UNIVERSIDAD NACIONAL DE COLOMBIA

A Cryptography-Based Mechanism For Identifying Nodes Applied To Detection Of Wormhole Intrusion In Ad-Hoc Networks

Carlos Felipe Téllez Castaño

National University of Colombia

Faculty of Engineering, Department of Industrial and Systems Engineering

Bogotá D.C., Colombia

2012

A Cryptography-Based Mechanism For Identifying Nodes Applied To Detection Of Wormhole Intrusion In Ad-Hoc Networks

Carlos Felipe Téllez Castaño

A thesis submitted in partial fulfillment of the requirements for the degree of:

Master in Systems and Computer Engineering

Director:

Ph.D. Jorge Eduardo Ortiz Triviño

Research Line:

Information Security and Cryptography

National University of Colombia

Faculty of Engineering, Department of Industrial and Systems Engineering

Bogotá D.C., Colombia

2012

A Dios por ser mi motor y mi guía, a mi esposa cuyo ejemplo, sacrificios y palabras de aliento me impulsaron a finalizar este trabajo y a mis Padres por sus oraciones y apoyo. A mi País esperando que la necesidad identificada pueda ser suplida en el futuro.

Acknowledgements

Special thanks to director Ph.D Jorge Eduardo Ortiz Triviño Associate Professor at the Department of Computer Systems and Industrial Engineering at National University of Colombia who shared with me his knowledge not only of matters pertaining to this work but also focused on issues such as the publication of a paper in the journal IJCSNS and presenting a paper at the conference CNIS of Colombia, among many other helpful tips during the course of this work. Thanks to Jaime Rodríguez engineer and software architect who instructed me in the generation of the software architecture of the simulations of this work. Thanks to Andrés Daza, systems engineer, who helped me in revising of the English grammar. Thanks to Andrés Quintero, systems engineer, who helped me in revising of the Java Code of Simulations.

Abstract

When it comes to ad-hoc networks, we refer to a technology which consists of wireless telecommunications network of dynamic topology, where a set of mobile communication nodes such as routers interact among themselves, passing on information without relying on any fixed infrastructure. Given this description, we find some limiting characteristics that make the Ad-Hoc wireless networks, very vulnerable to intruders and attacks that can damage the integrity of the network. Features such as the limited ability to process nodes, limited bandwidth, and an interaction that requires each node to be involved in decision making network make these networks a comprehensive field of study in communications. In this thesis, we intend to show in the security field above a specific type of intrusion that today has become very common for Ad-Hoc networks: Wormhole intrusion. We present a design of a mechanism to avoid this kind of intrusion based on Elliptic Curve Cryptography. This mechanism represents the result of several theoretical analysis about the intrusion, about the elliptic curve cryptography, about security in Ad-Hoc and all this accompanied by the implementation of a series of simulations that show a proposed security protocol based on the Collaborative Agents application of anomaly detection, in conjunction with the Elliptic Curve Cryptography to conclude how this proposed solution is capable of addressing the Wormhole attack in mobile wireless networks.

Key words: 1) Ad-Hoc, 2) Wormhole Intrusion, 3) Elliptic Curve Cryptography, 4) Performance Analysis, 5) State of the Art, 6) MANET Security.

Resumen

Cuando hablamos de Redes Ad-Hoc, nos referimos a una tecnología que consiste en redes de telecomunicación inalámbrica de topología dinámica, donde un conjunto de nodos móviles de comunicación interactúan como enrutadores entre ellos transmitiéndose información sin depender de alguna infraestructura fija. Frente a esta descripción, nos encontramos con algunas características limitantes que hacen de las redes inalámbricas Ad-Hoc, muy vulnerables al acceso de intrusos y ataques que pueden dañar la integridad de la red. Características tales como la limitada capacidad de proceso en los nodos, un ancho de banda limitado y una interacción que requiere que cada nodo se involucre en la toma de decisiones de la red hacen de este tipo de redes un campo de estudio exhaustivo en las comunicaciones. En esta tesis, se pretende mostrar dentro del campo mencionado de la seguridad un tipo de intrusión específica que hoy en día se ha vuelto muy común para las redes Ad-Hoc: La intrusión Wormhole. Se presenta un diseño de un mecanismo capaz de evadir este tipo de intrusión basado en criptografía de Curvas Elípticas. Este mecanismo, representa el resultado de varios análisis teóricos sobre la intrusión, sobre la criptografía de curvas elípticas, sobre la seguridad en Ad-Hoc y todo esto acompañado de la implementación de una serie de simulaciones que muestran un protocolo de seguridad propuesto basado en la aplicación de Agentes Colaborativos de detección de anomalías, junto a la Criptografía de Curvas Elípticas con el fin de concluir cómo esta solución propuesta es capaz de hacer frente al ataque Wormhole en redes móviles inalámbricas.

Título de la Tesis en Español: “Un mecanismo de identificación de nodos basado en criptografía para la detección de la intrusión Wormhole en redes Ad-Hoc”.

Palabras clave: 1) Ad-Hoc, 2) Intrusión Agujero de Gusano, 3) Criptografía de Curvas Elípticas, 4) Análisis de Rendimiento, 5) Estado del Arte, 6) Seguridad en MANET.

Table of Contents

Page

Abstract ..... **IX**

Resumen ..... **X**

List of figures ..... **XIV**

List of tables ..... **XVI**

Introduction **1**

1. Chapter 1 ..... **3**
1.1 Motivation 3
1.2 Main Goal 4
1.3 Specific Goals 4
1.4 Structure of the Thesis 4

2. Chapter 2 ..... **7**
2.1 Conceptual Framework 7
2.2 AD-HOC Features 8
2.3 Mobility Models 8
2.4 Types of Routing Protocols 9
2.4.1 AODV (Ad-Hoc On Demand Distance Vector) 10
2.4.1.1 Operation 10
2.4.1.2 Features 11
2.4.1.3 RREQ message contains 11
2.4.1.4 RREP message contains 12
2.4.1.5 Example 12
2.4.2 AODV: Advantages Over Other Routing Protocols 16
2.5 The Wormhole Intrusion 16
2.5.1 Definition 16
2.5.2 Actions That Wormhole Can Perform 17
2.5.3 Wormhole Types 18
2.5.3.1 According to its mode of attack 19
2.5.3.2 Depending on whether the attackers are visible in the path 19
2.5.3.3 Depending on the resources used for the attack 19
2.5.4 Proposed Solutions Against The Wormhole Attack 20
2.5.4.1 Location-based, Distance-based and Time-based 21
2.5.4.2 Hop-count Analysis 21
2.5.4.3 Graph-based and Geometric-based 21
2.5.4.4 Neighbor monitoring-based 22

2.5.4.5 Statistical 22
2.5.4.6 Key-based 22
2.6 Elliptic Curve Cryptography (ECC) 22
2.6.1 Definition 22
2.6.2 The Finite Field In ECC 23
2.6.3 Computational Levels and Field Representation 25
2.6.4 Domain Parameters and Types of Elliptic Curves 28
2.6.4.1 Curve Domain Parameters over $\mathbb{F}_p$ 29
2.6.4.2 Curve Domain Parameters over $\mathbb{F}_{2^m}$ 29
2.6.5 Elliptic Curve Point Representation 30
2.7 ECC Implementations for MANET (Related Work) 32
2.7.1 ECC Schemes 32
2.7.2 Key Establishment Process 33
2.7.2.1 By its distribution 33
2.7.2.2 By the prior information 33
2.7.3 Why ECC in MANET? 34
2.7.4 ECC Proposals Applied to MANET (Related Work) 34
2.7.4.1 By the organization of the nodes in the network 35
2.7.4.2 By Key Establishment Process 35
2.7.4.3 By the Use of MANET as a Way of Implementation and Improvement of ECC 36
2.8 ECC Implementation During Wormhole Attack In MANET 36
2.8.1 Security Requirements In MANET 36
2.8.2 Aspects to Ensure Security in MANET 37
2.8.2.1 Intrusion detection 37
2.8.2.2 Secure routing 37
2.8.2.3 Key management service 38
2.8.3 Key Management Service Attributes 38
2.8.4 Levels of Security Against a Wormhole 39
2.8.5 Analysis of the Behavior of ECC for the Wormhole Intrusion 40

3. Chapter 3 43
3.1 Proposed Solution and Justification 43
3.2 MANET Environmental Construction 43
3.2.1 Simulator Description 43
3.2.2 Choice of the System Organization of Network Nodes 44
3.2.3 Other Features to Consider For the Solution 44
3.3 Intruder Construction 45
3.4 Design Solution of Detection and Evasion 45
3.4.1 IDS to Use Against Wormhole 45
3.4.2 Safe Routing System to Use 46
3.4.3 Review of the ECC Implementation for the Solution 46
3.5 Summary of the Solution Represented In Simulations 47
3.6 List of Simulations 47
3.7 Solution Architecture 49
3.7.1 Background of the Solution and Logical Layers 49
3.7.2 Random Waypoint - Class Model 50
3.7.3 AODV Packages - Class Model 51
3.7.4 ECC Application - Class Model 52
3.7.5 Cross Components - Class Model 53

3.8 Description of Simulations 54
3.8.1 Simulation of the Mobility Model 54
3.8.2 Simulation of the Routing Protocol 56
3.8.3 Simulation of the Wormhole Intrusion 56
3.8.4 Simulation of the Wormhole Detection 57

4. Chapter 4 59
4.1 Experimental and Results - Behavior of Intruder 59
4.2 Results of the Detection and Evasion 66

5. Chapter 5 71
5.1 Conclusions 71

References 73

List of figures

Pág.

Figure 2-1: Graphical Representation of an Ad-Hoc Network 8
Figure 2-2: Random Waypoint Mobility Model (RWP). 9
Figure 2-3: AODV Step 1 12
Figure 2-4: AODV Step 2 13
Figure 2-5: AODV Step 3 13
Figure 2-6: AODV Step 4 14
Figure 2-7: AODV Step 5 14
Figure 2-8: AODV Step 6 15
Figure 2-9: AODV - RERR Message. 15
Figure 2-10: Intrusion in Ad-Hoc Network with Wormhole Tunnel. 16
Figure 2-11: Elliptic curves over the field $\mathbb{R}$. 23
Figure 2-12: Computational levels of an ECC. 25
Figure 3-1: Software solution components 49
Figure 3-2: Random Waypoint – Class model. 50
Figure 3-3: Random Waypoint on OTcl. 51
Figure 3-4: AODV packages - class model. 52
Figure 3-5: ECC application - class model. 53
Figure 3-6: Cross Components - class model. 54
Figure 3-7: Simulation of the mobility model. 5 nodes 55
Figure 3-8: Simulation of the mobility model. 50 nodes 55
Figure 3-9: Simulation of the routing protocol. 56
Figure 3-10: Simulation of the wormhole intrusion. 57
Figure 3-11: Simulation of the wormhole detection. 57
Figure 4-1: Simulation 1 - Results 60
Figure 4-2: Number of packets sent / received in a time t and number of packets that pass through the tunnel 62
Figure 4-3: Number of packets sent / received in total in a simulation and the number of packets that pass through the tunnel. 62
Figure 4-4: Number of packets sent / received in total in a simulation and the number of packets that pass through the tunnel with an active attack. 63
Figure 4-5: Number of packets sent / received in a time t and number of packets that pass through the tunnel with an active denial of service attack 65

Figure 4-6: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack. 65
Figure 4-7: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a EC-S-AODV functional protocol. 66
Figure 4-8: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a Distributed and Cooperative IDS. 68

List of tables

Pág.
Table 3-1: Summary of features in Simulations. 47
Table 4-1: Number of packets sent / received in a time t and number of packets that pass through the tunnel. 61
Table 4-2: Number of packets sent / received in a time t and number of packets that pass through the tunnel with an active denial of service attack. 64
Table 4-3: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a EC-S-AODV functional protocol. 67
Table 4-3: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a Distributed and Cooperative IDS. 69

Introduction

A MANET (Mobile Ad-Hoc Network) [1] is a set of autonomous and spontaneous routers or mobile nodes that communicate with each other through wireless connections, where there is no fixed network infrastructure and management is done distributed. That's how the nodes are involved in routing algorithms and security.

To the features of these important and useful networks such as the limited ability to process the nodes with high bandwidth connections scarce, dynamic topology and power constraints must be added vulnerability to attacks from intruders. Security in these networks is a challenge, even more when it comes to intrusions as Wormhole tunnel [3].

There are three aspects in the field of Ad-Hoc network security: the Intrusion Detection Systems (IDS), Secure routing and Authentication Access via key management [87]. The present research focuses on building a solution that combines these three aspects applied to the reactive routing protocol AODV (Ad-Hoc On Demand Distance Vector Routing) [91] and using Elliptic Curve Cryptography [44] for detection and avoidance of a specific type of intrusion called Wormhole [3]. In the end there will be constructed a series of simulations that demonstrate the application of the solution and its behavior in a MANET environment.

1. Chapter 1

1.1 Motivation

Wormhole is an attack on the routing protocol of the network where 2 colluder nodes or more intercept packets of information while traveling at a point A of the network, and quickly reinserted in another physical point B in the same network creating a "tunnel "from A to B [3]. By intercepting packets, the attacker could practically do with them as he pleases.

Some proposals to counter this type of attack have been raised. Some proposals have been of physical type [4]. Others are focused on how to attack the intruder from the network's geographic area (location of the nodes, distances between them, location of failures), [3], [5], [6], [8], other by analysis of the transmission times of nodes [7], [9] and other focused on monitoring routing [10]. Some studies even say that while there is a system of authentication and encryption, the attack can be carried out [2], [3].

Based on these studies, several questions arise: What happens then to all the proposed solutions based on Elliptic Curve Cryptosystems (ECC) and applied to Ad-Hoc networks that claim to guarantee security in such networks? Can an ECC applied to Ad-Hoc networks alone prevent, detect, evade and/or eliminate a Wormhole attack?, If not, is it necessary to satisfy the criteria of integrity, authentication, non-repudiation and application availability combine a cryptosystem with some of the solutions already proposed to attack the Wormhole intrusion?.

But, Why ECC? Today, it is becoming increasingly common the implementation of the Elliptic Curve Cryptography (ECC) for Ad-Hoc networks, because compared to cryptosystems such as RSA, ECC offers equivalent security level with smaller key sizes, faster computing, with low power and memory consumption and savings in bandwidth [11], which are precisely the characteristics that make it attractive to apply in this type of

networks with limited resources [12]. For this reason this study focuses on assessing the level of security offered by these new proposals based on elliptic curve cryptography for Wormhole intrusion.

