. The neighbor node selection algorithm calculate the distance between each node in the network and compare it with the transmission range, if the distance is less than the transmission range then that node will be selected as a neighbor node and will be added to neighbor node list else it will not be selected as a neighbor. Hence the neighbor selection algorithm allow all nodes in the network to know and list their neighbors at the initial stage of the network.

3.2.1.2 Bait Setup

The objective of the bait setup stage is to tempt a malicious node to send a RREP message when a bait RREQ message is sent to it, it used to advertise itself as having the shortest and optimal route to the destination node [1]. To achieve this, a bait RREQ generated, here the source node randomly select an adjacent node (one of its neighbor nodes) within its one-hop neighborhood node and cooperate with this node by taking its address as the destination address of the bait RREQ [4]. Since each baiting is done randomly and the adjacent node would be changed if the source node moved therefore, the bait will not remain unchanged. The bait procedure is always activated whenever the bait RREQ is sent earlier for seeking the initial path.

To check the presence or absent of malicious nodes in the bait procedure we check

I. If the bait node had not launch a black hole attack, then after the source node had sent out the RREQ, there would be other nodes RREP in addition to that of the bait node [18], this indicate that malicious node exist in the RREPs, therefore reverse tracing operation is initiated to detect malicious nodes along this routes.
II. If only the bait node had sent the RREP, it means there is no other malicious node in the network and normal route discovery process is initiated by the routing protocol [1].

III. If the bait node is the malicious node of the black hole attack, then after the source node had sent the bait RREQ, other nodes in addition to the bait node will have sent the RREP, which indicate the existence of malicious nodes thus the reverse tracing operation is activated to detect the malicious nodes

IV. If the bait node deliberately refuse to give RREP to the bait RREQ it will directly be listed on the black hole list by the source node

V. If only the bait node had sent the RREP, it means that there is no other malicious node in the network except the route that the bait node had provided.

3.2.1.3 Reverse Tracing Technique

The reverse tracing technique is utilized to identify the behavior of malicious nodes through the route reply to the bait RREQ message. If malicious node had received the bait RREQ, it will reply with a fake RREP. Then the reverse tracing technique will be initiated for nodes receiving the route reply RREP, with the goal to deduce the dubious path information and the temporarily trusted nodes [2], [4], [5], [6].

Initially an address P-list and a route information K_k –list is created

$$P = \{n1 \dots nk \dots n_m \dots nr\}[1] \tag{3.1}$$

$$K_k = \{n1 \dots nk\}\ [1] \tag{3.2}$$

So when a malicious node n_m, replies with a forged RREP, this address P-list is recorded in the RREP. If node nk receives the RREP, it will separate the P-list by the destination address n_1 of the RREP in the IP field and get the address list $K_k = \{n1 \dots nk\}$, where K_k-list represent the route information from the source node n_1 to destination nk. After that node nk determines the difference between the address P-list and the K_k-list.

$$K_k' = P_{List} - K_k\_List\ [17]$$

$$K_k' = \{nk + 1 \dots n_m \dots nr\}\ [17] \tag{3.3}$$

K'_k-list = is now stored in the RREPs and then they are reverted to the source node.

The source node receives the RREP, and the K'_k-list of the nodes which receives the RREP, in order to ensure that the list does not come from a malicious node. After receiving the RREP, node nk recheck the RREP by comparing

1. The source address in the IP fields of the RREP
2. The next hop of nk in the $P = \{n1 \dots nk \dots n_m \dots nr\}$ and
3. One hop of nk

If 1 is not the same with 2 and 3, then the received K'_k performs a forward back, otherwise, nk have to just forward back K'_k that was produced by it.

The dubious path information S is given by

$$S = K'_1 \cap K'_1 \cap \dots K'_n \text{ [18]} \quad (3.4)$$

The trusted set T is given by

$$T = P - S \text{ [17]} \quad (3.5)$$

To confirm that the malicious node is in set S, the source node would sent the test packets to this route and would send a recheck packet to the second towards the last node in set T. this requires that the node had entered a promiscuous mode in order to listen to which node the last node in T send the packet to and fed the result back to the source node [1]. The source node will then store the malicious node in the black hole nodes list and then broadcast an alarm packets throughout the network to inform all nodes to terminate their operations with this nodes. [1], [17].

3.2.1.4 The RSA Encryption Algorithm

This system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adlemman and hence, it is termed as RSA cryptosystem. The RSA cryptographic technique is introduced to the existing SCBDA to make sure that data packets are hidden from illegitimate nodes and are sent with security, so that only legitimate destination node is authorize to have access to the data packets, unlike in the SCBDA where a malicious node can compromised data transmission when the key

used for encryption is known by the attacker. Each node that desire to participate in the network using the RSA encryption needs to generate a pair of keys, namely public key, and private key. The processes followed in the RSA key pair generation are described below:

Generate the RSA MODULUS (n)

Select two large prime numbers, p and q.

Calculate n

$$n = p*q \tag{3.6}$$

Find Derived Number (e)

Compute the totient function of n.

$$\emptyset(n) = \emptyset(p) * \emptyset(q)$$
$$= (p-1) * (q-1) \text{ [36]} \tag{3.7}$$

Select an integer e, which must be greater than 1 and less than $\emptyset(n)$ that is to say $1<e<\emptyset(n)$ [36]

There must be no common factor for e and $\emptyset(n)$ except for one, in other words the two numbers e and $\emptyset(n)$ are co-prime.

Form Public key

The pair of numbers (n, e) form the RSA public key and is made public.

Generate Private Key

Private Key d is calculated from p, q, and e. for a given n and e there is a unique number d. number d is the inverse of e modulo $\emptyset(n)$ such that when multiplied by e, it is equal to I modulo$\emptyset(n)$.

This relationship is written mathematically as follows

$ed = 1 (\text{mod} \emptyset(n))$ [36] (3.8)

Encryption and Decryption in RSA

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy, RSA doesn't operate directly on strings of bits as in the case of symmetric key encryption. It operates on numbers

modulo n. hence it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

Suppose the source node wish to send some text to a destination node whose public key is (n, e), the source then represents the plaintext as a series of numbers less than n. To encrypt the first plaintext P, which is a number modulo n. The encryption process is a mathematical step as

$C = P^e \bmod n$ [29] (3.9)

In other words, the cipher text C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.

RSA Decryption

The decryption process for RSA is also very straight forward. Suppose that the receiver of public key (n, e) has received the cipher text C. The destination raises C to the power of its private key d. The result modulo n will be the plaintext P.

$P = C^d \bmod n$ [29] (3.10)

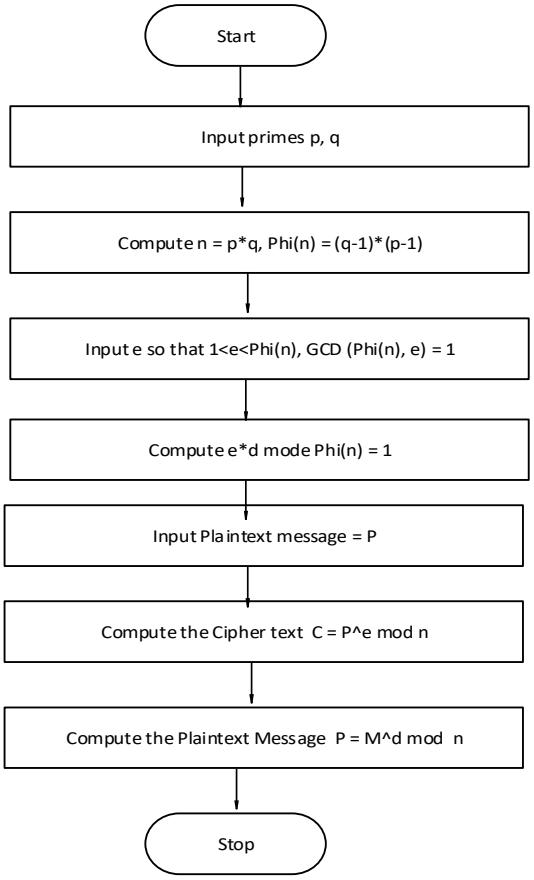

Figure 3.1 Basic RSA algorithm operation (adapted from [29])

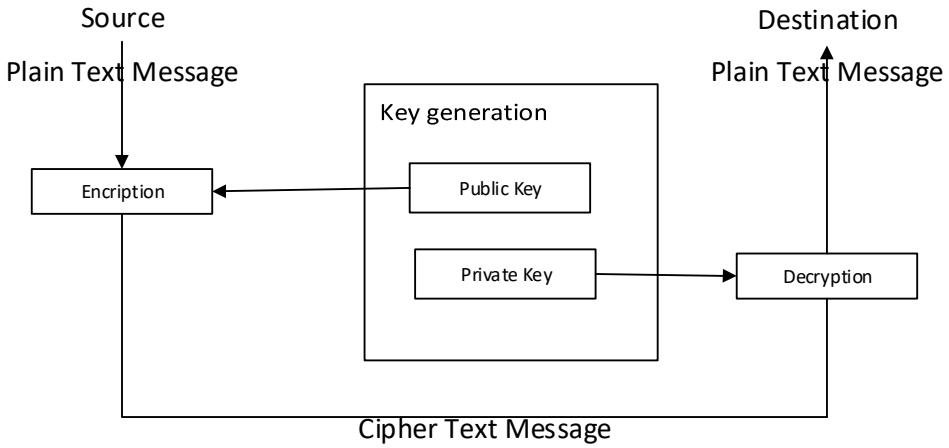

Figure 3.2 The RSA algorithm concept design

3.2.2 SIMULATOR AND TOOLS

Though, there are different kind of network simulators used to simulate wired and wireless networks, this research consider using Network Simulator (Version 2), widely known as NS2, which is simply an event driven simulator tool that has proved useful in studying dynamic nature of communication networks [38]. Simulations of wired as well as wireless network functions and protocols (e.g. routing algorithms TCP, UDP) can be done using NS2, it consist of two simulation tools.

The Network Animator (NAM) which is used to visualized the simulations, NS2 fully simulates a layered network for the physical radio transmission channel to high-level applications, it was originally developed by the University of California at Berkeley and VINT project [38], the simulator was recently extended to provide simulation support for ad hoc networks by Carnage Mellon University (CMU Monarch project homepage 1999) [39].

NS2 consist of two languages C++ and object oriented Tool Command Language (OTCL), while the C++ defines the internal mechanism (i.e. the backend) of the simulator objects, the OTCL sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e. the frontend) [38]. After the simulation, NS2 outputs either text-based or animation-based simulation results, to interpret these results graphically and interactively, tools such as NAM and Xgraph are used.

The result of the simulation is an output file that can be used to do data processing (calculate delay, throughput, routing overhead packet delivery ratio, etc.) and to visualize the simulation with a program called Network Animato (NAM). NAM is a very good visualization tool that visualizes the packets as they propagate through the network. Figure 3.3 shows an overview simulation in NS2.