The suggestion is to validate the ECC Elliptic Curve Cryptography [44], analyzing their ability to escape detection and intrusion Wormhole, without the use of physical devices in addition to the existing network and to demonstrate its efficiency in MANET.

1.2 Main Goal

To implement in a computer simulation a technique of Wormhole intrusion detection in Ad-Hoc networks using elliptic curve cryptography on AODV routing protocol.

1.3 Specific Goals

- Implement a computer simulation of reactive routing protocol AODV, in a MANET.
- Implement a computer simulation Wormhole attack with its features.
- Implement a computer simulation technique Elliptic Curve Cryptography for the implementation of intrusion detection.
- Conduct job evaluation in the final simulation experiments to present the statistical results obtained and determine the quality of the intrusion detection measured in terms of effectiveness.

1.4 Structure of the Thesis

This thesis is divided into 5 chapters. The first introductory chapter discusses the topic, the motivation and objectives that are intended to achieve and the explanation of the structure of the document. The second chapter sets the state of the art on the Ad-hoc networks, mobility models, routing, intrusion Wormhole, elliptic curve cryptography and some results of previous work on wormhole tunnel safety and application of elliptic curves are not directed towards this attack. In the third chapter describes the proposed solution based on cryptography, showing the development of simulations that support it. In the fourth chapter shows the simulations and the description of results. In the fifth chapter gives the conclusions, references and the additional data are appended.

2. Chapter 2

2.1 Conceptual Framework

Wireless networks have had a dizzying acceptance and expansion due to the proliferation of inexpensive wireless devices, widely available in the marketplace and the community's interest in mobile computing networks.

However, the uses of such networks go beyond the customized business use. In situations where the infrastructure is not available, or where it is not trusted to use Ad-Hoc networks becomes essential, even for emergencies. Some examples include: communication of military soldiers in the field, sensors scattered throughout a city for biological or climatological use; network infrastructure laptops in a conference or college, rare animal tracking, space exploration, undersea operations and the deployment of temporary offices [92] are some of the uses to which it can give this type of network, not counting future what could be many other applications such as communication between mobile robots [93], or the use of mobile devices in the process of rescue on a Colombian geography and geographical areas where there are highly rugged relief.

However, the use of networks such as functional has some limitations that will gradually have been mitigated in terms of research. Routing, security, maintenance, use of physical network resources, service quality [94] are some of the topics that have been studying and dealing with day to day to try to improve the use of the Ad-Hoc Mobile Networks also known as MANET.

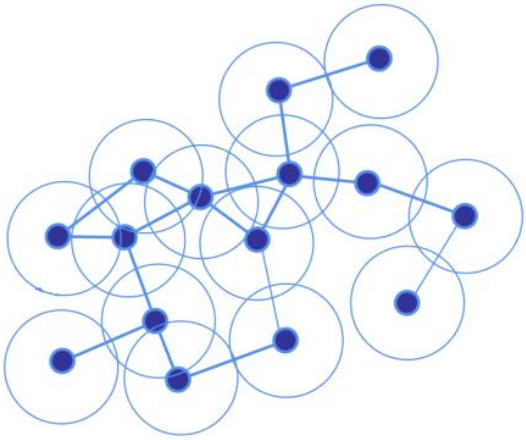
There is much that we can talk about this type of networks, however this research is focused on the issue of security, and more specifically, the application of algorithms based on Elliptic Curve Cryptography to evade one of the attacks that threaten the common security of such networks, the wormhole attack.

2.2 AD-HOC Features

Among the salient features of the Ad-hoc networks are [1], [92], [95], [96] and [97]: No fixed base stations - the deployment is fast, the network topology is highly dynamic multi-hop, found in hostile environments (with losses and / or noise) and connectivity is sporadic, automatically creates and adapts to changes, it multilayer within telecommunications networks (physical layer, data link layer, network layer, transport layer, etc.), the network layer needs to calculate the trajectories of a way to keep communication efficiency when changing the bandwidth links is a luxury, a key assumption is that not all nodes can communicate directly with each other and applications must be designed to handle the disconnection and reconnection maintaining stability.

Figure 2-1: Graphical Representation of an Ad-Hoc Network

.

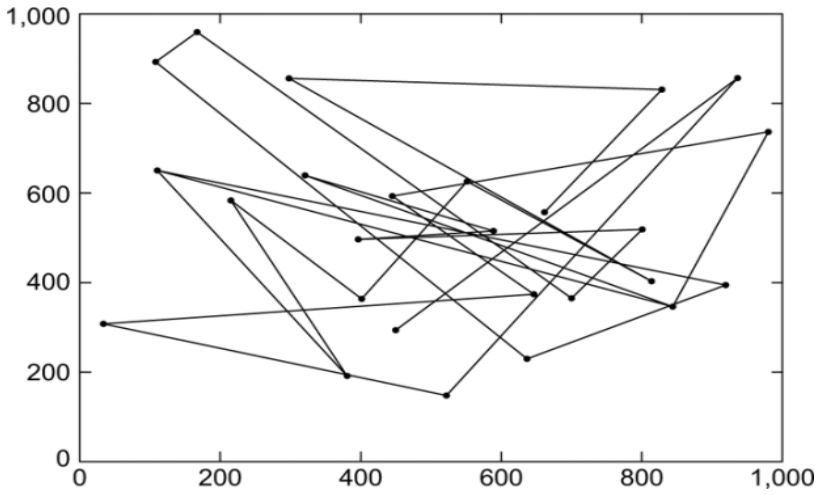


2.3 Mobility Models

A MANET mobility model is the algorithm that describes the behavior nodes with Ad-Hoc network to move within a given area. Some of the models in the literature are: Random Waypoint, Gauss-Markov mobility model city and group mobility model with benchmark [109]. For this research will be chosen Random Waypoint (RWP) to implement in the simulations will be developed later, as this model represents many real situations MANET

implementations. The RWP model has been extensively studied and in the literature there are some variants of it, however we will use the algorithm that consists of the following:
Each node in the network to move is in a pause between changing direction and speed. Each node starts at a random location with a long pause. After the break expires the node chooses a random destination and speed. It moves with the speed set to the destination chosen. Upon arriving begins again with a random break and returns to chooses a random destination and speed.

Figure 2-1: Random Waypoint Mobility Model (RWP).



2.4 Types of Routing Protocols

Generally there are several taxonomy proposals for the classification of routing protocols in Ad-Hoc networks [98]. However, the most used is the one where the protocols are divided into three groups: proactive, reactive and hybrid [98].

Proactive protocols maintain a route to all nodes, even when not needed at the time of the communication using the route. Reactive protocols seek the communication path from one node to another on demand and not stored as proactive protocols, it seeks better use of bandwidth. Finally, hybrid protocols mix the functionality of proactive and reactive protocols defining hierarchies between the nodes of the network and maintaining information on the status of local topology.

There are many proposals that can be listed in the history of research on routing protocols for ad hoc networks. However, at present only speak of three proposals that have been maintained despite the stiff competition. These proposals are:

- "Ad-Hoc On Demand Distance Vector" (AODV) [91]
- "Dynamic Source Routing for Protocol Mobile Ad- Hoc Networks" (DSR) [99]
- "Optimized Link State Routing Protocol" (OLSR) [100]

AODV and DSR use reactive routing also known as on-demand routing. The disadvantage of reactive protocols is in the initial delay of having to discover the route per demand which may affect interactive applications that require QoS, such as interactive audio and video. However, the use of a scarce resource such as bandwidth is optimal.

OLSR uses proactive routing. The disadvantage of such protocols is the level of network overhead; however, they can select valid routes almost immediately.
For this research we use the reactive protocol AODV.

2.4.1 AODV (Ad-Hoc On Demand Distance Vector)

It consists of a reactive or on-demand protocol [91], that is to say find a route only when needed, based on distance vector routing [101], which avoids the problems of count to infinity and the formation of loops. For control, use sequence numbers for each of the destinations, so only maintains routes to nodes with which it maintains active communications. In the nodes, the routing table stored for a limited time each of the entries, so if that time expires the routes are eliminated and must restart a new route search process for the destination, each entry has an associated sequence number which is used to check how new is the path and thereby avoid loops.

2.4.1.1 Operation

When is needed a route from a source node (Source) to a destination node (Destination), it floods the network with requests RREQ (Route REQuest) from the source. When a RREQ reaches the intended destination or any node that knows a route to the destination,

it generates a response RREP (Route Reply). The RREP knows how back to the source as the flooding of RREQ was created way back. When the RREP is going back to the source, it creates the way there. Once the source has received the RREP, you can send datagrams, which will follow the path round to the destination.

2.4.1.2 Features

a) Each node has a routing table.

b) Although the topology changes, an individual route is a time to live (TTL).

c) Hop by Hop Routing.

d) Each router decides the next hop only.

e) No node has a complete graph of the network.

f) For each possible destination only known where the first jump and the distance should be directed to the one found.

g) Use of a destination sequence number for each entry in the routing table. This number is created by the destination node.

h) The sequence number included in a RREQ or a RREP packet is sent to applicants. Guarantees do not remain in loops and is simple to program. They are used by other nodes to determine how new the routing information is. If a node has the possibility to choose between two routes to a destination, a node must choose the one that has the highest sequence number.

i) The information has just expired, typically after a few seconds.

j) Each node maintains information about its neighbors with periodic HELLO messages, TTL = 1.

k) Each node maintains routing information live (active).

l) If a change in the neighborhood affects a living path, an error is reported to generate new searches

2.4.1.3 RREQ message contains

a) Request ID (for flood control).

b) IP address of the destination.

c) Sequence number.

d) TTL.

2.4.1.4 RREP message contains

a) Destination IP address

b) Prefix Size

c) Destination Sequence Number

d) The next hop IP address

e) Lifetime (expiration or deletion time of the route)

f) Number of hops (to reach the destination)

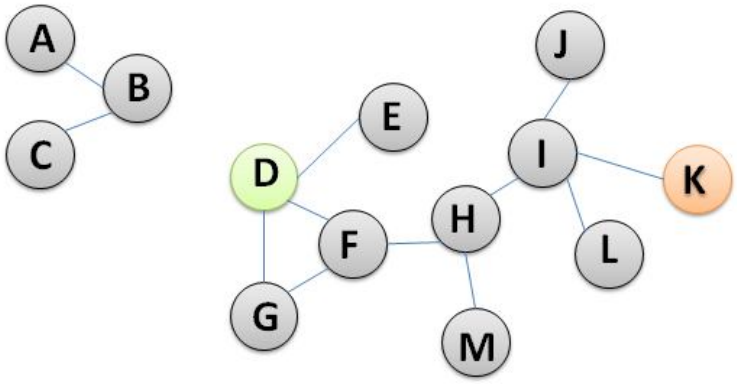
g) Network interface

h) Other state and routing flags (valid, invalid).

2.4.1.5 Example

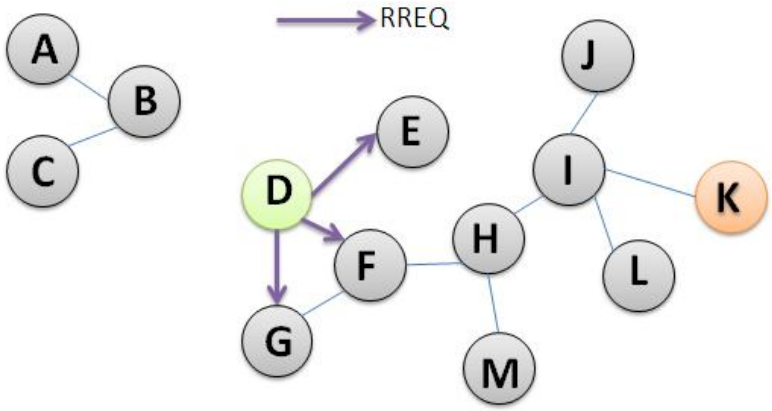
Step 1: D wants to communicate with K

Figure 2-1: AODV Step 1



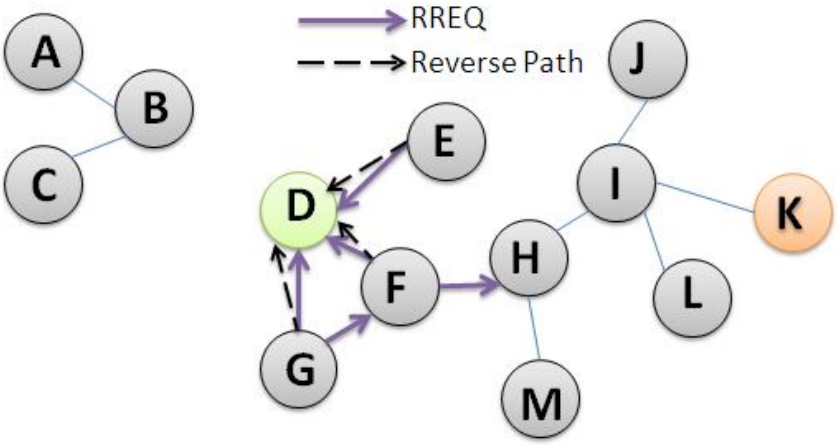
Step 2: The node D sends a message all its neighbors RREQ to find a route to the destination K.

Figure 2-2: AODV Step 2.



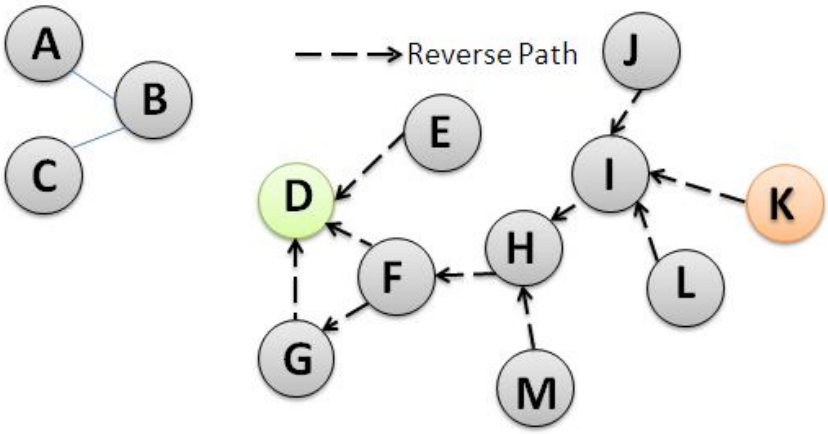
Step 3: Each node receiving the RREQ sends a copy of the route (Reverse Path) for the node.