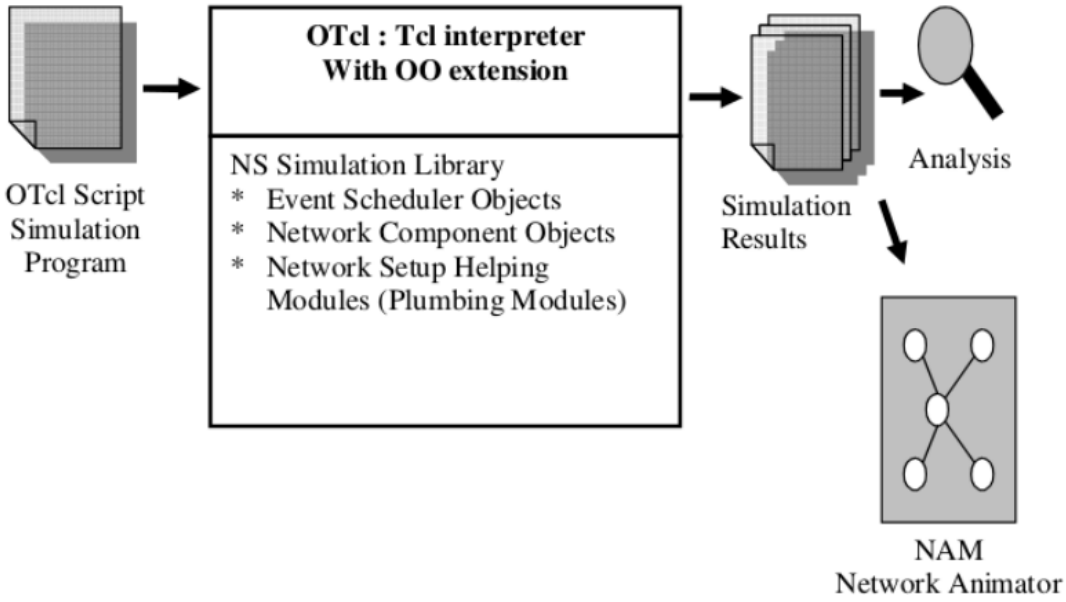

Figure 3.3 structure of NS2 [38]

NAM is a tcl/tk based animation tool for viewing simulation traces and real world packets trace data. The first step to use NAM is to produce the trace file, the trace file should contain topology information example nodes link as well as packet traces, and usually the trace file is generated by NS2. During NS2 simulation, the user produce topology configuration, layout information and packet traces using tracing events [38]. When the trace file is generated, it is ready to be animated by NAM. Upon startup, NAM will read the trace file, create topology pop up a window, do layout if necessary and then pause at the time of the first packet in the trace file through its interface. NAM provide controls over many aspects of animation. Figure 3.4 shows the main window of NAM.

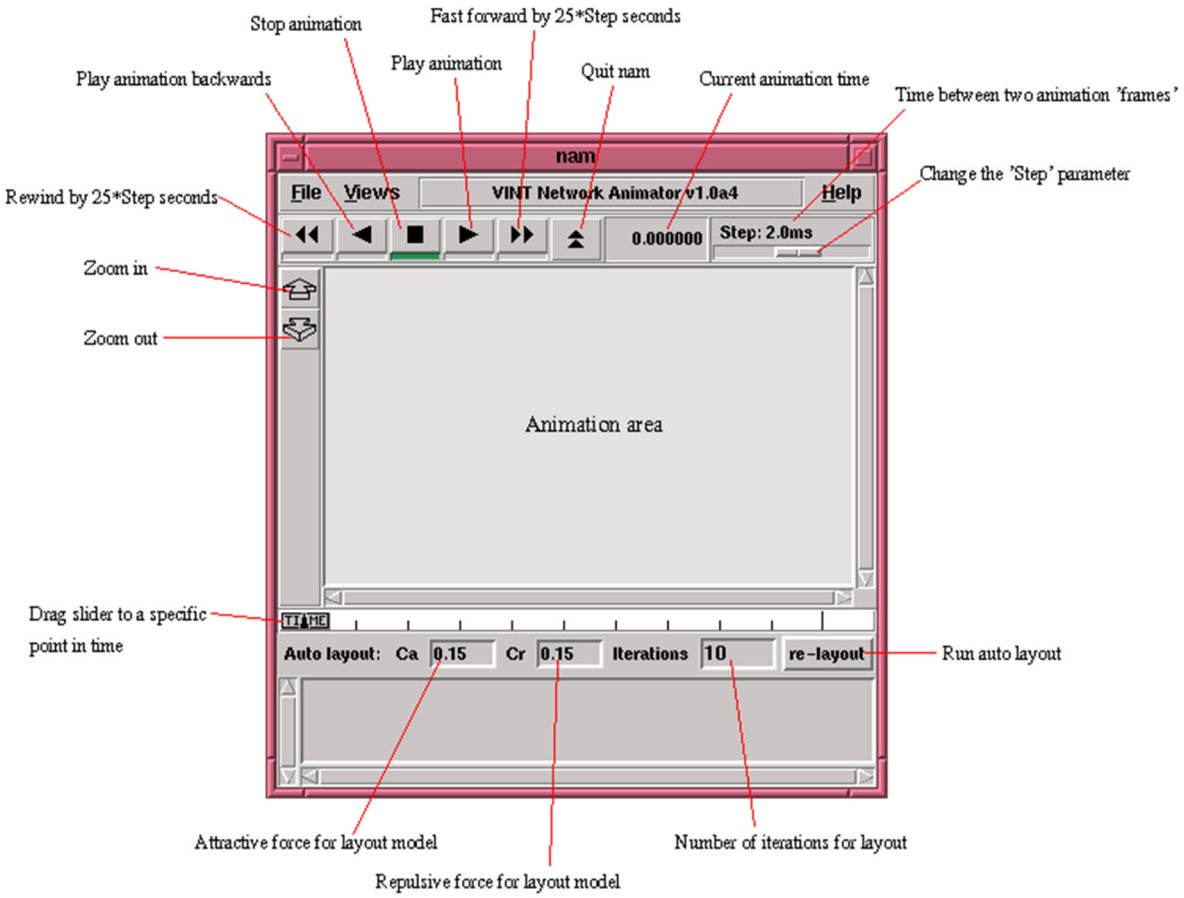

Figure 3.4 Network Animator [39]

Another part of ns-allinone package is "Xgraph" a plotting program which can be used to create graphic representations of the simulation results. Xgraph is on X-Windows application that includes interactive plotting, animation and derivatives portability and bugs fixes. So to plot the characteristics of NS2 parameter like throughput, end to end delay, packets delivery ratio we use the Xgraph. The Xgraph program draw a graph on X-display given data read from either data files or standard inputs. It annotates the graph with a title, axis labels, grid lines, or tic marks, grid labels and a legend [39].

3.2.3 SIMULATION ENVIRONMENT

A detailed simulation model was used based on network simulator version 2 (NS2) specifically ns-allinone-2.28 package which includes the Xgraph program for plotting graphs of the simulation results trace files for analysis and Network Animator NAM program to visualize the simulation result nam trace file to see how packets are transmitted from the source to destination nodes as it happen in real life scenario. In the research work the network simulator was installed and configured on windows XP using the Cygwin software that consist of libraries that implement the POSIX system call API in terms of win32 system call, a GNU development tool chain, including GCC and GDB to allow running of large number of applications programs equivalent to those on Unix-systems, thus many Unix GNU, BSD, and LINUX programs and packages have been ported to this software including x-windows system k-desktop environment 3, Apache and TEX. In short the Cygwin software allow Microsoft windows system to emulate UNIX and Linux servers [32]. Therefore, the reason behind using Cygwin software here is to provide a Unix-like and feel environment to the network simulator since it is developed based on UNIX environment.

The simulator also model a complete multi-hop (MANETs) wireless networks with complete physical, data link and Mac layer model. In a note shell the simulation environment consist of the following

I. Network simulator version 2.28
II. Network Animator
III. Xgraph
IV. Cygwin software and
V. Windows XP.

3.2.4 SIMULATION AND EXPERIMENT SETUP

The network in the simulation model consist of 35 nodes in the network of 700m by 700m area [1]. The network devices move at random, with a chosen speed between 0 to 20 m/s with zero pause time. Traffic Application patterns and Agent consist of

CBR/UDP connections between randomly chosen source-destination pairs. Each node in the network start immediately without a warm up period and continue at the simulation time of 40s. Data packets are to be specified by the size of the data that the user want to send from the source to the destination nodes with an interface queue of 50-packets CMUPrioqueue, and random way point mobility is used to model nodes movement.

Random way point mobility was used to model nodes movement with dynamic source routing protocol as the routing protocol for route discovery and maintenance processes. Other simulation, experiment setup and nodes configuration parameters as used in the simulation model includes neighbor node selection, bait setup, reverse tracing technique and the rsa public key encryption as explained in section 3.2.1, Omni-Antenna was used as the antenna model, TwoRayGround radio propagation model wireless physical interface and mac 802.11 mac layer model were employed for the node configuration. Table 3.1 shows the simulation parameter

Table 3.1 Simulation parameters adopted from [1]

Parameters	Values
Number of nodes	50
Area	700m by 700m
MAC	MAC IEEE 802.11
Application traffic	CBR
Radio Range	250m
Channel data Rate	11mbps
Pause time	0s
Maximum speed	20m/s
Malicious nodes	5
Simulation Time	20s

3.2.5 DATA COLLECTION AND ANALYSIS

The research work used network simulator version 2 (NS2) to model the network, it come with a very powerful data collection and analysis tools. Hence the aspect of data collection and analysis used in the research work are discussed below:

3.2.5.1 Data collection

Ns2 provides a build-in support for collecting /recording simulation results throughout the simulation time via trace files. The output of the simulation results are recorded in two separate files from the start of the simulation to the time when it will stop, these files are created in the tcl simulation script file, one of the simulation trace file which is the NAM trace file served as an input file to the network animator program to visualize the network animation through the name program the NAM trace file is executed. The animation shows a detailed network progress events, packet transmission and route discovery process. The other simulation result trace file serve as an input file to the Xgraph program that plot graphs for analysis and performance evaluation of the network. Thus the research work achieved data collection through the recorded simulation result recorded trace files.

3.2.5.2 Result analysis

The research work simulation software (NS2) provides an analysis and visualization tool, for analysis and visualization of the simulation results. The analysis and visualization programs take in the recorded trace files of the simulation results as inputs to visualize and analyses the performance of the network in terms of the performance evaluation parameters. The visualization tool also known as Network Animator (NAM) takes in and reads the data in the nam trace file that is containing the progression of the packets throughout the network, packet transmission event and draw the network events graphically. The analysis tool also known as the Xgraph takes in the simulation result trace files recorded, which is manipulated using the awk language to get the appropriate datasets for each of the performance evaluation parameters as an input to draw graph on x-display and annotate the graph with title,

axis label, grid lines, or tick marks and a legend. It also provide options to control the appearance of most components of the graph.

To create an analysis and visualization files in the network simulation model, inputs are created by setting the file handler of the file created and opened for writing, after which datasets related are recorded which consist of related inputs to be used for the analysis and visualization tools. To create an analysis input trace file, we have to set handler to the created trace file and open it for writing in the tcl simulation script to record the network activity. This is the NS main trace file in which the data to plot the graph is extracted from, the sample codes below show how trace file is created in tcl script file.

Set tracfile [open out.tr w]

$ns trace-all $tracefile

Where the trace file is the file handler, out is the file name .tr is the file extension specifying the file format and w indicate that the file is writable that is data will be written to the file and the second line tells the network simulator to trace all network activities and write it to the out.tr file.