Figure 2-3: AODV Step 3.



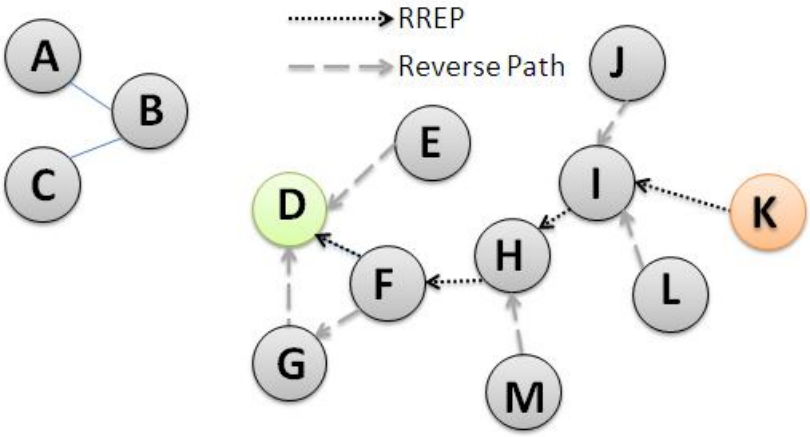
Step 4: A path can be determined when the RREQ reaches a node that provides access to the destination (can be the destination node itself).

Figure 2-4: AODV Step 4.



Step 5: The path is made available by sending back a RREP message from K and written on that route in the routing table D. After receiving the response from the road each node has to update its routing table if the sequence number is more recent.

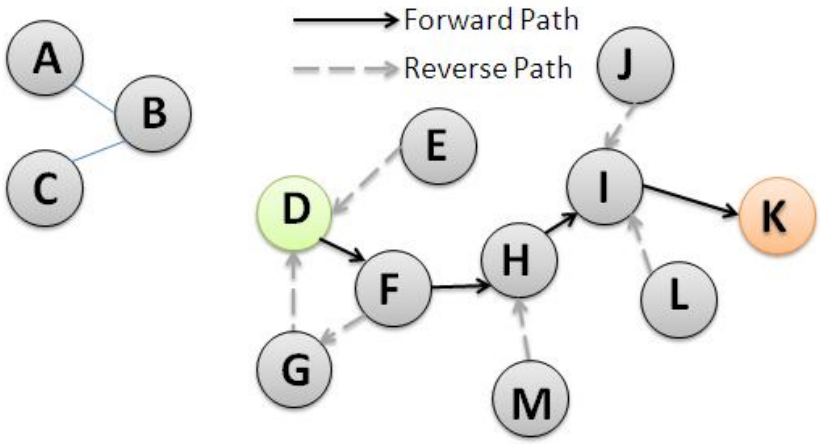
Figure 2-5: AODV Step 5.



Step 6: Then, node D can now communicate with node K

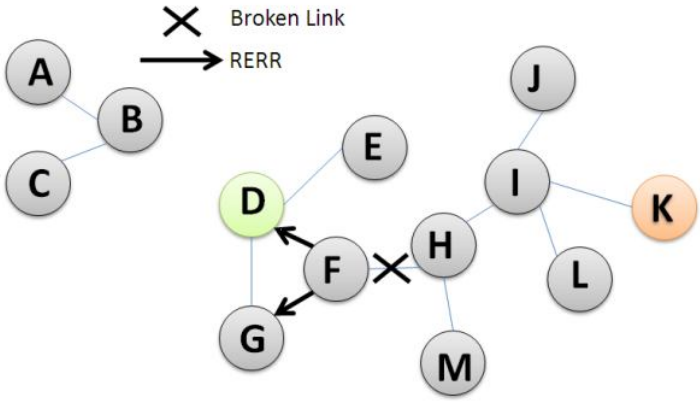
Figure 2-6: AODV Step 6.

.



When it detects a link break in an active route overrides this and sends a route error message RERR (Route Error) to other nodes. If the nodes have a route in its routing table with this link, the route is cleared. The node D sends back a route request to its neighboring nodes, or node on the path may try to find a route to K. This mechanism is called Local Route Repair (Figure 2-9).

Figure 2-7: AODV - RERR Message.



2.4.2 AODV: Advantages Over Other Routing Protocols

Within the study of performance comparison between different routing protocols for ad hoc networks, we found certain advantages in reactive protocols in sending information in [1], [102] and [103]. One such feature is the high adaptability of the protocol in different mobility models found in Ad-Hoc network. Also, by its nature reactive saves Energy and Bandwidth on the network, resources that are vital and scarce in these networks.

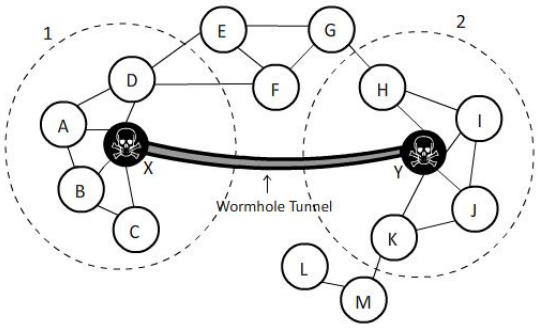
2.5 The Wormhole Intrusion

2.5.1 Definition

A Wormhole is an attack against the routing protocol [2] in a MANET where two or more nodes create the illusion that two remote regions of the network are directly connected through nodes that appear to be neighbors, but they are actually distant to each other [13]. This shortcut is created by connecting the apparent neighbors through a secret communication channel or tunnel, which is generated by an attacker that introduces transceivers connected to each other with a high quality, low-latency link [4]. In this way, the attacker takes the transmitted packets in one region and reinsert them into another region.

As shown in Figure 2.10: X and Y represent the Wormhole nodes connected through a tunnel that creates the illusion that region 1 and region 2 are directly connected, making believe that “A” is a neighbor node of “J”.

Figure 2-1: Intrusion in Ad-Hoc Network with Wormhole Tunnel.



The attacker is invisible in the upper layers, unlike a malicious node in a routing protocol, which can easily be identified, the presence of the Wormhole and the attackers involved in the endpoints of the tunnel are not visible on the route [3].

2.5.2 Actions That Wormhole Can Perform

There are several negative repercussions for Ad-Hoc networking when a Wormhole attack is successful. The consequences could be, according to [3]:

- Eavesdrop on communication: Process for intercepting packets flowing on the network.

- Spoofing attack: Inject bogus packets, impersonating another sender.

- Record packets: Using eavesdropping on communication, are generated copies of intercepted packets flowing on the network.

- Replay the packets: Passively can re-inserting the packets elsewhere on the network. Actively follow the same process but altering the intercepted packets.

- Unauthorized Access: The malicious node enters to a group or subgroup of nodes, masquerading as a belonging node to the network.

- Disrupt routing: In the route discovery process the attack generates interruption of the normal flow of the protocols in the search for a valid path. One consequence of this attack can be a Sinkhole attack [60] where modifying routing packets and masquerading as a trusted node, the attacker attracts other nodes so that all traffic passes through it, in order to launch after centralized attacks.

- Denial-of-Service (DoS): After having supplanted as reliable nodes that contain valid routes to send packets, malicious nodes discard all messages received and not sent to the destination node. This attack is also known as Black Hole Attack [61].

- Selectively discarding data packets: It is a Black Hole Attack but not drop all the intercepted packages, only some of them. This attack is known as Gray Hole Attack [61].

- Clandestine Traffic Analysis [2]: At a given time t the Wormhole tunnel obtained the traffic statistics from the network to use them against it.

- Creating routing loops [4]: To waste the energy of the network.

The attack directly affects the network routing protocols both reactive and proactive routing. [3].

In Reactive protocols:

According to [3], when the network uses on-demand routing protocols such as AODV or DSR, the attacker can penetrate into the route discovery process tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. The destination node receiving the message RREQ, it answers to attacker who is impersonating a trusted node. Being able to interconnect two different regions of the network, the attacker becomes a preferred node for the route discovery process by making the destination node discards the other received ROUTE REQUEST.

In Proactive protocols:

For protocols such as DSDV, several colluding Attackers can create a tunnel through which pass each advertisement sent by routing nodes within the network. This will make two nodes far apart to believe that they are neighbors. In determining the best number of hops required for communication, the nodes within the network end up relying on colluder nodes and there attacks occur.

According to previous studies, these consequences of the attack could be implemented even if there is a system used for authentication and encryption in the network [2], [3]. That is, ensure that a cryptosystem is not enough to counter a Wormhole attack. This is one of the reasons for doing this study: Analyze these assertions and from them to study the recent implementation of the ECC to verify their behavior to an attack such as Wormhole.

2.5.3 Wormhole Types

Previous studies have been mentioned some classifications of the Wormhole attack.

In [14] Wormhole attack is classified according to its mode of attack and depending on whether the attackers are visible on the route. In [2] Wormhole is classified according to the resources used for the attack.

2.5.3.1 According to its mode of attack

Wormhole is classified as [14]:

- *Wormhole using encapsulation*: Between two colluder nodes a tunnel is generated through which pass the RREQ messages which were received by a Node A which encapsulates the route request and sends it to the other node which decapsulates it and forwards the RREQ.
- *Wormhole Out-of-Band Channel*: Using a long-range directional wireless link or a direct wired link nodes send RREQs between them.
- *Wormhole with High Power Transmission*: A node gets a RREQ, it broadcasts it at a high power level, Any node that hears the high-power broadcasts, rebroadcasts it towards the destination.
- *Wormhole using Packet Relay*: Nodes relay Packets between two distant nodes to convince them that they are neighbors.
- *Wormhole using Protocol Deviations*: Nodes do not back off to let the request packet it forwards arrive first at the destination.

2.5.3.2 Depending on whether the attackers are visible in the path

Wormhole is classified as [14]:

- *Open Wormhole Attack*: The attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.
- *Half open Wormhole Attack*: One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.
- *Closed Wormhole Attack*: The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet from one side of wormhole to another side and it rebroadcasts the packet.

2.5.3.3 Depending on the resources used for the attack

Wormhole is classified as [2]:

- *Out-of-band wormholes*: The colluder nodes establish a direct link between the two end-points of the wormhole tunnel in the network. This link is established using an external wired link or a long-range wireless transmission. This type of attack is also known as Hidden Wormhole Attack [15], using only hardware introduced by the attacker and without compromising any hosts in the network. The “Out-of-band” concept initially was introduced in [3].
- *In-band wormholes*: An in-band wormhole does not require any additional hardware infrastructure. It consumes existing communication medium capacity for routing the tunneled traffic. Thus, the belonging nodes on the network will be involved in the attack. The “In-band” concept initially was introduced in [13] although it has been studied in another as [16], [17] and [18]. According to [13], this type of attack is subdivided into 2 types: Self-contained in-band wormhole and Extended in-band wormhole.
- *Self-contained in-band Wormhole*: Is a subtype of “In-band wormhole”. Using the resources of the network and involving other nodes within the network, intruders create a false link between the attacker nodes themselves.
- *Extended in-band Wormhole*: Also known as Exposed Wormhole Attack [15] and also known as Byzantine Wormhole Attack [19], is another subtype of “In-band Wormhole”. Creates a wormhole that extends beyond the attackers forming the tunnel endpoints. A false link is advertised between two nodes that are not the attacker nodes.

2.5.4 Proposed Solutions Against The Wormhole Attack

The proposed solutions to counter the Wormhole attack are based on the symptoms that may suffer a network with the presence of a tunnel. According to [20] some of these Symptoms may be:

- Longer propagation time than generally expected one
- Larger delay per hop than any other usual route
- Bigger transmission range than that of normal node
- Previous node that is not a neighbor

Based on these symptoms [20], knowing that the tunnel is an attack against the routing protocol in the network [2], and taking the related works mentioned in [25], [26] and [27], we classify the proposed solutions against Wormhole attack in:

- Location-based, Distance-based and Time-based
- Hop-Count Analysis
- Graph-based and Geometric-based
- Neighbor monitoring-based
- Statistical
- Key-based

2.5.4.1 Location-based, Distance-based and Time-based

That kind of proposals are based on clock synchronization, flags or marks on packets and use of additional hardware such as GPS, ultrasound or antennas in order to analyze geographic location of nodes in a network, measuring the distance between transmitter and receiver, and measurement transfer latencies of the packets to determine speed of reception and communication and to catalog some as suspicious that they are possibly Wormhole tunnels. Among the solutions are: [3], [4], [9], [10], [15], [19], [21-24].

2.5.4.2 Hop-count Analysis

These are proposals that examine the number of hops that requires transmission of a packet from a source node to a destination node in order to analyze the probability of a Wormhole attack when the number of hops is unusual. Among the proposals are: [28] and [29].

2.5.4.3 Graph-based and Geometric-based

These solutions propose to construct graphical models of network links based on the transmission range of nodes, in order to determine what types of communications are allowed and which not, based on a graphic model or geometric pattern. Some of them are: [5], [8], [27], [30-33].

2.5.4.4 Neighbor monitoring-based

Is the analysis of the behavior of neighboring nodes, when each belonging node on the network participates in the routing process, where is validate in their routing lists, the confidence level of the neighbor node with whom it is communicating. Among the solutions are: [8], [20], [34], [35], [36], [37].

2.5.4.5 Statistical

Proposals are described as through statistical analysis based on calculating the number of routes generated during routing with the frequency of occurrence of these can be detected in the observation of unusual behavior to the possible existence of a Wormhole tunnel. Some of these proposals are: [38], [39].

2.5.4.6 Key-based

Proposals are based on authentication between nodes that require additional geographic component to determine the location of the nodes and to identify possible locations between authentication and intrusion. An example is: [40] (Note that this type of authentication solution requires additional security component).

2.6 Elliptic Curve Cryptography (ECC)

2.6.1 Definition

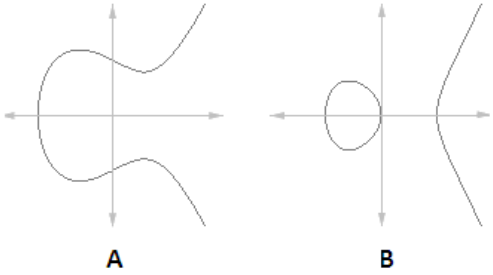
An Elliptic Curve Cryptosystem (ECC) [44] is a public key system based on Diffie-Hellman methods and Digital Signature Algorithm (DSA), but instead of using whole numbers as the symbols of the alphabet of the message to digitally sign or encrypt, uses points in a mathematical object called Elliptic Curve.