The other trace files used in the research work are extracted from the ns main trace file to enable it differentiate the plotting of different performance evaluation parameters. The NAM trace file is also created the same way as the analysis trace file except that the NAM trace file have different file handle and extension and is read by the network animator as an input to produce the network animation. The below tcl script codes show how the nam trace file is created

"Set namtrace [open out.nam w]

$ns namtrace-all $namtrace

$ns namtrace-all-wireless $namtrace $Val(x) $Val(y)"

3.2.6 PERFRMANCE METRICS

Though there are different performance metrics for evaluating the performance of the proposed secured cooperative bait detection scheme, the research work decide to choses packet delivery ratio, throughput, end-to-end delay, and routing overhead as its performance metrics.

a. Packet delivery ratio

Packet delivery ratio is defined as the ratio of the number of data packets received by the destination to the number of packets sent by the source. Mathematically, it can be defined as:

$PDR = pktd \div pkts$ (Adapted from [1]) (3.11)

Where $pktd$ the sum of the data packets is received by the destination and $pkts$ is the sum of the data packets sent by the source node.

b. Routing overhead

Routing overhead represent the ratio of the routing related control packets transmission to the amount of data transmissions. Mathematically it is represented as:

$RO = cpk \div pkt$ (Adapted from [1]) (3.12)

Where cpk is the sum of the number of control packets transmitted in the application traffic and pkt is the sum of the number of data packets transmitted in the application traffic and the routing overhead is denoted by RO.

c. Throughput

Throughput is defined as the total amount of data ($pktd$) that the destination receives from the source node divided by the time (time) it takes for the destination to get the final packet. The throughput denoted by T, is obtained mathematically as

T = $pktd \div$ time (3.13)

d. End to end delay

The average end to end delay is delay is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is d and the number of packets received by the destination node $pktd$. Therefore, the average end to end delay denoted by E, is mathematically obtained as:

E = d $\div pktd$ (3.14)

3.2.7 WHY NS2

The choice of NS2 simulator as the simulation tool for the simulation of the of the proposed secured cooperating bait detection scheme (SCBDS) was made necessary for the research work after looking at some of its advantages as given below:

i. It provides a range of features and it has an open source code that can be modified and extended.
ii. It is clear, well-defined documented and hierarchically nested classes or modules, which are available in source codes in the NS2 software directory, so one can extend them to meet his/her requirements
iii. It provides a powerful analysis tool such as the Xgraph program which plots the graph for the performance evaluation which make analysis easier than using other simulators
iv. It also provide a powerful animation tool which is a tcl/tk based animation tool that is used to visualize the ns simulations and real world packet trace data.

3.3 AN ENHANCED APPROACH FOR DETECTING AND PREVENTING SINGLE AND COLLABORATIVE ATTACKS IN MANETs (CBDS+RSA)

An enhanced approach for detecting and preventing single and collaborative attacks in MANETs proposed by the research work, in-cooperate an asymmetric encryption scheme specifically RSA public key encryption scheme to the existing cooperative bait detection scheme.

The proposed work achieve its aim by selecting source and destination nodes, then the source node use the neighbor node selection algorithm and the bait setup phase as discussed in section 3.2.1 to randomly select one of its neighbor node to use it ID as the bait destination ID to lure malicious nodes send fake RREP, these malicious nodes are therefore detected using a reverse tracing technique discussed in section 3.2.1, there by adding them to the black hole/ malicious nodes list and alert the nodes

in the network to stop communicating with these nodes. After the initial malicious node detection the DSR routing protocol is call to discover route to the destination.

To avoid packet interception, unauthorized read and write of the transmitted data and to ensure that it is sent with security to the destination node through the discovered route, the RSA encryption technique is used to encode the transmitted data, the advantage of using RSA over single key encryption is that, the encryption key (which is the public key (e, n)) is distributed to any node in the network, the private key is kept secret [35], so that only the recipient can read the encrypted message. The research work assumed that each and every node in the network has its private and public key for encryption and decryption, and each node has published its private key to the public.

As discussed in section 3.2.2 the RSA encryption technique has three subsystems which are

a. Key generation subsystem which assumed in the research work
b. Encryption subsystem and the
c. Decryption subsystem.

The RSA generate the cypher text (C) by taking each block of the plain text (P) and computing $C = P^e \bmod n$. Similarly the Plain text (P) is generated by taking each block of the cypher text (C) and computing $P = C^d \bmod n$.

3.4 DATA FORWARDING IN THE PROPOSED CBDS WITH THE RSA

3.4.1 Route Discovery Process

This is a process for finding route from the source to the destination, as discussed in section 2.4.1.1 whenever the source needs route to a destination, this process is initiated from the source which will give the destination IP address in the RREQ command over the prompt. The RREQ packet is flooded throughout the network and nodes that receive several copies of the same RREQ packet, consider only the first copy and form a reverse path to the source from the destination and discard the other

copies of the same RREQ it received. Figure 3.5 shows the data flow diagram of the route discovery process.

3.4.2 Route Caching

In the route discovery process when the source receives the RREP packet from the destination, it saves the path from the destination to itself in its route cache which it can use immediately, or in future to send data packets to nodes which are in the path between the source and the destination. Also when each node receive and send the RREQ packet, it also finds a path from the source to itself and it store the path to send data packets in future. In a situation where a node receives multiple packets for the same destination from two different source it can save both path in its cache and the information about this routes can be used when one of the path link is broken or damaged. Thus route caching serve as alternative and also optimizes the route discovery process, let's consider a scenario where a RREQ for some destination is received by some intermediate node and that node has the route from itself to the destination, instead of broadcasting the RREQ packet, this node can easily append the address from its cache to the RREQ packet and send the RREP packet to the source node.

3.4.3 Data Transmission

When the source wants send data to the destination, it first checks if a path to the destination is available in its cache, if route is available it start sending the data through that route, else it initiate the route discovery process to find the route from the destination to itself. In this case when the route to the destination is found the source uses the public key of the destination node and encrypt the data before transmitting it to the destination. When an intermediate node receives the encrypted data it follows the route list in the route list IP field in the data packet and forward it to the appropriate next hop node in the route list and wait for an UACK, this process continues until the destination is reached which will now consume the data packet and send a UACK confirming to the source node that it has received the data packets.

3.4.4 Route Maintenance

The route maintenance here is done after finding the route, the source will send the data to the destination along the path it has known by route discovery. For a successful delivery of data packet an immediate intermediary node wait for acknowledgement from its next hop node for some predefine amount of time for the UACK to come and if it didn't, then that node will generate and send RERR packets to all nodes in the path from which it received the packet, informing them that it cannot reaches the destination or the link is damaged or broken. This is done to maintain link breakage and link failures as discussed in section 2.4.1.2 of chapter two.

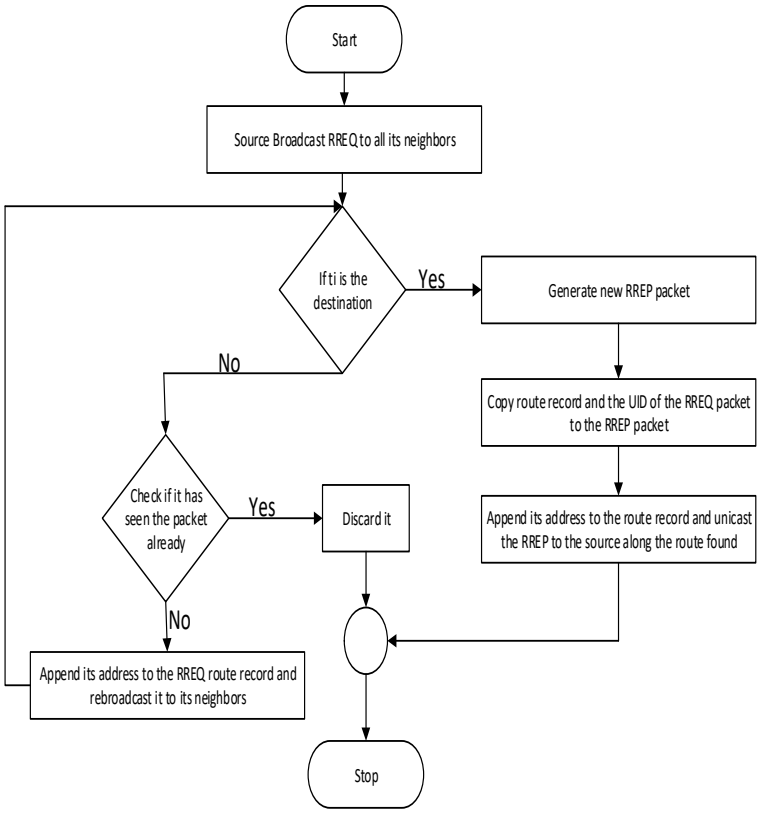

Figure3.5Route discovery process flow chart diagram [7]

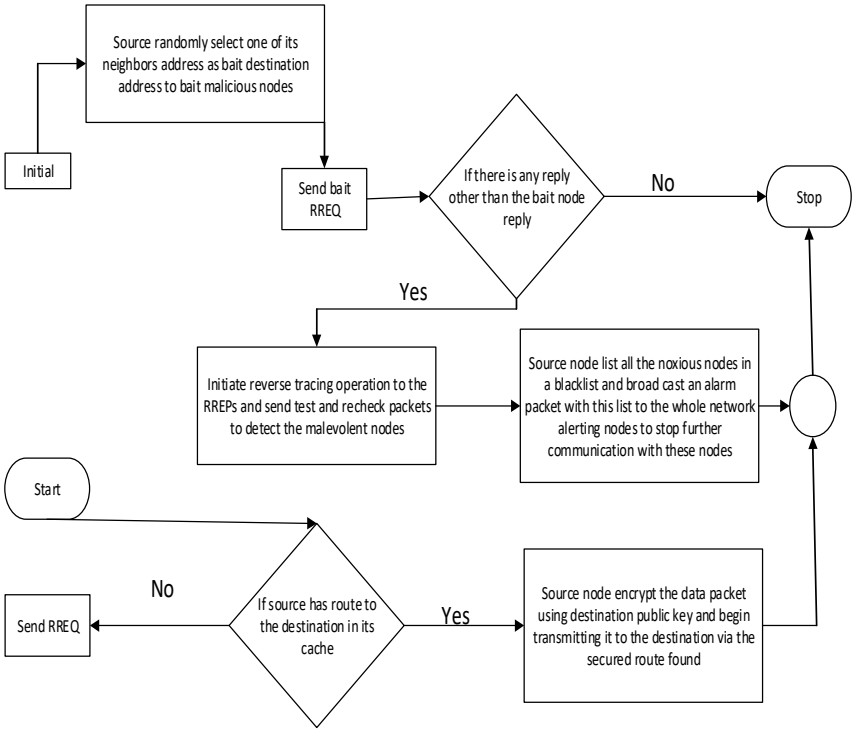

Figure 3.6 Basic operation of the proposed work adapted from [1]