An elliptic curve is a plane curve defined by a cubic equation (third degree) as:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \quad (1)$$

For example, a representation of an elliptic curve over the field of real numbers ($\mathbb{R}$) would be:

Figure 2-1: Elliptic curves over the field $\mathbb{R}$.



Where the curve A is the representation of equation (1) with $a_1=a_2=a_3=0;\ a_4=-1;\ a_5=1$ and curve B is the representation of equation (1) with $a_1=a_2=a_3=a_5=0;\ a_4=-1$, ie:

Curve A: $y^2 = x^3 - x + 1$ Curve B: $y^2 = x^3 - x$

According to [48] there are some preliminary considerations to be taken into account before implementing the Elliptic Curve Digital Signature Algorithm (ECDSA), however in this review we shall take them in general for any application of ECC. Considerations involve choosing:

1. A Type of underlying finite field $\mathbb{F}_q$ ($\mathbb{F}_p$ or $\mathbb{F}_{2^m}$).

2. A Field representation (Polynomial or Normal Basis for $\mathbb{F}_{2^m}$).

3. A Type of elliptic curve *E* over $\mathbb{F}_q$ (Random curve or Koblitz curve).

4. An Elliptic curve point representation (Affine Coordinates or Projective coordinates).

2.6.2 The Finite Field In ECC

An elliptic curve with an appropriate arithmetic Cryptography usually defined on two fields [45]:

- The prime finite field $\mathbb{Z}_p$ over the $\mathbb{Z}$ numbers where p is an odd prime and the field $\mathbb{Z}_p$ containing p elements.
- The binary finite field $\mathbb{F}_{2^m}$ containing 2^m elements, with $m \geq 1$.

A field $\mathbb{F}_q$ is a finite field when $q = p^m$, where p is prime [48]. The order of the field is of q elements. $\mathbb{F}_p$, $\mathbb{F}_2^m$, and $\mathbb{F}_p^m$ where p is prime are called Galois Fields (GF), or also known as $GF(p)$, $GF(\mathbb{F}_2^m)$, and $GF(\mathbb{F}_p^m)$, respectively. In a field $\mathbb{Z}_p$, an elliptic curve E over $\mathbb{Z}_p$, denoted $E(\mathbb{Z}_p)$, is defined by the equation of the form:

$$y^2 \equiv x^3 + ax + b \ (mod\ p) \quad (2)$$

where p is an odd prime, and $a, b \in \mathbb{Z}_p$, satisfy:

$$4a^3 + 27b^2 <> 0 \ (mod\ p) \quad (3)$$

Denote now an extra point on the curve at an infinitely place above the vertical axis and that is the identity of the elliptic curve group, such that added it to any point P results the point P. This point is called the *point at infinity* O.

Thus the set $E(\mathbb{Z}_p)$ with point O is the set of all solutions or points $P = (x,y)$, for $x,y \in \mathbb{Z}_p$ that satisfy the equation (2).

On the other hand, taking the finite field of Galois $\mathbb{F}_2^m$, which consists of the two elements 0 and 1, with $m \geq 1$ an elliptic curve E (not supersingular) over $\mathbb{F}_2^m$, denoted $E(\mathbb{F}_2^m)$, is defined by the equation of the form:

$$y^2 + xy = x^3 + ax^2 + b \text{ on } \mathbb{F}_2^m \quad (4)$$

where $a, b \in \mathbb{F}_2^m$, $b \neq 0$ on $\mathbb{F}_2^m$ and $E(\mathbb{F}_2^m)$ is the set of all solutions or points $P = (x,y)$, for $x,y \in \mathbb{F}_2^m$ that satisfy the equation (4), with the *point at infinity* O.

The elements of a finite field $\mathbb{F}_2^m$ with $m \geq 1$ can be represented by all binary polynomials of degree $\leq m - 1$ as follows [48]:

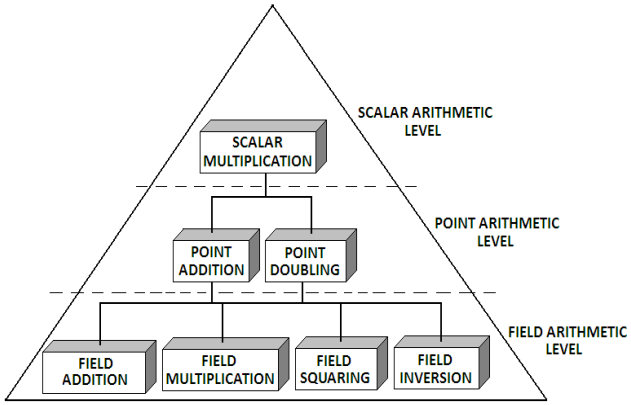
$$\mathbb{F}_{2^m} = \{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 | a_i \in \{0,1\}\} \quad (5)$$

This representation makes these fields are very useful for applications in cryptography, since its elements fit neatly into a data word length of m bits of the form $(a_{m-1}a_{m-2} \ldots a_1a_0)$. For example a point $A \in \mathbb{F}_2{}^4$ is a 4-bit binary word such that $A = (a_3a_2a_1a_0) \neq (0000)$.

2.6.3 Computational Levels and Field Representation

According to [44], the structure of an ECC operation has three computational levels:

Figure 2-12: Computational levels of an ECC.



- *Scalar Arithmetic Level*: In this computational Level the Scalar multiplication algorithm is applied. The scalar multiplication calculation is kP where k is a positive integer and P denotes the point that is added k copies to itself.

$$kP = \sum_{i=1}^{k} P \quad (6)$$

- *Point Arithmetic Level*: In this computational Level point addition and point doubling operations are applied. Point addition is to take two points P and Q of the curve and add them, resulting in a third point as follows:

$$P + Q = R \quad (7)$$

Point doubling is to add two times the same point P:

$$2P = R \quad (8)$$

Point Doubling is a special case of the sum, because is the addition of a point to himself. However it is defined independently to optimize its implementation.

In the top layer computation of ECC, the scalar Multiplication requires multiples calculations of the Point addition $(P \neq Q)$ and Point doubling $(P = Q)$. This procedure is the pillar on public key cryptography using elliptic curves. Let P and Q two points of the elliptic curve with $P = (x_1 , y_1)$ and $Q = (x_2 , y_2)$. The result of adding $P + Q = R = (x_3 , y_3)$ is obtained from the following equations:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad (9)$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \quad (10)$$

$$\lambda = \begin{cases} \dfrac{y_2 + y_1}{x_2 + x_1} & , \quad P \neq Q \\ \dfrac{y_1}{x_1} + x_1 & , \quad P = Q \end{cases}$$

There is another operation on this computational level called point tripling. According to [41] in the effort of some approaches to compute faster scalar multiplications, such as ternary/binary method [46] and double-base chain [47] was introduced the point tripling operation.

Point tripling is to add three times the same point P:

$$3P = R \quad (11)$$

- *Field Arithmetic Level*: In this computational Level is important to differentiate the $\mathbb{F}_q$ finite field ($\mathbb{F}_p$ or $\mathbb{F}_{2^m}$) to which operations are applied and depending on the field, the basis representation being used for that field. In this computational Level the addition, multiplication, squaring and inversion field operations can be applied.

For example, for the Finite Field $\mathbb{F}_2{}^m$ the multiplication rule depends on the basis selected [48], and usually are taken two kinds of bases: Polynomial Bases and Normal Bases (within the latter is the implementation: Gaussian Normal Bases – GNB of ANSI X9.62 [48]).

To minimize the explanation of this computational level we take only finite field $GF(\mathbb{F}_2{}^m)$ with $m \geq 1$,and with a Polynomial Bases representation. For further details of the arithmetic of this computational level to know the operations applied on $GF(\mathbb{F}_p)$ and $GF(\mathbb{F}_2{}^m)$, and according to the Basis Representation of $GF(\mathbb{F}_2{}^m)$, to know the operations applied on Polynomial Bases and Normal Bases, is suggested deepen in [44] and [48].

Previously we had shown the representation of field elements in $\mathbb{F}_2{}^m$ with a Polynomial Basis Representation in (5), where we said that a field element is usually denoted by the bit string of the form $(a_{m-1}a_{m-2} \ldots a_1a_0)$.

In this field $(GF(\mathbb{F}_2{}^m))$, with this Basis Representation (Polynomial) operations that can be applied are: addition, multiplication and inversion [48].

- *Addition*:

The sum of two elements $A, B \in GF(\mathbb{F}_2{}^m)$ with:

$A = (a_{m-1}a_{m-2} \ldots a_1a_0)$ and $B = (b_{m-1}b_{m-2} \ldots b_1b_0)$ is equal to:

$A + B = C = (c_{m-1}c_{m-2} \ldots c_1c_0)$

where $c_i = (a_i + b_i) \ mod \ 2$

- *Multiplication*:

The Multiplication of two elements $A, B \in GF(\mathbb{F}_2^m)$ with:

$A = (a_{m-1}a_{m-2} \dots a_1a_0)$ and $B = (b_{m-1}b_{m-2} \dots b_1b_0)$ is equal to:

$A \cdot B = r = (r_{m-1}r_{m-2} \dots r_1r_0)$ where the polynomial:

$$r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \cdots + r_1x + r_0$$

is the remainder when the polynomial

$$(a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0) \cdot (b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0)$$

is divided by an irreducible polynomial $f(x)$ of degree m over $\mathbb{F}_2$ such that:

$$f(x) = x^m + f_{m-1}x^{m-1} + f_{m-2}x^{m-2} + \cdots + f_2x^2 + f_1x + f_0$$

Where $f_i \in \{0,1\}$ for $i = 0,1,\dots,m-2,m-1$

- *Inversion*:

The inversion of an element $A \in GF(\mathbb{F}_2^m)$ denoted A^{-1} with:

$A = (a_{m-1}a_{m-2} \dots a_1a_0)$ and $A \neq 0$ in $\mathbb{F}_2^m$ is the unique element $C \in GF(\mathbb{F}_2^m)$ for which $A \cdot C = 1$.

2.6.4 Domain Parameters and Types of Elliptic Curves

Domain parameters of elliptic curves are the basic values needed to define the finite field to use. In general, [49] describes the Elliptic curve domain parameters over $\mathbb{F}_p^m$ like an octuplet:

$$T = (p, m, f(x), a, b, G, n, h)$$

a) p and m specifying the finite field $\mathbb{F}_p{}^m$

b) An irreducible polynomial $f(x)$ of degree m to determine the representation of $\mathbb{F}_p{}^m$

c) Two elements a, $b \in \mathbb{F}_p{}^m$ specifying the elliptic curve $E(\mathbb{F}_p{}^m)$, defined by the equation: $E: y^2 = x^3 + ax + b$ in $\mathbb{F}_p{}^m$

d) A base point $G = (x_G, y_G)$ on $E(\mathbb{F}_p{}^m)$

e) A prime n which is the order of G

f) An integer h which is the cofactor $h = \#E(\mathbb{F}_p{}^m)/n$.

More specifically we can define the domain parameters over $\mathbb{F}_p$ and $\mathbb{F}_2{}^m$ [50], [51].

2.6.4.1 Curve Domain Parameters over $\mathbb{F}_p$

The parameters that define the domain of elliptic curves over $\mathbb{F}_p$ [50] are a sextuple of the form:

$$T = (p, a, b, G, n, h)$$

These parameters already explained previously generally. For T, the curve $E(\mathbb{F}_p)$ is defined by the equation (2).

2.6.4.2 Curve Domain Parameters over $\mathbb{F}_2{}^m$

The parameters that define the domain of elliptic curves over $\mathbb{F}_2{}^m$ [50] are a septuplet of the form:

$$T = (m, f(x), a, b, G, n, h)$$

These parameters have already been explained previously in a general way. For T, the curve $E(\mathbb{F}_2{}^m)$ is defined by the equation (4).

To see the detail of the generation and validation of these domain parameters for curves over $\mathbb{F}_p$ and over $\mathbb{F}_2{}^m$ see [50].

In [52] NIST presented a list of 15 elliptic curves that were recommended for U.S. Federal Government use. This revised standard is called FIPS 186-2. NIST describes that when choosing appropriate curves must take into account two types: *Pseudo-random curves and Special curves.*

- *Pseudo-random curves*

Are those whose coefficients are generated from the output of a seeded cryptographic hash. If the seed value is given along with the coefficients, it can be verified easily that the coefficients were indeed generated by that method [52].

- *Special curves*

Whose coefficients and underlying field have been selected to optimize the efficiency of the elliptic curve operations [52].

According to [52], elliptic curves suitable for ECC taking into account the finite field $GF(\mathbb{F}_q)$ can be: Pseudo-random curve over $GF(\mathbb{F}_p)$, pseudo-random curve over $GF(\mathbb{F}_2^m)$and special curve over $GF(\mathbb{F}_2^m)$ called a Koblitz Curve or Anomalous Binary Curve. For more detail see [52].

2.6.5 Elliptic Curve Point Representation

One problem faced by the ECC in the direct calculation of equations (9) and (10) of the *Point Arithmetic Level* is that to obtain the sum of points is necessary to calculate two field inversions, which is a very expensive operation since computational point of view considering that is ten times more expensive than a multiplication. To avoid the use of field inversions, the representations of points called Projective Coordinates are used.

The Affine Coordinates are those such that each point in the coordinate system is represented by the vector (x, y). The Projective Coordinates system is a system representation of Affine Coordinates creating an equivalence relation of a point using three coordinates X, Y, and Z of the form $(x,y,z)\sim(X,Y,Z)$. According to [46] the equivalence class containing (X,Y,Z) is:

$$(X : Y : Z)=\{(\lambda^c X , \lambda^d Y, \lambda Z) : \lambda \epsilon GF(\mathbb{F}_2{}^m)\}$$

$(X : Y : Z)$ is called a Projective Point, and (X,Y,Z) is called a Representative Point of that class. $(X : Y : Z)$ with $Z \neq 0$ corresponds to the affine coordinates $x = X/Z^c$ and $y = Y/Z^d$ where the fixed exponential integers c and d over $GF(\mathbb{F}_2{}^m)$ will determine the characteristics of the arithmetic of elliptic curves and therefore the definition of the algorithm of addition of points in this representation.

There are several types of projective coordinates [54], [55], [56], [57]. A Projective Coordinates (X,Y,Z) corresponds to an Affine Coordinates (x,y) as follows:

- *Ordinary Projective or Homogenous Projective*: with $c=1$ and $d=1$ where:

$$(x,y) =(X/Z , Y/Z).$$

- *Jacobian Projective*: with $c= 2$ and $d= 3$ where:

$$(x,y) =(X/Z^2 , Y/Z^3).$$

- *Lopez –Dahab Projective*: with $c= 1$ and $d= 2$ where:

$$(x,y) =(X/Z , Y/Z^2).$$

- *ML–Projective*: A Projective Coordinates (X,Y,Z,T) with $T= Z^2$, $c= 1$ and $d=3$ where:

$$(x,y) =(X/T , Y/Z^3).$$

For example, in Ordinary or Homogenous Projective Coordinates, the curve equation (1) can be expressed as:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$$

And in Lopez – Dahab Projective Coordinates the curve equation (1) can be expressed as:

$$Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4$$

To know the operations applied to different projected coordinate systems is recommended to see [54], [55], [56], [57].

2.7 ECC Implementations for MANET (Related Work)

2.7.1 ECC Schemes

As mentioned above, an Elliptic Curve Cryptosystem (ECC) is based on the methods of Diffie-Hellman and Digital Signature Algorithm (DSA). These in turn are based on the Discrete Logarithm Problem (DLP) [62]. The problem is finding an integer x such that $\alpha^x = \beta$ that is, in general, the definition of GDLP (Generalized Discrete Logarithm Problem). Thus the Elliptic Curve Discrete Logarithm Problem (ECDLP) based on the DLP consists of an elliptic curve E on $\mathbb{F}_q$, a point $G \in E(\mathbb{F}_q)$ of order n (odd and large number) and a scalar multiple Q of G, to find an integer k such that: $Q = kG$ (see Scalar Multiplication in the section 2.6.3 of this document). This is a difficult problem to solve, also allows all the DLP-based cryptosystems can be adapted using elliptic curves [63].

According to [63]: The Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme is a variant of the Diffie-Hellman key agreement protocol. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA). The Elliptic Curve Integrated Encryption Scheme (ECIES) is a public-key encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks, also known as the Elliptic Curve Augmented Encryption Scheme (ECAES) or simply the Elliptic Curve Encryption Scheme.

Other extensions as shown in [43] are: The Group Elliptic Curve Diffie-Hellman (GECDH) protocol which is an extension of GDH based on ECDLP, and Tree-based Group Elliptic Curve Diffie-Hellman (TGECDH) which is a variant of TGDH based on ECDLP.

2.7.2 Key Establishment Process

The process by which two or more entities (in our case Ad-Hoc nodes) establish a shared secret key (session key) in order to be used to achieve some cryptographic goals, such as confidentiality or data integrity is called: Key Establishment Process [58].

We can classify the Key Establishment Process by its distribution, or by the prior information that each entity has before starting the process:

2.7.2.1 By its distribution

The key distribution problem in MANET is the problem of how to set up secret keys between communicating nodes [59]. There are two possible modes of distribution: *Key Transport* and *Key Agreement*.

- *Key Transport Protocols*: A key is generated by one entity sometimes called CA (Certificate Authority) and then is transmitted through a secure channel to a second entity [58]; this mode of distribution is also known as Key Management.

- *Key Agreement Protocols*: Also known as *Key Exchange Protocols* both parties perform a negotiation process in order to contribute information to generate and exchange a secret key.

2.7.2.2 By the prior information

There are two possible modes of Key Establishment: Symmetric and Asymmetric protocols.

- *Symmetric Protocols*: The two entities have from the beginning of the process common secret information for the establishment of the key.

- *Asymmetric Protocols*: The two entities involved only share public information that has been authenticated previously.

2.7.3 Why ECC in MANET?

There are many reasons why there have been introduced the concept of ECC in MANET. According to [11] and [41], Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

In [42], it is shown how the energy cost for RSA is greater than that of an ECDSA (a Signature Algorithm of ECC) showing better performance.

However, in [43] although it is recognized that attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead, also is showed that: the methods for computing general elliptic curve discrete logarithms are much less efficient than those for factoring or computing conventional discrete logarithms and it indicates that more computation time is required for ECC and considers that the overall performance of ECDLP-based applications needs to be evaluated.

However, compared to many other conventional cryptosystems, ECC is a very good alternative to the characteristics of a MANET.

2.7.4 ECC Proposals Applied to MANET (Related Work)

There are several proposals based on ECC that advertise to guarantee security in Ad-hoc networks. The proposals focus their research on ECC according to certain features in MANET. We can classify the proposals: by the organization of the nodes in the network, by the Key Establishment Process and by the use of MANET as a way of implementation and improvement of ECC.

2.7.4.1 By the organization of the nodes in the network

This is one of the features that take into account the proposals based on ECC due to dynamic network topology. For example [64] presents an organization of the nodes through a *Region-Based Group*, where a group of nodes in a region, which in turn is divided into sub-groups that are responsible for keeping your keys using GECDH Protocol and links with other subgroups in a tree structure using TGECDH protocol with nodes which are assigned tasks of communication management. A similar organization is found in [65] based on networks Near Term Digital Radio (NTDR) presents an organization *Cluster-based* where all mobile nodes are divided into different clusters controlled by clusterheads and with two Classes of communication intra-cluster and inter-cluster using ECC. Other *Cluster-based* proposals using ECC are [66], [67]. Another organizational scheme is the proposed *Self-Organization* [68] where each node of the network after establishing key groups and subgroups, operates synchronously regular updating of their keys in order to let in new members to the network. Another type of organization applied in MANET using ECC is the Threshold Cryptography as in [69] where no one has the complete key, but there are a number of nodes t (t = Threshold) with a piece of this and the t nodes are required to encrypt and/or decrypt a message. Another proposal that uses Threshold based on ECC is [70].

2.7.4.2 By Key Establishment Process

When implementing ECC in MANET, the Related Works focus on the type of Key Establishment Process to use, which we studied earlier in this document (section 2.7.2.). Some proposals use Key Management Protocols as in [71] with Cluster-based organization, or [70] with Threshold organization. Another proposals applying ECC in MANET with Key Management are: [72], [73], [74], [75], [76], [77]. Some proposals use Key Agreement Protocols as [78] that seeks resist the off-line password guessing attack, others simply apply ECDH in its Key Agreement Protocol as [79]. Other proposals applying ECC in MANET with Key Agreement are [64] and [80].

2.7.4.3 By the Use of MANET as a Way of Implementation and Improvement of ECC

Some proposals study the application of software libraries to implement ECC on MANET as [63] and [81]. In [82] is presented a fuzzy controller for a dynamic window sizing to optimize the calculation of an ECC scalar multiplication and evaluate their performance in MANET. In [83] is sought through the code development over some microcontrollers the optimization faster implementation of an ECC in MANET. In [42] is compared the application of ECC versus RSA in MANET in order to observe their strengths and in [59] shows how some ECC implementations have some limitations on MANET performance.

2.8 ECC Implementation During Wormhole Attack In MANET

2.8.1 Security Requirements In MANET

In order to combat passive and active attacks [84], according to [85] a secure Ad-hoc network is expected to meet the following different security requirements:

- *Confidentiality:* Only the intended receivers should be able to interpret the transmitted data.
- *Integrity*: Data should not change during the transmission process, i.e., data integrity must be ensured.
- *Availability*: Network services should be available all the time and it should be possible to correct failures to keep the connection stable.
- *Authentication*: Every transmitting or receiving node has its own signature. Nodes must be able to authenticate that the data has been sent by the legitimate node.
- *Non-repudiation*: Sender of a message shall not be able to later deny sending the message and that the recipients shall not be able to deny the receipt after receiving the message.

And [86] adds another requirement:

- *Access and usage control:* Access control makes sure that access to information resource is controlled by the Ad-Hoc networks. Usage control ensures the information resource is used correctly by the authorized nodes having the

corresponding rights. This mechanism provides the ability to control information after it is transmitted.

2.8.2 Aspects to Ensure Security in MANET

In [86] and [87] are proposed three key aspects to be covered by any security policy on Ad-Hoc networks in order to satisfy the aforementioned 6 Security Requirements in Section 2.8.1.

2.8.2.1 Intrusion detection

Intrusion detection based on analysis of network behaviors is defined as a process of monitoring activities in a system which can be a computer or a network to detect anomalies. [104]. The mechanism that performs this task is called an Intrusion Detection System (IDS).

According to [86] the intrusion detection techniques can be classified into misuse detection and anomaly detection.

- *The misuse detection*: Uses patterns of known attacks to match these when they are applied and the IDS to detect. The advantage is that an attack can be detected previously analyzed accurately, but lacks the capacity to detect new attacks. Another disadvantage of this type of IDS is the complexity in modeling patterns of known attacks, due to the dynamic MANET topology.

- *The anomaly detection*: Monitors the behavior of nodes and events generated on the network to detect signs of intrusion. This type of monitoring to detect new attacks, but its main disadvantage is that it can generate false alarms.

2.8.2.2 Secure routing

Establishing a reliable and secure route between each pair of nodes. According to [105] the most common attacks that attack the routing protocols are:

- Attacks using modification
    - Redirection by modifying route sequence number
    - Redirection by modifying hop count

  - Source route modification
  - Tunneling
- Attacks using fabrication
  - Falsifying route errors
  - Broadcast falsified routes
- Spoofing attacks
- Rushing attacks

Establish a secure routing protocol means to counter these attacks on the time to find a suitable route for communication between nodes.

2.8.2.3 Key management service

Generation of authentication, digital signature and encryption of information.

It is important to note that [86] and [88] state that is not enough to implement a Key Management Service, it should be accompanied by the other two types of solutions including network security policies.

2.8.3 Key Management Service Attributes

Returning to the Key Management Service aspect from the three previous Key aspects in section 2.8.2., when applying a security policy in MANET according to [84] a Key Management Service (For Example a: key agreement protocol) must conform to number of desirable attributes:

a) *Known session keys*. A protocol still achieves its goal in the face of an adversary who has learned some previous session keys.
b) *Perfect forward secrecy*. If long-term secrets of one or more entities are compromised, the secrecy of previous session keys is not affected.
c) *Unknown key-share*. An entity (in our case an Ad-Hoc node) cannot be coerced into sharing a key with other entity without its knowledge.
d) *Key-compromise impersonation*. When the secret value is disclosed an adversary that knows this value can now impersonate one entity. Even so, the

opponent to know this information cannot impersonate the entity attempting to supplant.

e) *Loss of information*. Compromise of other information that would not ordinarily be available to an adversary does not affect the security of the protocol.

f) *Message independence*. Individual flows of a protocol run between two honest entities are unrelated.

Additionally, [89] states that in terms of computation load a Key management service should fulfill:

g) *Computational efficiency.* This includes the number of operations required to execute a protocol. In order to achieve this property, the protocol should have the minimum number of operation as possible.

h) *Communication efficiency.* This includes the number of passes (message exchanges) and the bandwidth required (total number of bits transmitted).

2.8.4 Levels of Security Against a Wormhole

Based on [9] and [90] we have developed a model against Wormhole Attack in MANET for establishing different required levels of security against this attack. There are several levels of security that can determine the state that the Wormhole intrusion is. These security levels can be applied in chronological order before, during and after the attack. The idea is to classify these levels in order to determine what strategy to take against a Wormhole. These levels are:

a) *Preventing* (*Avoiding*): Consists of applying one or more strategies to avoid creating a Wormhole tunnel. That is, this level of security is applied when the attack does not exist yet.

b) *Predicting* (*Hypothesizing*): Is the strategy which aims to find by observing suspicious behavior on the network that can lead to detection of an attack. These observations can validate transmission times (latencies), sudden changes in the ways of routing among others.

c) *Detecting* (*Locating*): Once the prediction activities yield positive results from a Wormhole attack, proceeds to locate malicious nodes within the network, identifying their routes, the nodes involved, committed network regions, among others.

d) *Analyzing*: Is the level where it seeks to take action against the detected attack. The strategy to use is of vital importance since it cannot afford to keep going on the attack.

e) *Mitigating* (*Evading*): It is the action which removes the impact of the attack within the network, even if malicious nodes are present within it. The full identification of the attack will lead to the preparation of the nodes to avoid communication with the colluder nodes.

f) *Removing*: Is the level where the Wormhole tunnel, is permanently excluded. The nodes within the network know which of them are malicious, and they do not carry out any task of communication with them. They are excluded from the routing tables and the reliable links in the network are recognized.

2.8.5 Analysis of the Behavior of ECC for the Wormhole Intrusion

As shown in section 2.5.2. of this document, some previous studies have stated that applied to MANET, the cryptosystems are not enough to counter a Wormhole attack. For example [3] states: "*The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys*" or as in the case of [2] where says: "*Also some approaches rely on using source authentication using signing keys. Such defenses can be defeated if a node is compromised and the attacker has access to secured information*".

Let's analyze these assertions*:*

- Is it possible that an ECC is the only efficient way of security within an Ad-Hoc network?: The answer is No [110]. As discussed in this document (Section 2.8.2.): in [86] and [87] must take into account three key aspects when implementing a security policy in Ad-Hoc networks: Intrusion Detection, Secure Routing and Key Management Service. The ECC would be involved only in the Key Management Service process.

- Are the proposed ECC able to satisfy the Security Requirements in MANETs presented in section 2.8.1.?: The only requirements to be satisfy with applied ECC in MANET, are those of Authentication and the Confidentiality, since they are precisely the functions of any cryptosystem in MANET, however, cannot be guaranteed the remaining requirements, being that Wormhole attack directly affects the Routing process [3] and the attacker can carry out Denial of Service (Not would be met Non-repudiation neither Availability), packet alteration (Not would be met Integrity), or Disrupt routing and Spoofing attack (Not would be met Access and usage control).