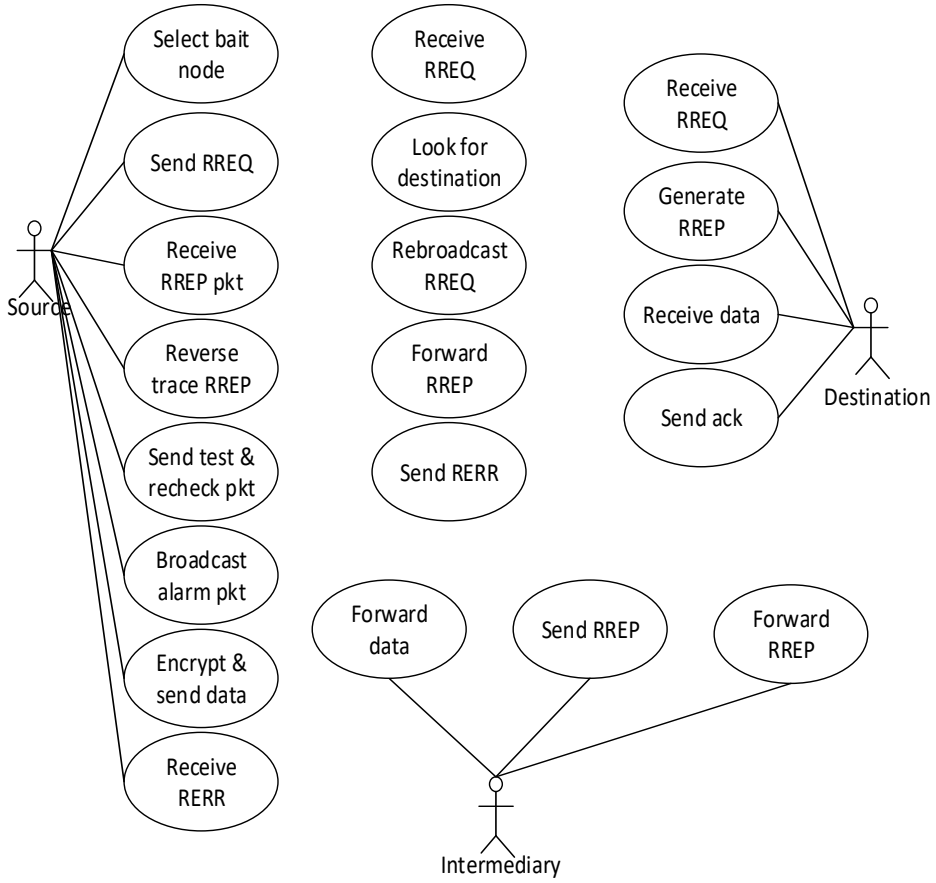

Figure 3.7 Use case diagram of the proposed CBDS with RSA

CHAPTER 4

RESULTS AND DISCUSSION

4.1 PREAMBLE

This chapter consist of evaluation of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs and concludes with the discussion of the simulation results.

4.2 PERFORMANCE EVALUATION

The performance of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs such as cooperative black hole, grayhole eavesdropping and sinkhole attacks, was carried out using NS2 network simulator tool. The main objective here is to evaluate the effectiveness of the proposed scheme relative to the cooperative bait detection scheme CBDS proposed in [1], in the presence of malicious nodes. Other objectives includes reliability of data transmission in terms of security, understanding the advantage that the proposed work has over the existing system in terms of secured data transmission.

The performance of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs or cooperative bait detection scheme with the RSA algorithm (CBDS+RSA) was evaluated in comparison with the CBDS proposed in [1]. Figure 4.1 show the main simulation frame from which the simulation is run.

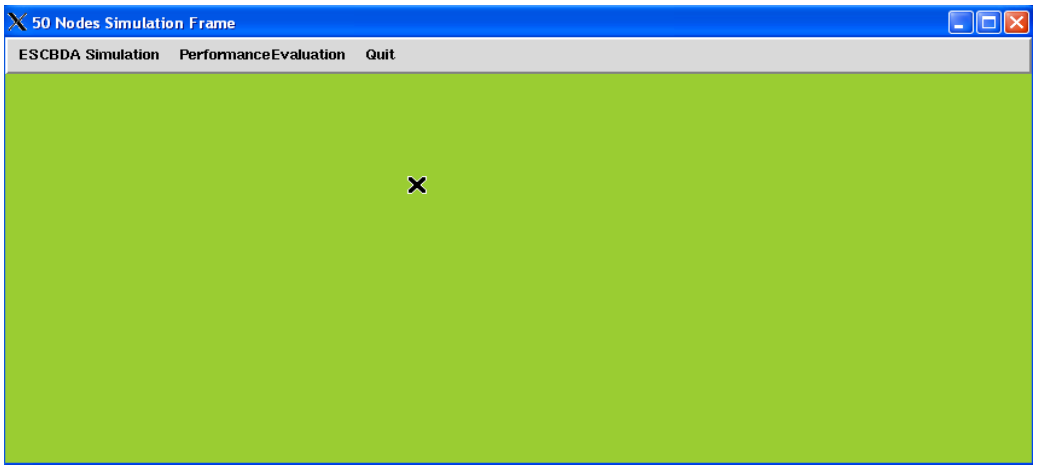

Figure 4.1 the main Simulation frame

This frame has two menus Simulation from which to run the simulation or to run the existing Network animation after the simulation, and the Quit menu from which to quit the simulation scenarios.

To run the simulation we go to Simulation menu in the simulation frame menu bar shown in figure 4.2, click on the Run Simulation. This will start the simulation by loading both simple and complex modules that defines the network architecture, followed by linking all the tcl and the C++ files that implement the behavior of the loaded modules. The simulation parameters that controls the number of devices the network should have, the height and width of the simulation area, the total simulation time, the type of the data transmission channel to be used, the rate at which the data flows, the mobility, the type to be used by the network devices, the speed at which they are to move, and the types of security model employed are all loaded.

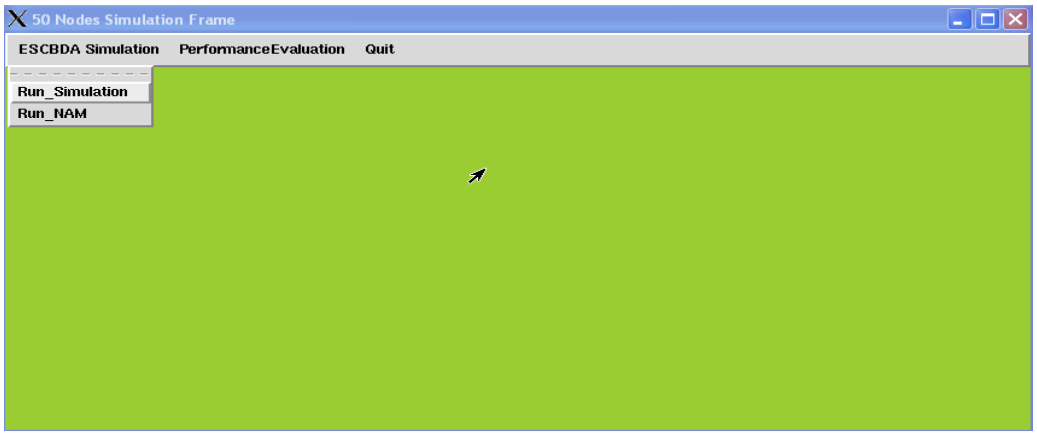

Figure 4.2 Main simulation frame menus

Clicking on the run-simulation in figure 4.2 will start the simulation which will lead to the display of figure 4.3 after some time.

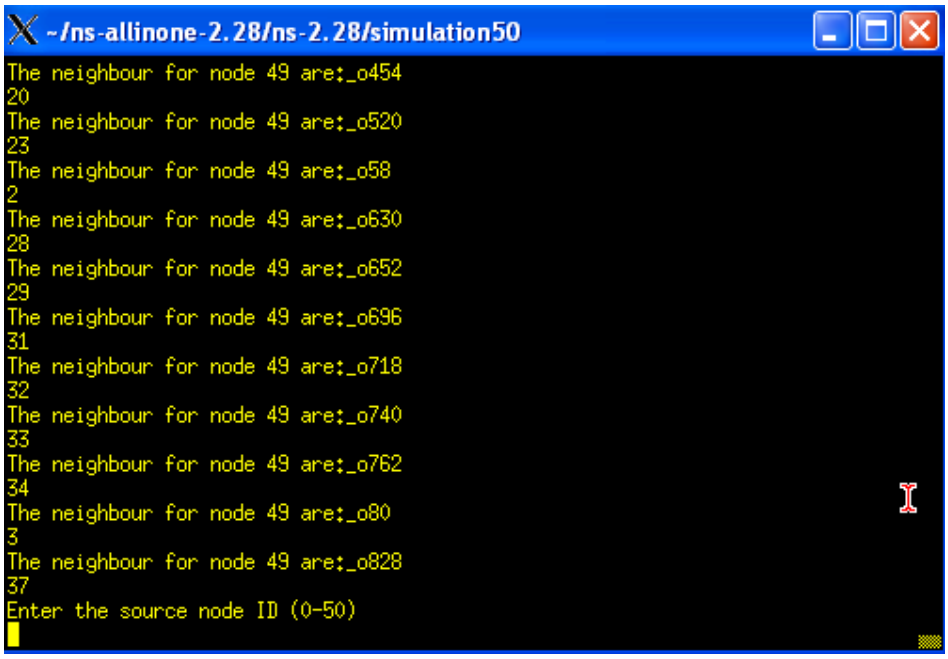

Figure 4.3 shows request for user to enter source and destination ID from 0 to 50.

This figure allow the user to enter the source and destination address from zero inclusive to 50 exclusive, after which the user will be requested to enter the data he or she want to transfer from the source to the destination.

After loading the necessary files and parameters for the simulation, the simulation start by creating the wireless mobile nodes and calculate the distance from each node in the network, from this calculated distance each node in the network would select its neighbors, that is the nodes that are directly within communication range with it in the network, as described by the neighbor selection algorithm. Figure 4.2shows the X-Window displaying the above described event and request the user to select the source and destination ID between 0 inclusive to 50 exclusive. Figure 4.4 shows that the user has selected 36 and 35 as the source and destination IDs, and also shows "FCSIT BUK" as the message that the user want to send from the source to the destination, it also shows the message been encrypted and transmitted to the destination via the route found (36, 0 31 14 35).