- Could "the current proposals for ECC" satisfy the Attributes of a Key Management Service (Section 2.8.3.) in middle of a wormhole attack?: The ECC attributes that are affected in a negative way with a Wormhole intrusion are: Key-compromise impersonation, Loss of information and Message independence. As discussed in Section 2.5.2. of this document are precisely the characteristics of the wormhole that affect these attributes. Wormhole is able to impersonate a node pretending to be reliable, to impersonate a node has the ability to share information with members of the network nodes and even participate in a Key Establishment Process. At this point it does lose the Message Independence, because there is communication between a malicious node and a belonging node on the network. Information loss occurs with packet capture by malicious nodes and the attacker's ability to do with them as it pleases. However, revisiting some of the proposals of Related Work some important things can be seen: In [64] can be guaranteed Key-compromise impersonation, considering the organization of the network into groups and sub-groups. This makes the nodes know each other, despite being limited organization considering a node outside the network will make it harder to belong to it, however, prevent the rapid generation of a Wormhole tunnel. In addition, it would satisfy the Computational efficiency and Communication efficiency attributes, because as we saw in Section 2.7.3., the implementation of the GECDH and TGECDH protocols have better performance than other traditional cryptography schemes. In the same way happen with the Cluster-based

organization proposals, e.g.: [65], [66] and [67], such organizations can avoid impersonation given the high level of reliability between neighboring nodes and distrust generated by the entry of a new node to the network, have their advantages and disadvantages.

- The ECC proposals that are applied to MANET Can they perform the actions carried out in the levels of security against Wormhole attack (section 2.8.4.)? The answer is No. The actions and strategies that fall within these security levels are not exactly an ECC task, but an Intrusion Detection System.

- If the ECC application in MANET is not sufficient to offset the Wormhole Attack, Should it be combined with other solutions so that it can be applied? The answer is Yes. As we saw previously an ECC application is part of the Key Management Service, but it requires being mixed with "Intrusion detection Systems" and "Secure routing solutions" to attack the Wormhole intruder. In fact, some proposals that apply ECC in their solutions, combine it with other strategies: For example in [67] it is performed an estimation of trust values of neighbors, a Secure end-to-end route discovery using Antnet routing mechanism is carried out and it is mixed with mutual authentication using ECC. Such combinations prevents many of the actions of a wormhole attack and there is used an ECC.

3. Chapter 3

3.1 Proposed Solution and Justification

To bring a solution to counter the Wormhole attack using Elliptic Curve Cryptography, it is necessary to return to the conclusion in previous chapters on the need to combine three aspects of security in MANET: Intrusion Detection Systems (IDS), Key Management Service and Secure Routing Algorithms (See Section 2.8.2.).

We begin by making a description of the simulator to use and their technical characteristics, then there will be a MANET environment analysis required in the model simulations in terms of mobility, routing protocols, features resources between nodes, number of nodes to simulate Area, time simulation model of data collection and organization of the nodes. Then there will be a description of the proposed solution by combining the three aspects of security: Understanding Using Elliptic Curve Cryptography, Description of Intrusion Detection System to use and justification and choice of secure routing algorithms. Finally, the simulations describe the development, will present the software architecture model and class models.

3.2 MANET Environmental Construction

3.2.1 Simulator Description

We have chosen the simulator NS-2 [106] to build the MANET environment, the intruder and security solution. There is now a NS-3 version of the simulator, but there is more documentation of the NS-2 and as many classes available for MANET environments.

NS-2 is a discrete event simulator targeted at networking research with GNU General Public License, based built in C++ with simulation interface through OTcl. It will run on Windows XP with Cygwin interface on a computer with 2.8 GHz Intel Core i5 Processor

and 4 gigabytes of RAM. NAM tool will be used as a GUI tool simulator and XGRAPH to plot results.

3.2.2 Choice of the System Organization of Network Nodes

As discussed in previous chapters organizing systems Ad-Hoc networks and cluster-based are very safe when analyzing which nodes are part of the network nodes avoiding strangers enter to carry out attacks such as organization maintains a closed nodes with the same participants as well as the use of hierarchies where a Cluster Head node acts as a CA (Certification Authority) and nodes know their subjects. However, this approach does not always serve for any application in Ad-Hoc networks. This approach would be useful for military applications battlefield as we know hardly change hierarchies and similarly there is a dynamic and constantly to expand the number of participants in the network. However, for other applications such as rescue operations, financial transactions, conferences, among others, it is useful to use this type of organization and tightly restricts access to new members who want to be part of the network. Thus we see that the system of organization of the nodes of the network, either through a hierarchical system or one where all nodes maintain the same level of responsibility, are valid, but its use depends on the application of the network.

For this work we decided to develop a solution against the Wormhole attack on networks that do not have a hierarchical organizational system in order to evaluate the performance of the network through a wormhole attack when nodes that are not part of the network wish to enter the same. It also extends the use of ECC using a system based on Threshold Cryptography agreement where all the nodes will have a portion of the private key.

3.2.3 Other Features to Consider For the Solution

Because the behavior of the solution will be tested in a series of simulations is necessary to establish the extent of these by naming the nodes features. Networks will be simulated with a number not more than 200 nodes. Nodes that have the same characteristics simulate each other, with radius equal transfer, bandwidth between nodes the same for

any link, and power capacity, power and memory of the nodes equally among them. I.e. it simulates a homogeneous MANET (the heterogeneous MANET are those in which the nodes have different resource characteristics together). The detail of the physical characteristics of each set of nodes and the type of link that will have each other will be specified later in each simulation run.

Another feature that will ad-hoc networks to be simulated is the routing protocol. For our work we take the well-known and most studied reactive routing protocol AODV.

Another feature to be taken into account in the simulations is the size of the area to simulate and simulation times. The idea is to simulate areas greater than our 5000 square meters with interactions up to 20 minutes.

3.3 Intruder Construction

Wormhole tunnel will be constructed of type Out-of-band (See section 2.5.3.3.) to perform actions of attack Denial-of-Service (DoS) and replay the packets altering the Intercepted packets.

3.4 Design Solution of Detection and Evasion

3.4.1 IDS to Use Against Wormhole

Returning to the earlier study of the solutions that have been raised to counter the attack Wormhole (See Section 2.5.4) based on the analysis of [104] which assesses the performance of intrusion detection systems it is decided to choose for this work a Distributed and Cooperative IDS based on agents monitoring neighboring Anomaly Detection rate [86]. Among the advantages are:

- The level of observation is large since no abnormalities are observed only in the node itself but also on the behavior of neighbors.
- It detects malicious - routing is the first thing that strikes an intrusion Wormhole.
- The use of network resources is low.
- You can detect attacks varied as producing a new wormhole and are not known.

3.4.2 Safe Routing System to Use

The idea is to use the well-known AODV routing protocol [91], however, expanding its functionality without changing it. To do this, take the safe routing protocol AODV: "S-AODV: Secure Ad-hoc On-Demand Distance Vector Routing". [107]. Based on information and non-mutable mutable AODV packets as they travel through the network, this protocol uses two security mechanisms: A digital signature system to authenticate non-mutable information and an implementation of hash chains in order to verify that the hop count of RREQ and RREP messages have not altered by an attacker Been [108]. However, since the idea is to combine the three aspects of security (see Section 2.8.2.), What we do for the digital signature system is to implement an algorithm ECDSA on RREQ routing packets and S-AODV RREP. The implementation of this algorithm will call EC-S-AODV.

3.4.3 Review of the ECC Implementation for the Solution

To mitigate the most of the actions to carry out an attack like Wormhole is necessary to apply an ECC system for authentication, generation/trading public key and digital signature in compliance with the aspect Key Management Service. To this were implemented ECDSA and ECDH protocol in two phases. A first phase as we have seen in the previous section applies where an ECDSA digital signature system on S-AODV protocol when generating the routing process which we call EC-S-AODV. The other phase is the implementation of ECDSA digital signature system for when the last packet RREP has been received successfully by the source node information and begins the process of sending data packets with payload. This will be done using the same public key for the two phases. The key agreement process will be done through the scheme ECDH.

3.5 Summary of the Solution Represented In Simulations

Based on the issues just mentioned the summary of features has the simulations is [111]:

Table 3-1: Summary of features in Simulations.

FEATURE	DESCRIPTION
Simulator	NS-2 Version 2.7
Mobility model	Random Waypoint (RWP)
Routing Protocol	Ad-hoc On-Demand Distance Vector Routing (AODV)
Characteristics of resources between nodes	Homogeneous
Number of nodes	Less than or equal to 200
Area to simulate	Less than or equal to 5000 square feet
Simulation time	less than 20 minutes
Organization of Nodes	Nonhierarchical
Model data collection	stochastic
IDS to use	Distributed and Cooperative agent-based monitoring of neighbors of Anomaly Detection type
Secure routing system to use	EC-S-AODV
Implementation of ECC	ECDSA for digital signature

3.6 List of Simulations

The simulations were performed are:

- Simulation of the mobility model

- Simulation of the routing protocol

- Simulation of Wormhole intrusion

- Simulation of the IDS

- Simulation of the implementation of ECC for authentication, digital signature and key negotiation with the routing protocol secure

- Simulation with the whole scenario

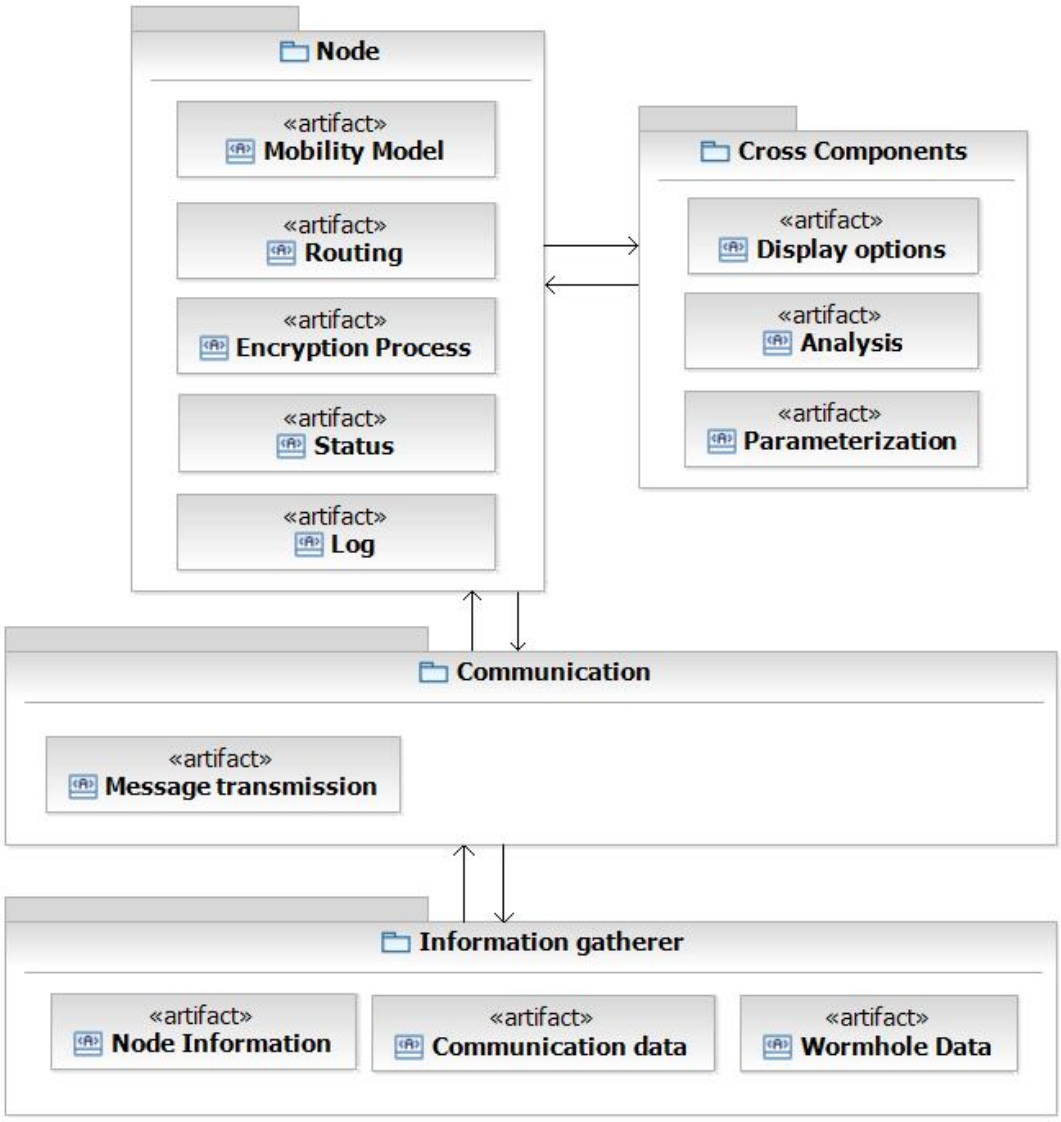
- Other simulations: Zero Knowledge and OLSR routing algorithm

3.7 Solution Architecture

3.7.1 Background of the Solution and Logical Layers

This section shows the analysis of component structure of the solution architecture.

Figure 3-1: Software solution components.



The solution designed contains the following functional components:

- **Node**: is the component that contains the general behavior of the elements of the simulation. Within the same component are inherited routing algorithms, ECC, IDS and the basic characteristics of the nodes.

- **Communication**: is the component that coordinates communication between the nodes. Routing methods communicate directly with this and that is where management is developed to generate messages according to the AODV protocol.

- **Information Collector**: is the component that captures the statistical information from the simulation and writes trace files. These same files are then used to graph the results.

- **Transverse component**: The component that handles the basic configuration of the environment and visual manager of it.

3.7.2 Random Waypoint - Class Model

Below is the class model of RWP mobility model used. Java was initially designed as shown in Fig. Then implemented on the NS-2 simulator using C language classes already built and implemented an interface OTcl to use these classes.

Figure 3-1: Random Waypoint – Class model.

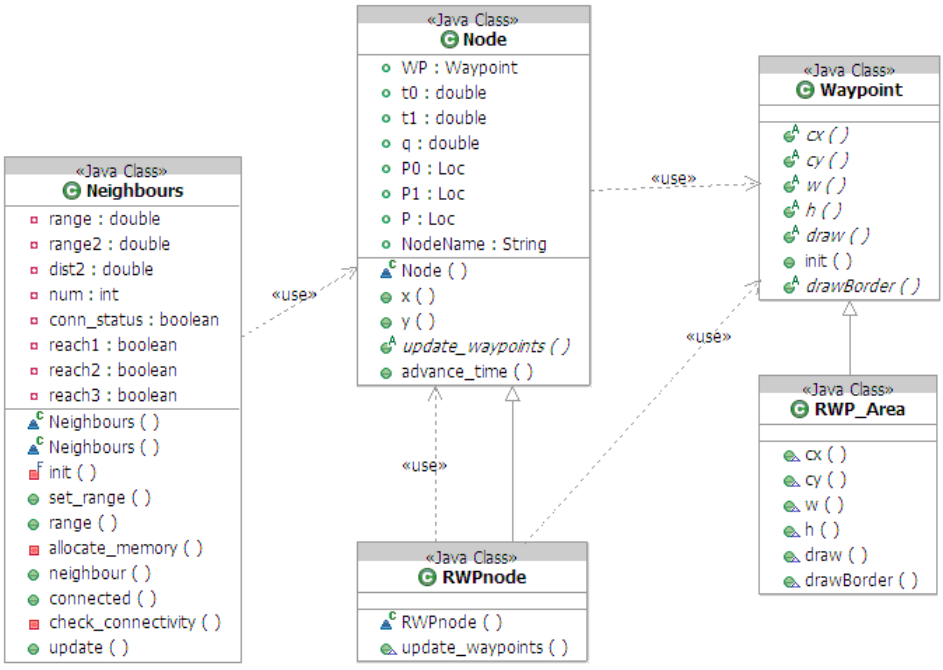


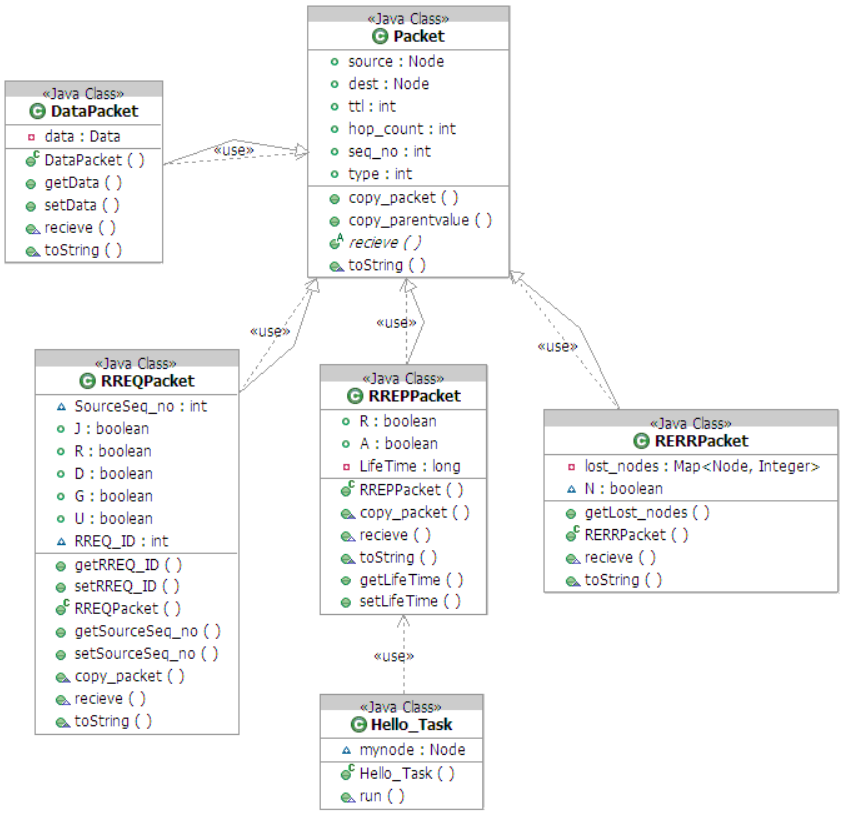
Figure 3-2: Random Waypoint on OTcl.

```
58
59  for {set i 0} {$i < $val(nn) } {incr i} {
60      set node_($i) [$ns_ node]
61      $node_($i) random-motion 0       ;# disable random motion
62
63      # Provide initial location of mobilenodes
64      set num_X1 [expr {floor(rand()*490.0)}]
65      set num_Y1 [expr {floor(rand()*490.0)}]
66      set num_Z1 0.0
67      puts "Coordenadas nodo $i :"
68      puts "X:$num_X1 , Y:$num_Y1 , Z:$num_Z1 "
69      $node_($i) set X_ $num_X1
70      $node_($i) set Y_ $num_Y1
71      $node_($i) set Z_ $num_Z1
72
73      # Generation of movements
74      set num_mov [expr {floor(rand()*20)+2}]
75      puts "num_mov:$num_mov"
76      for {set j 1} {$j < $num_mov } {incr j} {
77          puts "$j"
78          set num_X2 [expr {floor(rand()*490.0)+1}]
79          set num_Y2 [expr {floor(rand()*390.0)+1}]
80          set num_Z2 [expr {floor(rand()*7.0)+1}]
81          set randtime [expr {floor(rand()*($val(stop)))}]
82
83          puts "Tiempo de Accion = $randtime antes de = $val(stop)"
84          puts "num_X2 = $num_X2"
85          puts "num_Y2 = $num_Y2"
86          puts "num_Z2 = $num_Z2"
87
88          $ns_ at $randtime "$node_($i) setdest $num_X2 $num_Y2 $num_Z2"
89      }
90  }
91
92  # Set a TCP connection between node (0) and node (1)
93  set tcp [new Agent/TCP/Newreno]
```

3.7.3 AODV Packages - Class Model

Taking into account the different types of packets used in the AODV routing protocol, was initially a model of their respective relationship in terms of Java classes (see figure 3-4). Then in NS-2 was implemented to perform the capture of important data for this work, using the AODV model that already exists in the simulation tool and modifying the trace files.

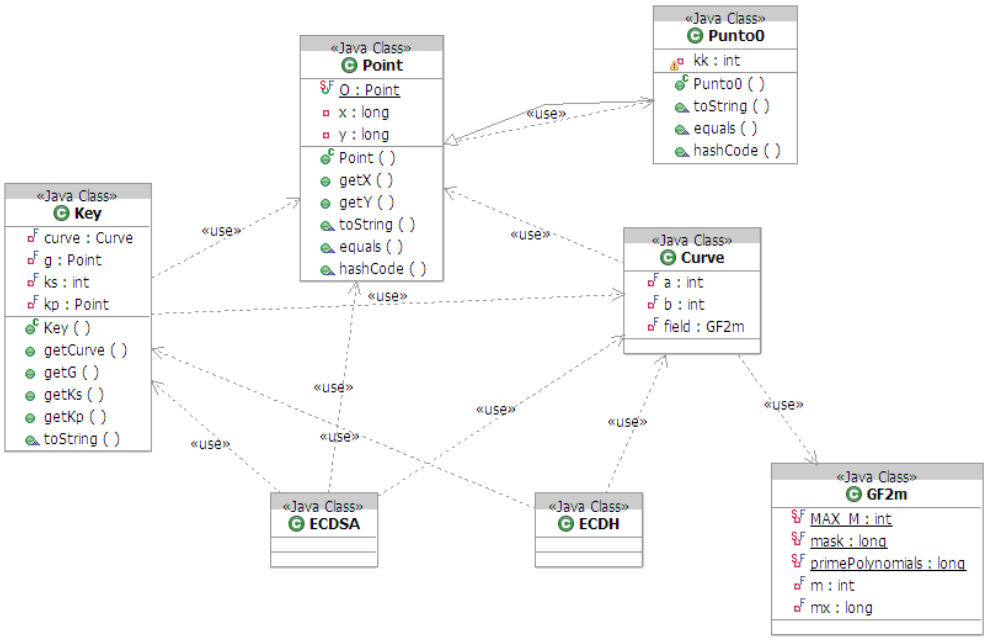
Figure 3-1: AODV packages - class model.



3.7.4 ECC Application - Class Model

Java was initially performed on a design for the implementation of an ECC in MANET, then took this design and were built in C++ classes for NS-2. Finally with OTcl interface is generated using this model. It is important to note that we used the finite Galois field $GF(\mathbb{F}_2{}^m)$.

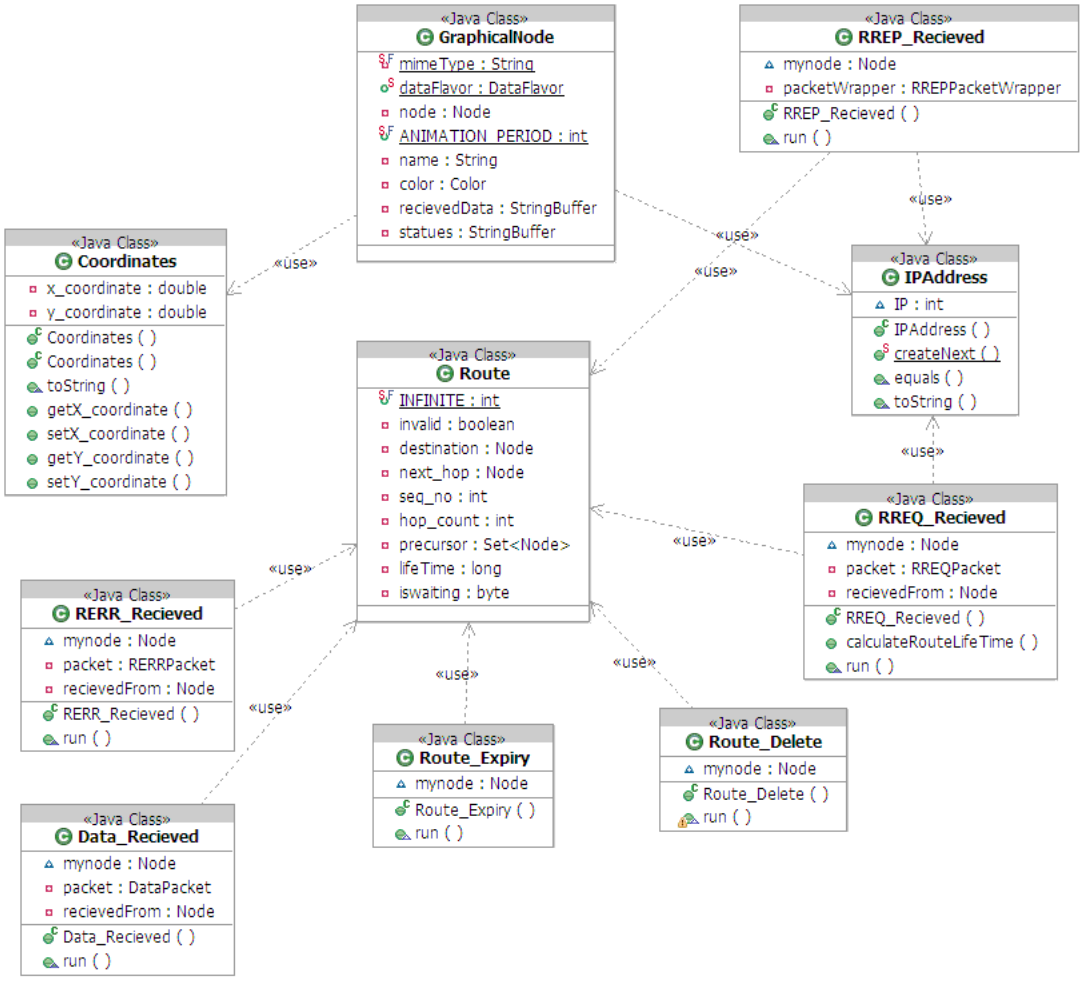
Figure 3-1: ECC application - class model.



3.7.5 Cross Components - Class Model

Initially a model was constructed to link the Java transverse components and characteristics of the system, taking into account routing, mobility model, packet types and physical characteristics. Then, using the characteristics of the NS-2 simulator, took the packages that already existed and were built that are not included in the tool.

Figure 3-1: Cross Components - class model.

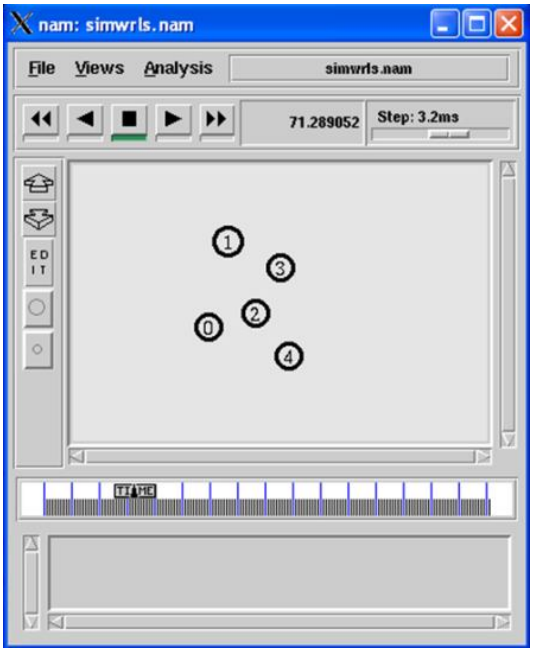


3.8 Description of Simulations

3.8.1 Simulation of the Mobility Model

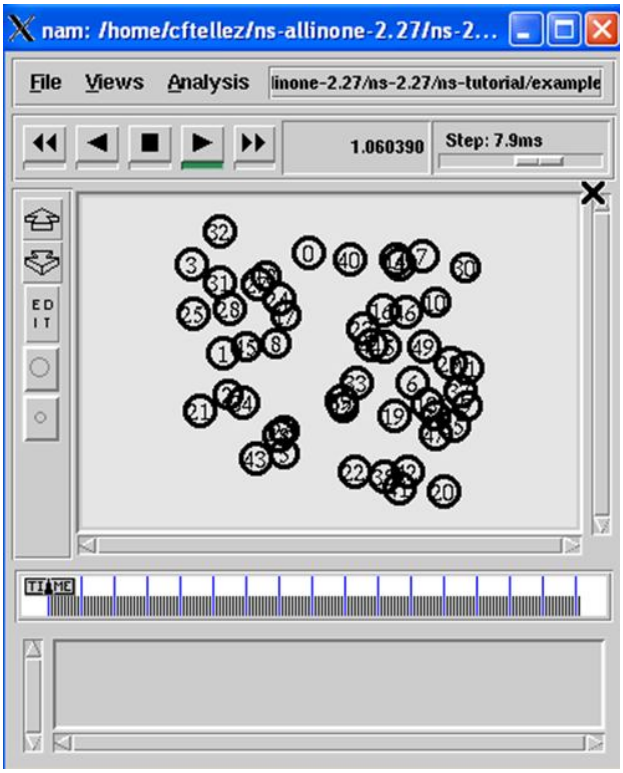
It builds the NS-2 simulation of the Random Waypoint mobility model initially for 5 nodes.