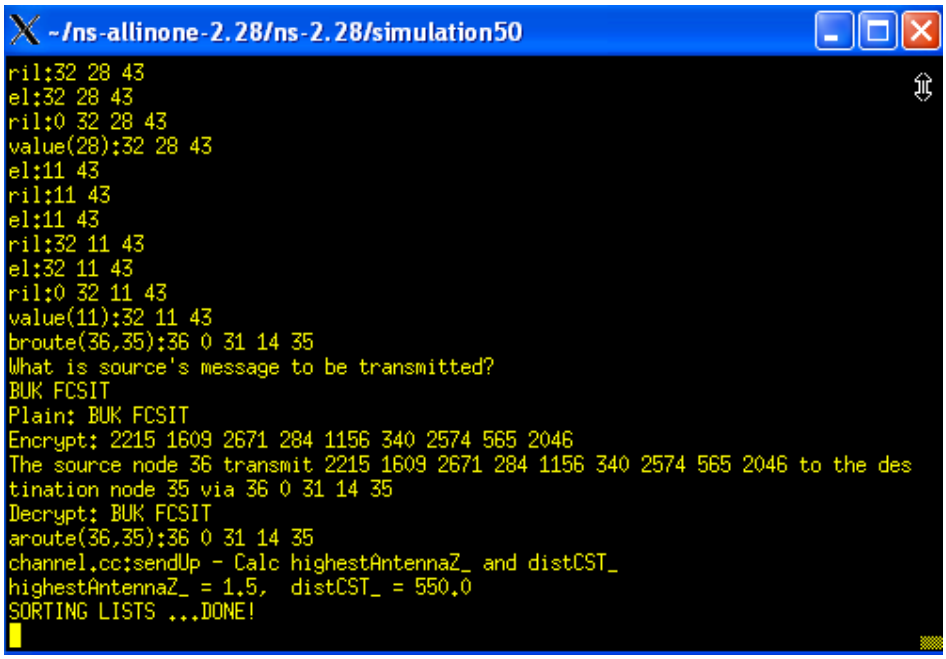

Figure 4.4 Secured transmission via the route found

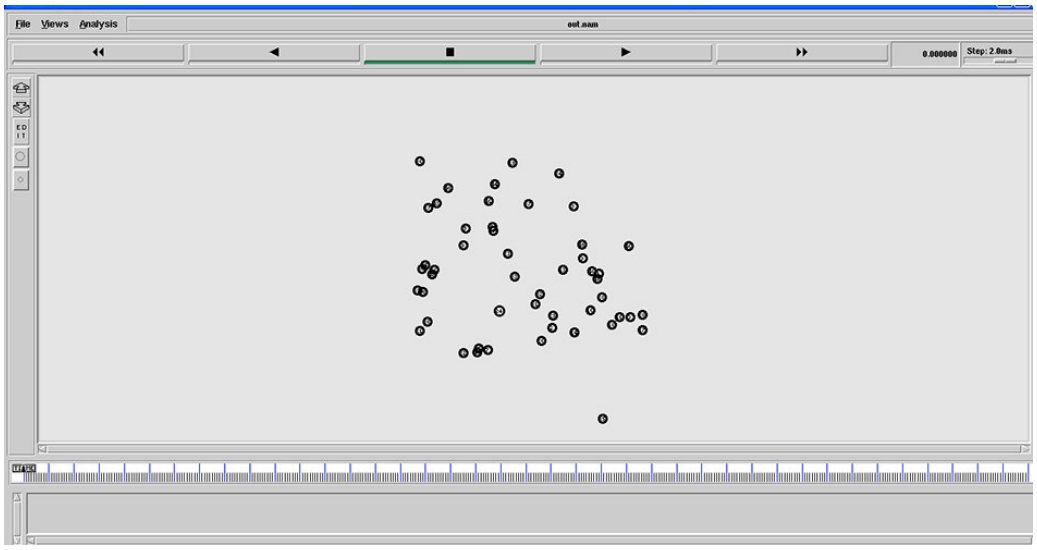

Figure 4.5 Proposed scheme complete setup.

This figure shows a more secured cooperative bait detection scheme network complete setup scenario before it start running, it also shows the initial nodes position in the network. Pressing the play button from the menu bar will cause the network animation to start which is shown in figure 4.6 below

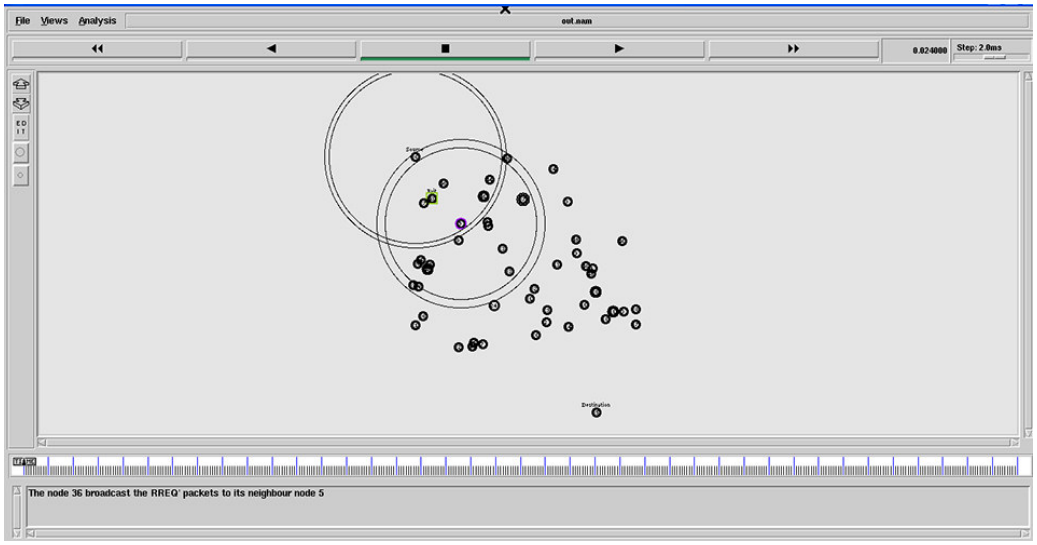

Figure 4.6Source select bait node among its neighbours'

Figure 4.6 shows the proposed scheme network with its entire setup as described in chapter three above, on clicking the paly button on the network animation window tool bar, the network animation will start at zero (0) second of warm up time and the source will immediately select all its neighbors and randomly select one of them as its bait node that it will use to bait malicious nodes as described in the bait setup phase in chapter three above. Figure 4.10 shows the source has selected its bait node as indicated by a yellow green square and a label bait around the node selected, figure 4.7 shows source sent bait RREQ and received RREPs from both malicious and non-malicious nodes, figure 4.8 shows the source detecting malicious nodes labeled malicious in red color using the reverse tracing operation and rechecking nodes that have send RREPs as indicated in yellow color in the figure. Figure 4.9 shows the source broadcasting an alarm packet with the list of the detected malicious nodes to the entire network warning all the network devices to terminate operation with these nodes. Finally figure 4.10 shows the source transmitting the data packet to the destination in a secured manner through the route found.

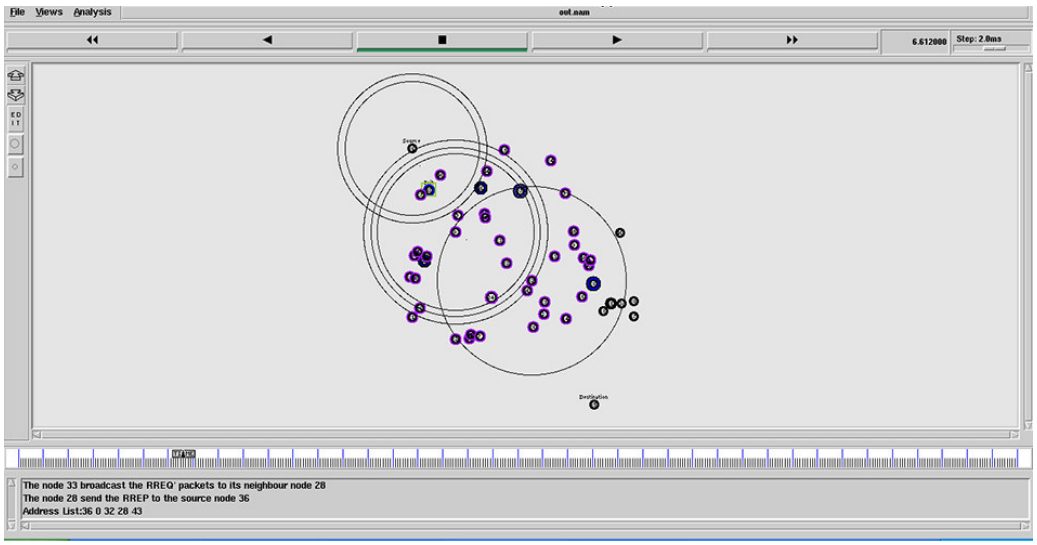

Figure 4.7 source sent bait RREQ and received RREPs

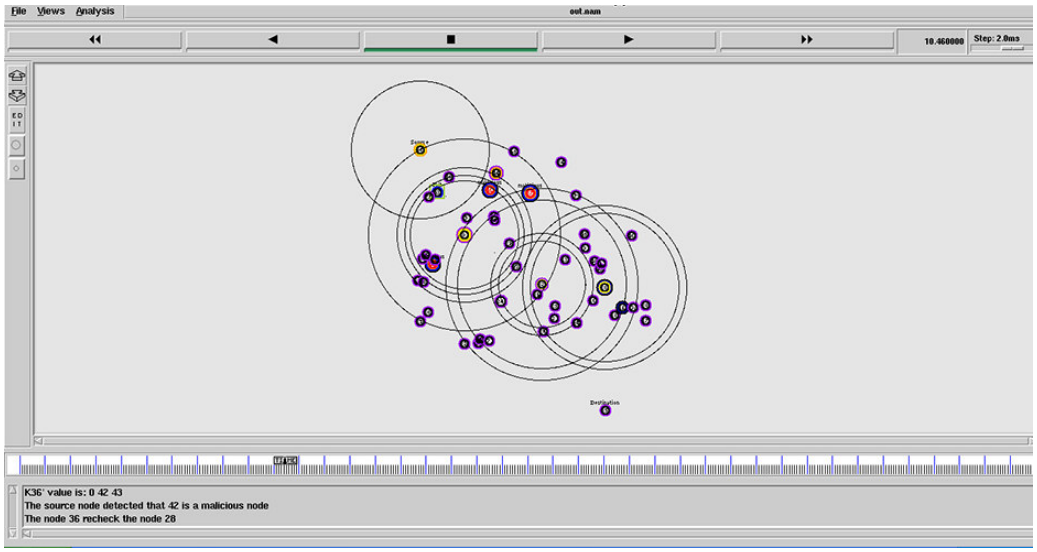

Figure 4.8 source recheck RREPs

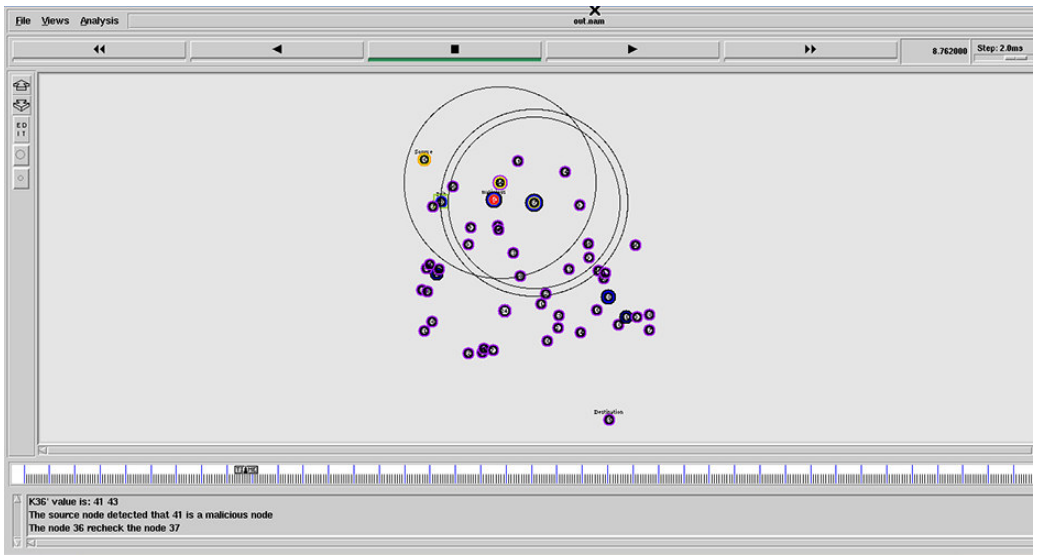

Figure 4.9 Source detect malicious nodes

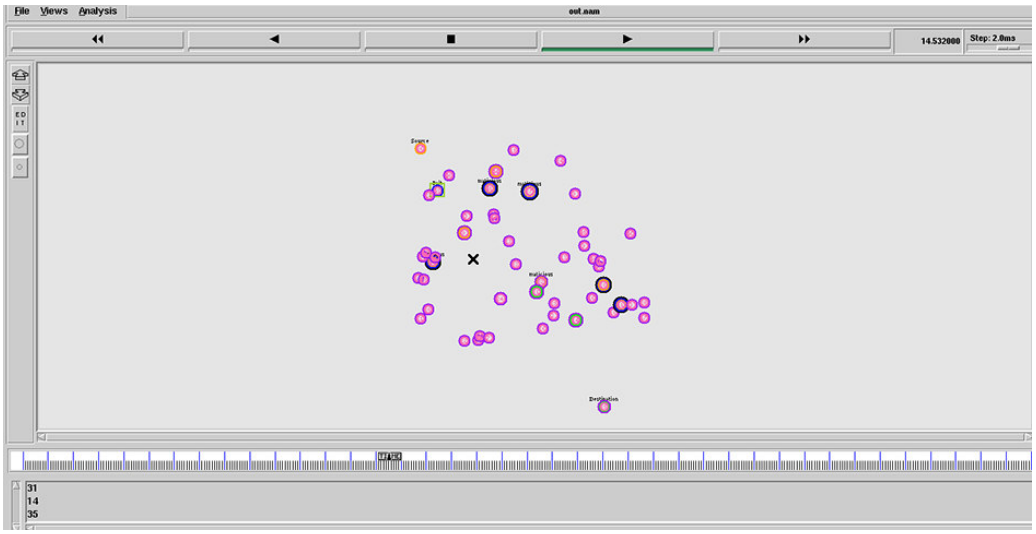

Figure 4.10 source broadcast alarm packet and transmits message to the destination.

After the source node detected the malicious nodes, it will then broadcast an alarm packet with the list of malicious nodes to the whole network, alerting the network nodes to stop further communication with this nodes, then the source will start transmitting the encrypted data through the secured route found thus making data transmission more secured in the presence of malicious nodes. Hence no malicious node can be able to compromise the data sent through it, because of the strong implication of the RSA encryption scheme unlike the cooperative bait detection scheme that employ no encryption scheme.

4.2.1 SIMULATION RESULTS OF THE PROPOSED ENHANCED APPROACH FOR DETECTING AND PREVENTING SINGLE AND COLLABORATIVE ATTACKS IN MANETs AND THE CBDS

The simulation results of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs proposed by the research work and that of the cooperative bait detection scheme proposed in [1] are shown. Two simulation scenarios where considered by the research work, scenario one under fixed mobility and fixed percentage of malicious nodes. The effect of the RSA cryptosystem introduced to the CBDS was studied based on the performance metrics

discussed in chapter three. The second scenario is under fixed percentage of malicious nodes and varying mobility form 0 to 20m/s (0, 5, 10, 15, and 20). Figures 4.16, 4.17, 4.18, and 4.19 shows the simulation results of the performance parameters floated against the simulation time under fixed mobility and percentage of malicious nodes.

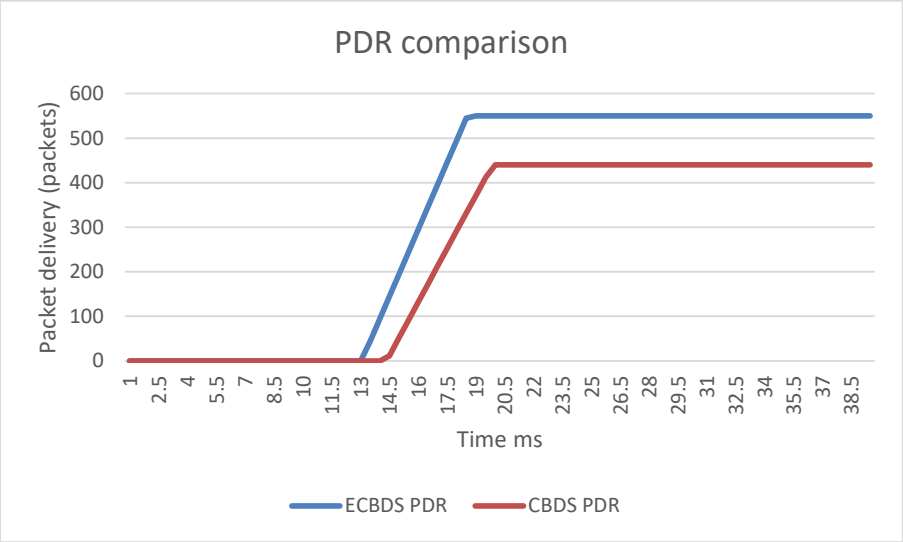

Figure 4.11 PDR comparisons under fixed mobility and percentage of malicious nodes

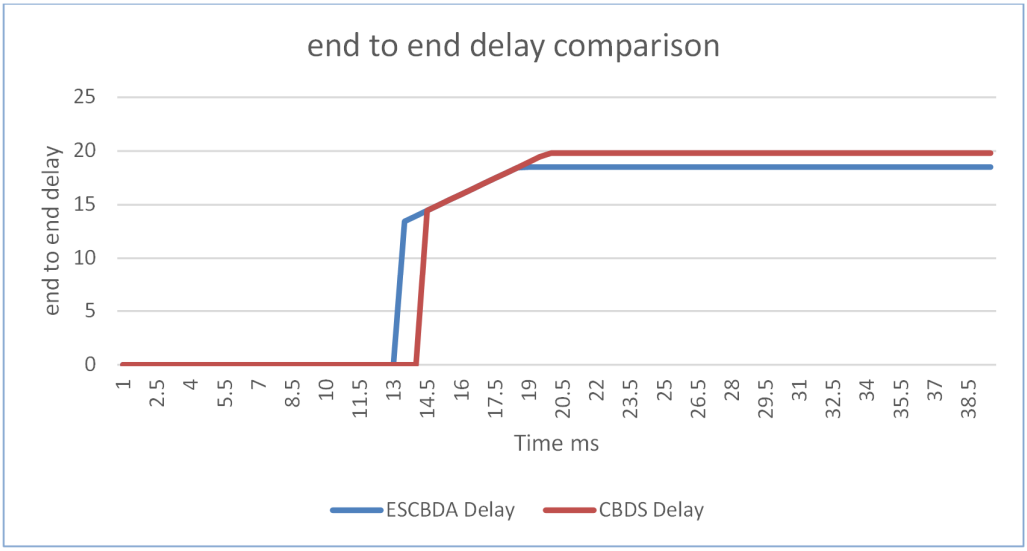

Figure 4.12 end to end delay comparison under fixed mobility and malicious node percentage

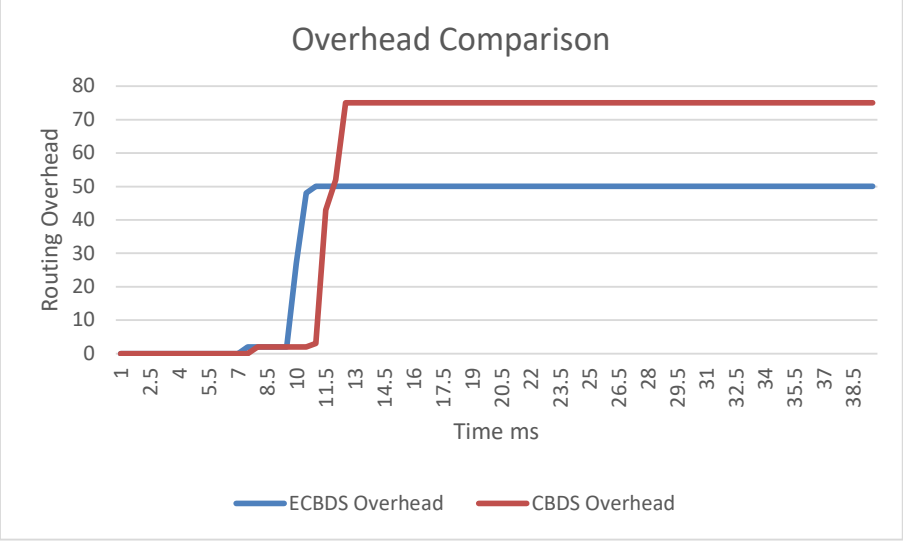

Figure 4.13 Network throughput comparisons under fixed mobility and percentage of malicious nodes

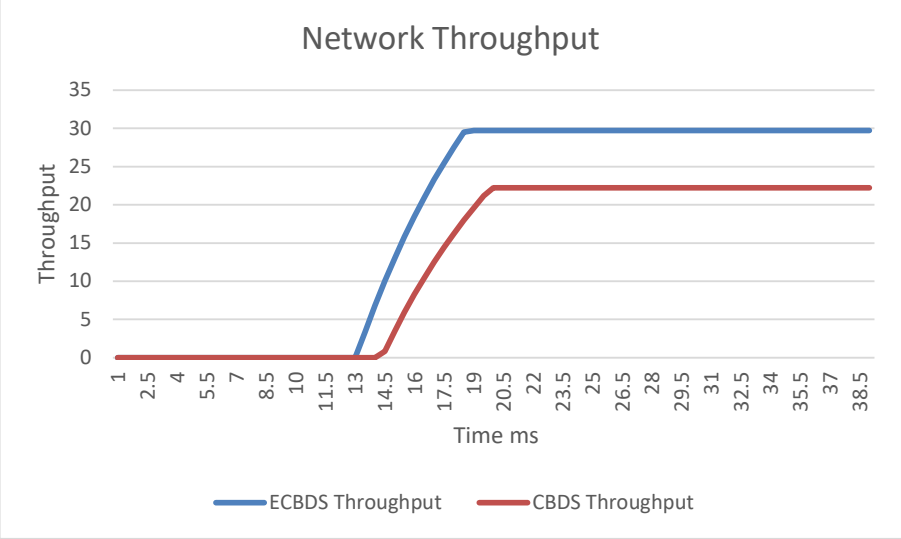

Figure 4.14 Network throughput comparisons under fixed mobility and percentage of malicious nodes

Figure 4.11, 4.12, 4.13 and 4.14 shows the packet delivery ratio, end to end delay, routing overhead and the network throughput of the proposed work and that of the

existing CBDS under fixed percentage of malicious nodes and varying mobility of 0m/s, 5m/s, 10m/s, 15m/s and 20m/s respectively.

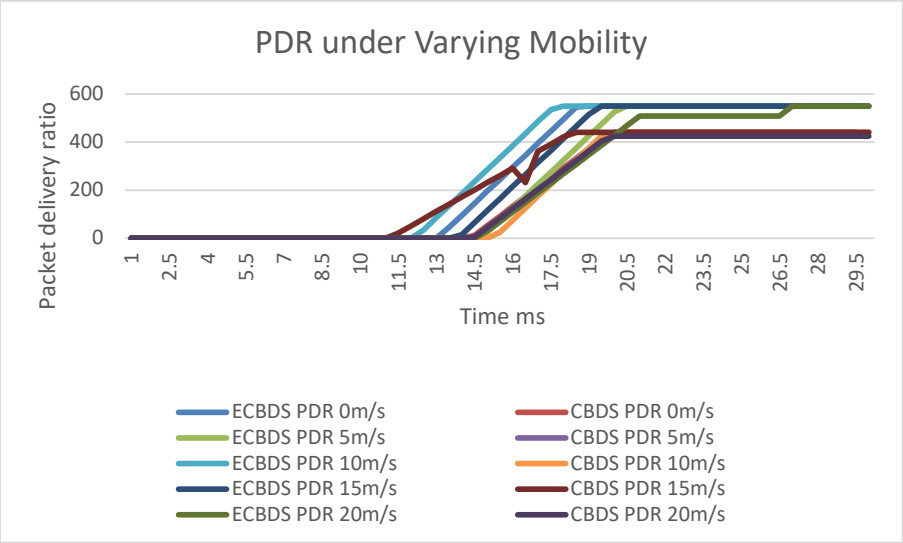

Figure 4.15 Packet delivery ratio under varying mobility

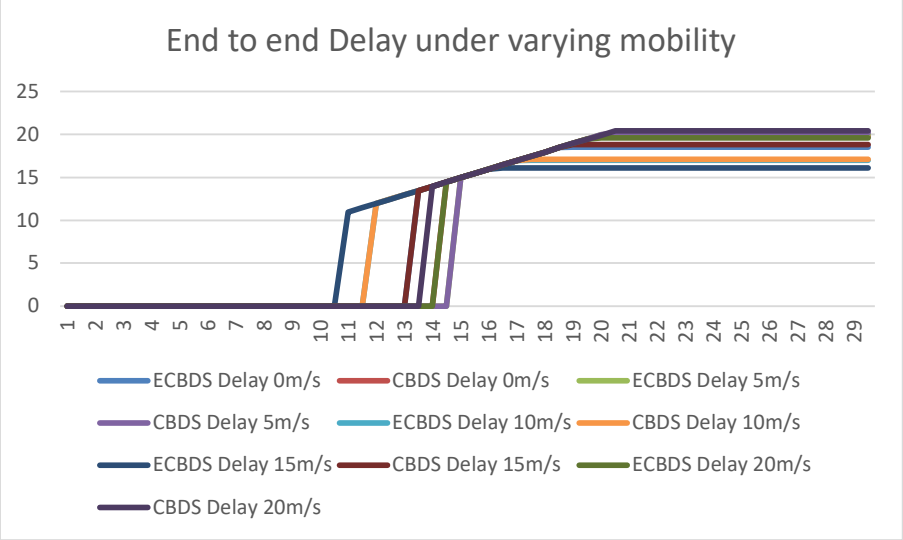

Figure 4.16 end to end delay under varying mobility

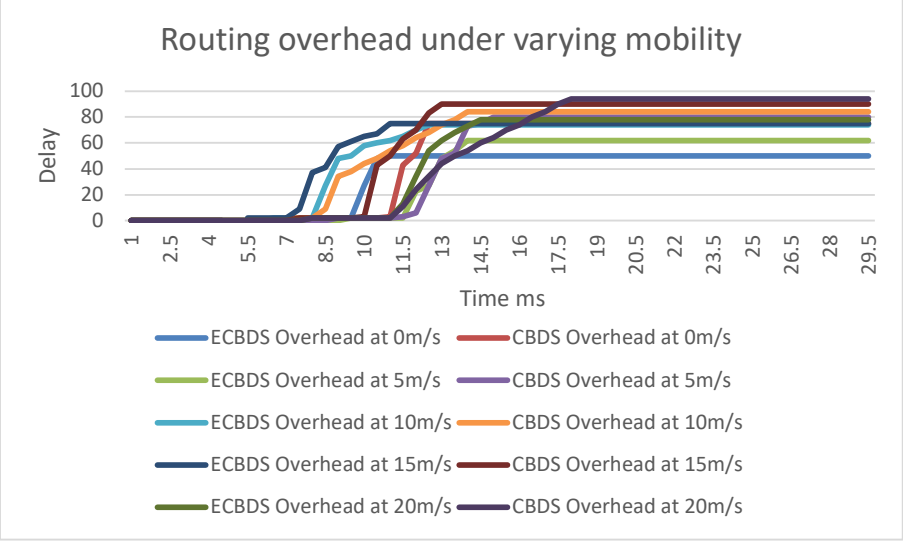

Figure 4.17 routing overhead under varying mobility

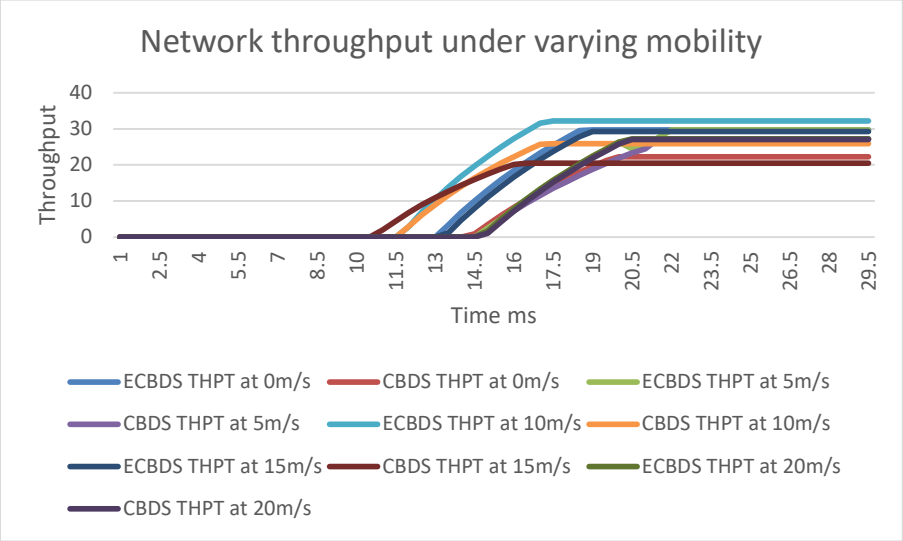

Figure 4.18 Network throughputs under varying mobility

4.3 RESULTS DISCUSSION

Figure 4.11 compares the packet delivery ratio of the proposed enhanced approach for detecting and preventing single and collaborative attacks in MANETs and that of the cooperative bait detection scheme proposed in [1] under fixed percentage of malicious nodes and fixed mobility, it can be observed from the graph that the

proposed work out performs the CBDS in terms of the delivery ratio and this is attributed to the fact the proposed work uses the RSA cryptosystem to prevent reoccurrence of malicious nodes after the initial reverse tracing operation whereas in the CBDS the reverse tracing operation is only recalled to detect the reoccurrence of malicious nodes only when the delivery ratio is below the threshold value, hence cannot detect malicious nodes when presence in the network after the initial reverse tracing and the delivery ratio is net below the threshold value. Also the proposed work can prevent eavesdropping attacks by using the RSA cryptosystem to prevent the eavesdropping nodes from unauthorized reading of the data content which is not the case in the existing CBDS.

Figure 4.12 shows the end to end delay of the proposed work and that of the existing CBDS proposed in [1], from the figure it can be observed that the two scheme have negligible difference in end to end delay and this is due to the fact that both schemes need more time to bait and detect malicious nodes, but the existing CBDS may use the baiting procedure more than once whenever the delivery ratio is below the threshold value thus may produce more delay than the proposed work where the key generation process of the RSA that require more time is assumed in the research work.

Figure 4.13 shows the routing overhead of the two scheme under fixed mobility and percentage of malicious nodes, from the figure it can be observed that the existing CBDS proposed in [1] produces more overhead compared to the existing enhanced approach for detecting and preventing single and collaborative attacks in MANETs and this is due to the use of more control packets by the CBDS when using the threshold value to recall the reverse tracing operation after its initial used, whereas the proposed scheme eliminate the use of the threshold value used in the CBDS to minimizes the use of control packets which help reduce the overhead.

Figure 4.14 shows the network throughput of the proposed scheme and that of the existing CBDS scheme proposed in [1], from the figure it can be observed that the proposed scheme produce more network throughput as compared to the existing CBDS. This shows that the existing CBDS suffers the most from malicious nodes attacks when compared to the proposed scheme.

Figure 4.15 shows the delivery ratio of the proposed scheme and that of the existing CBDS scheme under fixed percentage of malicious node and maximum node mobility speed of 0 to 20m/s. from the figure it can be observed there is a little or negligible decrease in the delivery ratio for both schemes whenever there is increase in node mobility speed. The proposed scheme produces more delivery ratio at 0m/s, 5m/s, 10m/s 15m/s and 20m/s respectively, than the existing CBDS scheme.

Figure 4.16 shows the end to end delay of the proposed scheme and that of the existing CBDS under varying node mobility speed maximum of 0 to 20m/s, from the figure it can be observed that there is little difference in the delay which is due to the fact that both scheme uses the bait and reverse tracing operation which require more time to detect and prevent malicious nodes, but the CBDS shows more delay than the proposed scheme and this is because the CBDS recalled the baiting and the reverse tracing operation to detect the reoccurrence of malicious nodes in the network whenever the delivery ratio is below the threshold value which is not the case in the proposed scheme.

Figure 4.17 shows the routing overhead simulation results of the proposed scheme and that of the existing CBDS under varying node mobility speed, though the routing overhead of the two schemes increases with increase in node mobility speed, the proposed work produces lower overhead than the existing CBDS at all levels and this is because the it employ the use of more routing control packets than the existing scheme which help increase the overhead.

Figure 4.18 shows the network throughput simulation results of the proposed scheme and that of the existing CBDS under varying node mobility. It can be observed that the network throughput for both scheme is affected by node mobility, but the proposed work outperform the existing CBDS in terms of network throughput and this is due to the incorporation of the RSA cryptosystem to the CBDS in order to prevent and detect single and collaborative attacks in mobile ad hoc networks.

4.4 CONTRIBUTIONS OF THE RESEARCH WORK

The research work incorporate an RSA cryptosystem to the existing cooperative bait detection scheme which help detect and identify malicious nodes there by finding an

alternative secured path for routing data in the network. The research work give the following contributions:

I. Increase in packet delivery ratio by 22.22% over the existing CBDS scheme taking as benchmark
II. Increase the network throughput by 26.67% over the existing CBDS scheme taking as bench mark.
III. Lower the routing overhead by 36.36% over the existing CBDS scheme taking as benchmark
IV. Lower the end to end delay by 10% over the existing CBDS scheme taking as bench mark.
V. Able to encrypt data packet before sending it to destination thus improve security in routing data to the destination by preventing unauthorized read and write on the data.

Hence the research work was able to achieve its aim by incorporating the RSA cryptosystem to the existing CBDS, and has helped the research work achieved its objectives by detecting and identifying single and collaborative attacks in MANETs, it also help find a more secured routing path from source to destination by avoiding malicious nodes. Thus the research work achieved its aim and objectives.

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 PREAMBLE

This chapter consist of the summary of the proposed research work, conclusions drawn from it and some recommendations

5.2 SUMMARY

Mobile ad-hoc networks is an infrastructure-less network with mobile nodes as network devices, serving as sources of data or routers used for routing data to other nodes. The network has unpredictable nodes mobility which makes the network topology to be dynamically changing. This dynamical change in topology and nodes mobility makes it difficult to use local routing protocols used in infrastructure based networks to be used in MANETs, to withstand such frequent nodes mobility and dynamical topological changes researchers come up with routing protocols design to be used in MANETs. These routing protocols includes proactive routing protocols which are table-driven MANETs protocols examples include DSDV and OLSR, reactive MANETs routing protocols which are on-demand routing protocols examples includes DSR and AODV and the hybrid MANETs protocols which combine the features of proactive and reactive routing protocols examples includes TORA and ZRP.

In MANETs the primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other [1], but because of the dynamical change in network topology, nodes mobility, lack of infrastructure and lack of central administrator, MANET is susceptible to security flows such as exploiting vulnerabilities to routing protocols, lack of cooperation, transferring harmful packets to the network which results in adverse effect on it. Some of these routing related attacks includes single and cooperative black hole (a situation where an intermediary node present itself to the source node as having the shortest and

freshest route to the destination and in the process drop or refuse to forward the data to the intended destination), gray hole, sinkhole and eavesdropping attacks.

Several researches have been done on the detection and prevention of single malicious nodes attacks in MANETs, some of the researches that have been done for the detection and prevention of cooperative malicious nodes in MANETs includes defending against collaborative attacks by malicious nodes in MANETs using CBDS [1], an efficient protection against collaborative attacks in MANETs using CBDS [8], EMAODV [9], and an enhanced bait approach to defend against collaborative attacks in MANETs proposed in [13]. Though these researches were able to detect cooperative malicious nodes in MANETs at the initial stage of the network, there are re-occurrences of malicious nodes during data transmission, thus the researches cannot be able to prevent attacks from nodes that turn to be malicious after the initial detection stage. Though the CBDA proposed in [1] an approach that uses bait procedure and reverse tracing operation and a threshold value to detect malicious nodes in MANETs, still there are possible occurrence of malicious nodes in the network, and the schemes lacks good message security scheme that help construct a secured routing frame work to prevent MANETs against miscreant.,

To address the above problems a scheme to improve the security of message transmission and to detect and prevent MANETs from further occurrence of cooperative and single malicious nodes attacks during data transmission and other attacks such as sinkhole and eavesdropping that cannot be prevented in the previous work, which will also lead to the improvement of the packet delivery ratio, end to end delay, network throughput and the routing overhead, by in cooperating the existing CBDS with an RSA encryption technique in order to construct a comprehensive secure routing framework to prevent MANETs against miscreant.

5.3 CONCLUSION

The dissertation presents an enhanced approach for detecting single and cooperative attacks in mobile ad-hoc networks under gray/collaborative black hole, eavesdropping and sinkhole attacks, by incorporating RSA cryptosystem to the

existing CBDS. Simulation results shows that the proposed scheme outperforms the existing cooperative bait detection scheme in terms of security, packet delivery ratio, routing overhead, end to end delay amd the network throughput. Hence the research work aim and objectives are achieved.

5.4 RECOMMENDATIONS

The research work contribution consist of a technique that attempts to build an enhanced secured routing framework in MANETs by making data transmission more secured, thus preventing MANETs against malicious nodes attacks. Some of the recommendations given by the research work are:

I. The proposed protocol should be tested in real life environment to see how near to perfect it can take routing security in mobile ad-hoc networks. This will no doubt point out how other protocols may be incorporated with the RSA cryptosystem in order to build a comprehensive routing framework in MANETs.
II. In addition to routing security, more efforts should be dedicated to other aspects that matters in determining the flexibility level of MANETs, some of them are battery power, optimization and mobility of devices in the network to mention but few.
III. Conferences, seminars, lectures, and tutorials should be carried out regularly with the aim of exploring the importance of MANETs and the reasons why people should move to such networks.

5.5 FUTURE WORK

There is need to find a way of generating the RSA cryptosystem to minimize assumption. Investigate the possibility of determining the effectiveness of the performance of the proposed enhanced approach for detecting single and collaborative attacks in mobile ad-hoc networks by running the two schemes on the same machine in real world environment.

REFERENCES

[1] Jiang-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Ching-Feng Lai Member IEEE. "Defending Against Collaborative Attacks By Malicious Nodes In Manets: A Cooperative Bait Detection Approach" IEEE system journal 2014

[2] B. Konadiaha and Dr. M. Nagendra. "An Efficient Protection against Collaborative Attacks in MANETs Using Cooperative Bait Detection Scheme" international journal of innovative research in computer and communication engineering vol. 4 issue 2 February 2016

[3] Akinlemi Olushola O. and K. Suresh Babu "Cooperative Bait Detection Scheme CBDS to Avoid the Collaborative Attacks of Nodes in MANET" International journal of Scientific Engineering and research (www.ijser.in) impact factor (2014) 3:05

[4] Mohan M, M Ramakrishna and K N Narasimha Murthy "A Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs" IJIRCCE vol.3 Issue 5 May 2015

[5] Prachi Arya, Gogan Prakash Negi, Pushpender Kumar Dhiman and Kapil Kapoor, "CBDS (Cooperative Bait Detection Scheme) Attack- A Review" international journal of advance research in computer engineering and technology (IJARCET) vol.4 issue 8 August 2015

[6] Mohan M and Ramakrishna M "A Survey on Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs" International journal on recent and innovative Trends in computing and communication Vol3 Issue 3.

[7]M. Rajkumar, U Shiny and R. Rani "Detection of Wormhole Attack Using Cooperative Bait Detection Scheme" world scientific news vol. 49 Issue 2 2016

[8] Priya C and Kumar C "An Efficient Approach for Detecting Malevolent Nodes in MANETs Using Cooperative Bait Detection Scheme" International Journal of Advance Research in Biology Engineering Science and Technology Vol.2 Special Issue 10 March 2016

[9] Anuj Rana, Vinay and Sandeep Gupta "EMAODV: Technique to Prevent Cooperative Attacks in MANETs" 4th international conference on eco-friendly computing and communication system, ICECCS 2015

[10] Vishnu K and Amos J Paul "Detection and Removal of Cooperative Black hole gray hole attacks in MANETs" International journal of computer Application (09975-8887) vol.1 no.22, 2010

[11] A. Syeda Mustafa, Dr. C. Nelson Kennedy Babu and R. Kasthuri "Token Ring Based Cooperative Bait Detection for Both Selfish and Malicious Node Attacks in Ad hoc Communication" Middle-East journal of Scientific Research 24, 2016

[12] Abudl-Jawad PP and Bismin Chacko "ECBDS: Enhanced Cooperative Bait Detection Scheme for Preventing Collaborative Attacks in MANETs" International journal of science and Research Volume 6 issue 14 2013

[13] Kruthi Hedge S and Uvraj Aruthumaran S "An enhance Bait Approach to Defend against Collaborative Attacks in MANETs" international journal of emerging technology in computer science and electronics volume 13 issue 1-March 2015

[14] S Abirami, S Barani, B Dhivya and D Meena "Defending Malicious Node Using MANETs in Cooperative Bait Detection with the Onion Routing Protocol" International Journal of Innovative Science and Engineering and Technology Vol. 3 Issue 3 March 2016 (www.ijiset.com)

[15] Sanjay Ramaswami, Huirong Fu, Manihar Sreekantaradhya, John Dixon and Kendali Nygard "Prevention of Cooperative Black hole Attacks in Wireless Ad hoc Networks"

[16] P.S. Hiremath and Anuradha T. "Detection and Prevention of Cooperative Black hole Attacks in MANETs" international Journal of Research in Computer and Communication Technology Volume 3 Issue 5 May-2014

[17] V. Abinaya and Dr. Santhi "Hop Count Based Enhanced Cooperative bait Detection Scheme to Prevent Collaborative Black hole Attacks in MANETs" International Journal of Research and Application Vol. 7 Issue 2, 253-260 March-April 2016

[18] Syeda Arshiya Sultana and Samreen Banu Kazi “Reverse Tracing Scheme to Prevent the Cooperative Attacks in MANETs” International Journal of Emerging Technology in Computer Science and Electronics Vol. 14 Issue 2 April-2015

[19] Muhammad Adam Aldod Ibrahim “Implementation of RSA and ECC Security Protocol for MANETs” Sudan University of Science and Technology, college of Post Graduate Studies 24 April 2015

[20] Krishna Gorantala “Routing Protocols in MANETs” UMEA University Department of Computer Science Sweden 2006

[21]Akshata Prabhu and Shobha Krishnan “Effect of Black hole attack on MANETs Routing Protocols” International Journal of Engineering Research in Electronics and Communication Engineering Vol. 2 Issue 11 Nov. 2015

[22] D. Ganesh Kumar, N. Kumar and M. Ramesh Kumar “A Complete Study on Unipath Routing Protocols in MANETs” International Journal of Engineering Trends and Technology Vol. 6 Nov-Dec 2013

[23] Arun Mukhija and Dr. Ranjan Bose “Reactive Routing Protocol for MANETs” Department of Mathematics Indian Institute of Technology Delhi Dec. 2001

[24] Hemagowri J, Barani Kumar C and Brandha B. “A Study on Proactive Routing Protocol in MANETs” International Journal of Modern Engineering Research ISSN: 2249-6645

[25] Subhananda, Joardar and Bikash Das “Reactive and Proactive Routing Protocols Performance Metric Comparison in MANETs Using NS2” International Journal of Advance Research in Computer and Communication Engineering vol. 3 issue 1 Jan. 2014

[26] Jose Costa-Requena “A Hybrid Routing Approach for MANETs” Helsinki University of Technology, Networking Laboratory ESPOO 2007

[27] Aniruddha Bhattacharyya, Arnab Banerjee and Dipayan Bose “Different Types of Attacks in Mobile Ad hoc Networks: Prevention and MitigationTechnique” Department of Computer Science and Engineering, Institute of Engineering and Management Saltlake

[28] Vimal Kumar and Rakesh Kumar “An Adaptive Approach for Detecting Black hole Attack in MANETs” International Conference on Intelligent Computing and

Communication and Convergence (ICCC-2015) Procedia Computer Science 48(2015) 472-479

[29] Bello Musa Yakubu, Mr. Pankaj Chajera and Dr. Ahmed Baita Garko "Advance Secure Method for Data Transmission in MANETs Using RSA Algorithm" International Journal of Advance Technology in Engineering and Science Vol.3 Issue 1 Sept. 2015

[30] Gaurav Dwivedi and Manveer Kar "Prevention fromBlack hole Attack Using RSA Algorithm" Journal of Computer Science and Software Development Vol.2 Issue 1 July-2016

[31] Sapna Boora, Sonia Ohri "A Survey of Layer Specific and Cryptographic primitive attacks and their countermeasures in MANETS"

International Journal of P2P Network Trends and Technology (IJPTT) - Volume3 Issue4- May 2013

[32] Aditya Bakshi, A.K. Sharma and Atul Mishra "Significance of Mobile Ad hoc Networks (MANETs)" International Journal of Innovative Technology and Exploring Engineering (IJITEE) Vol. 2 Issue 4 March 2013

[33] Forouzan B. A. "Data Communication and Networking (4 Edition)", McGraw Hill Inc. New York, 2008.

[34] Tutorials Point "Cryptography just for beginners" www.tutorialspoint.com

[35] Cryptographic Algorithm Report

[36] Cipher This Category A: Competitive New Mexico High School Super Computing Challenge Report

[37] RSA ALGORITHM BY AURESH SAXEENA (HOTBURN)

[38] NS-Doc Network simulation Manual for NS2

[39] Chapter Six Performance Comparison

[40] Praven Kumar, Suresh P, and Tanmay Gupta "IMPLEMENTATION OF DYNAMIC SOURCE ROUTING PROTOCOL" Project submitted in partial fulfillment of the requirement for the Megree of Master of Technology Department of Computer Science and Engineering, Indian Institute of Technology Delhi May 2015

Appendix A
Sample Appendix

<This is a sample Appendix. Insert additional appendices with the “Start New Appendix” command.>