Figure 3-1: Simulation of the mobility model. 5 nodes.



Then for 50 nodes

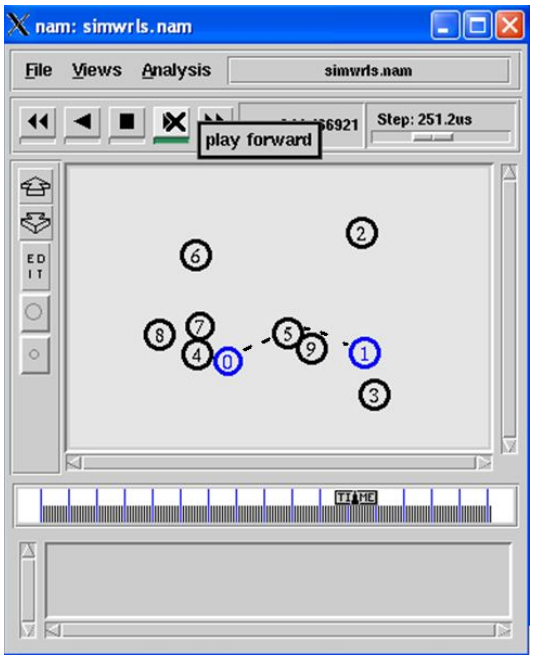
Figure 3-2: Simulation of the mobility model. 50 nodes.



3.8.2 Simulation of the Routing Protocol

It builds the NS-2 simulation of AODV routing protocol using C + + classes of the tool and adding functionality to implement the secure algorithm. It is tested for 10 nodes. NAM are shown in blue nodes are communicating through the protocol.

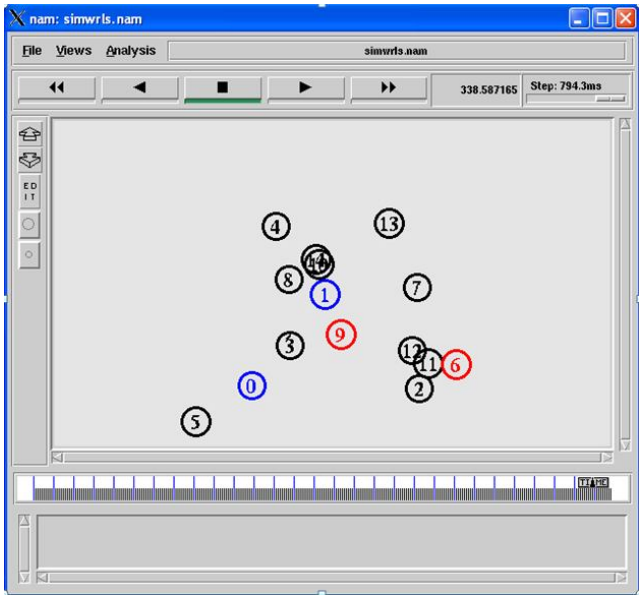
Figure 3-1: Simulation of the routing protocol.



3.8.3 Simulation of the Wormhole Intrusion

Wormhole tunnel is simulated using some existing packages and modifying the tool features Denial of Service. Attackers are represented on NAM as red nodes.

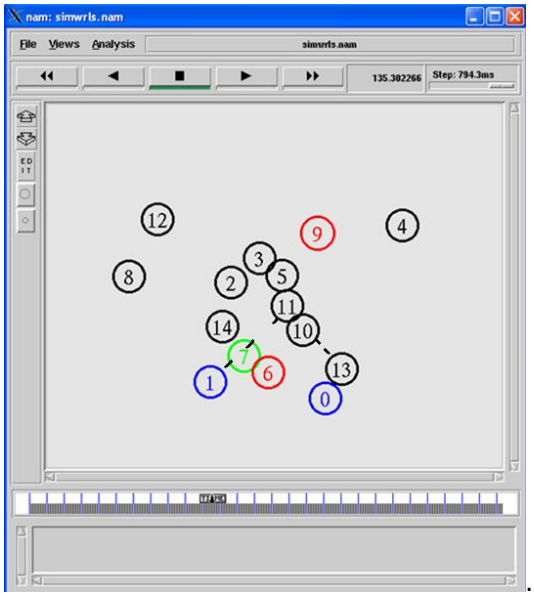
Figure 3-1: Simulation of the wormhole intrusion.



3.8.4 Simulation of the Wormhole Detection

Classes are implemented the solution by modifying the AODV algorithm, adding the functionality of the S-AODV and then making EC-S-AODV. After implementing a nodes monitor for the IDS. Green shows the node with the agent that detected the intrusion monitoring using IDS protocol without using EC-S-AODV.

Figure 3-1: Simulation of the wormhole detection.



4. Chapter 4

After implementing the simulations described in the previous chapter of this thesis were collected traceability data files to evaluate several of the behaviors that had the job of simulation [111] and plotted in the tool NS-2 simulator called Xgraph, disabling the NAM tool after confirming the behavior of the network with few nodes visually. Then see the results.

4.1 Experimental and Results - Behavior of Intruder

We initially experimented with simulations representing MANET environment (including mobility model, routing algorithm and other physical characteristics of the network), where a tunnel was present type Wormhole Out-of-band formed by two malicious nodes. In the first simulation was created Wormhole tunnel but disable any harmful action I could take this to validate how many messages were sent from any node transmitter and how many messages were received by any receiving node to determine the efficiency of transmission / reception network and similarly how many packets passing through the tunnel that took no active action.

Figure 4-1: Simulation 1 - Results.

In the graph, the red line represents the number of packets sent from any point on the network, ie, whenever any node in time sent packages that number added to this value. The line in blue represents the number of packets received from anywhere in the network, ie, whenever any node in the received packet time that number added to this value. The line in green represents the number of nodes that are happening in a given time through the wormhole tunnel, ie, it is count from when a packet arrives from a malicious node and another node reaches the attacker. As we can see there are points where most packages are sent at time t but is due to the accumulation of packages that have not been received and may be traveling in the course of time as they reach their goal. What we cannot stop looking at is the number of packets that are passing through the tunnel. Extracting the data for graphing in a controlled manner and by sampling 40 simulations of 5 minutes each with 200 nodes values are obtained as follows.

Table 4-1: Number of packets sent / received in a time t and number of packets that pass through the tunnel.

Test 32	PACKAGES		
TIME ti	**SENT**	**THROUGH THE TUNNEL**	**RECEIVED**
t1	34	0	0
t2	56	23	0
t3	12	2	45
t4	6	3	32
t5	4	0	2
t6	45	23	34
t7	67	38	45
t8	91	67	63
t9	180	89	79
t10	32	10	68
t11	45	40	113
t12	72	51	47
t13	4	2	34
t14	49	37	10
t15	34	23	3
t16	56	49	4
t17	67	34	2
t18	34	11	5
t19	37	14	119
t20	39	28	89

Figure 4-2: Number of packets sent / received in a time t and number of packets that pass through the tunnel.

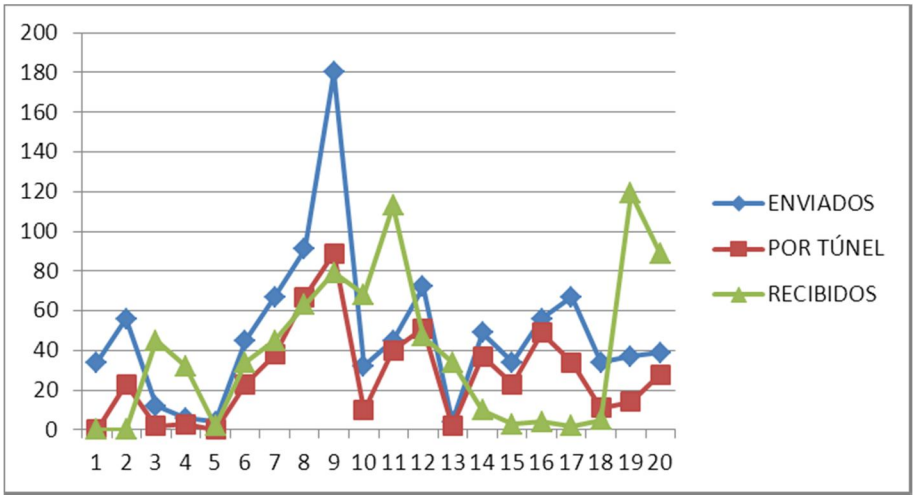
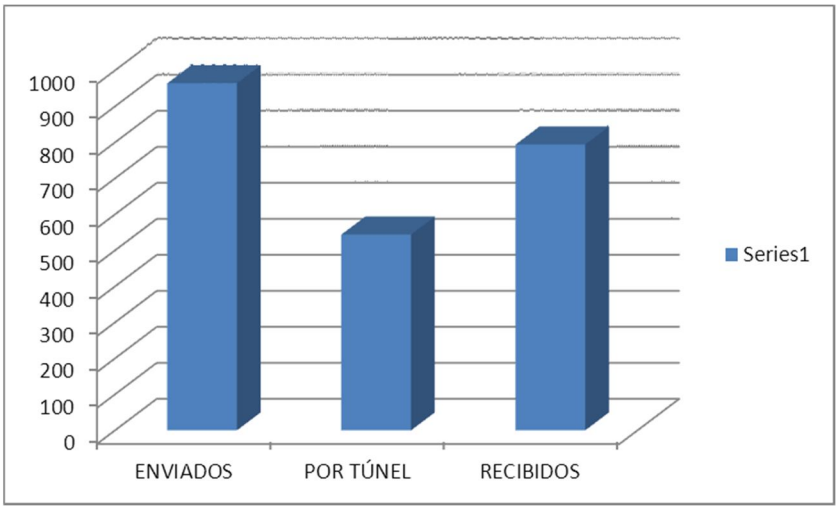


Figure 4-3: Number of packets sent / received in total in a simulation and the number of packets that pass through the tunnel.



Pondering the results of the simulations, 81.34% of the packets sent are received successfully. This is a very common value for AODV reception. It was also found that 55.19% of the packets pass through the tunnel. Note that here are not making an active attack, simply by a passive attack is analyzing the traffic that passes through the tunnel without taking some negative action as we have discussed in the section 2.5.2.

Then, we performed the same test but this time an action is triggered of denial of service in the tunnel to drop all packets passing through it (BlackHole Attack). (See Figure 4-4).

Figure 4-4: Number of packets sent / received in total in a simulation and the number of packets that pass through the tunnel with an active attack.

Given the same conventions, ie Red line: packets sent from anywhere in the network, Blue line: packets received and Green line: packets passing through the wormhole tunnel we noticed the large packet loss that occurs when the attack venturing with an action of denial of service.

Extracting the data for graphing in a controlled manner and by sampling 40 simulations of 5 minutes each with 200 nodes values are obtained as follows.

Table 4-2: Number of packets sent / received in a time t and number of packets that pass through the tunnel with an active denial of service attack.

Test 11	PACKAGES		
TIME ti	**SENT**	**THROUGH THE TUNNEL**	**RECEIVED**
t1	2	0	0
t2	5	0	0
t3	45	2	3
t4	4	3	6
t5	7	0	2
t6	16	3	3
t7	34	38	5
t8	52	67	1
t9	64	89	13
t10	79	10	23
t11	92	40	10
t12	90	51	4
t13	45	2	1
t14	2	37	0
t15	34	23	0
t16	56	49	0
t17	67	34	2
t18	3	11	5
t19	37	14	11
t20	39	28	2

Figure 4-5: Number of packets sent / received in a time t and number of packets that pass through the tunnel with an active denial of service attack.

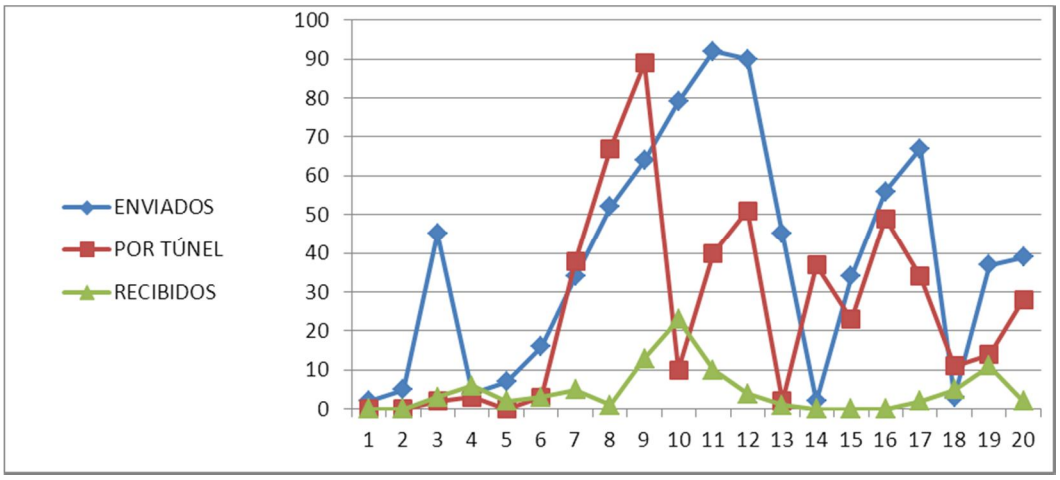
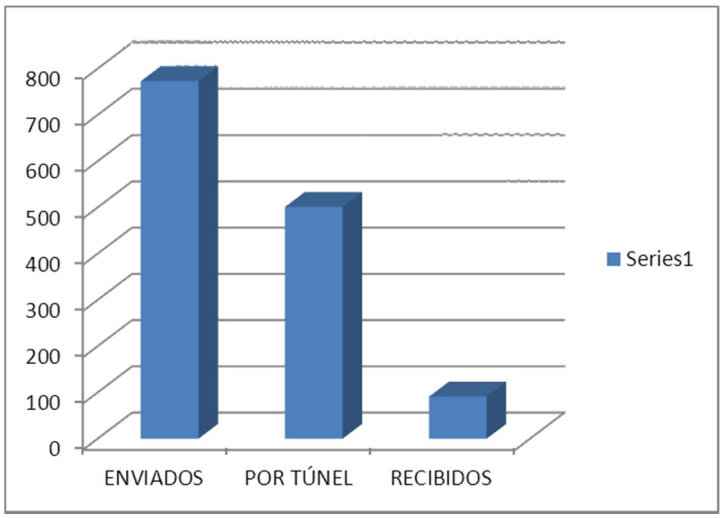


Figure 4-6: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack.



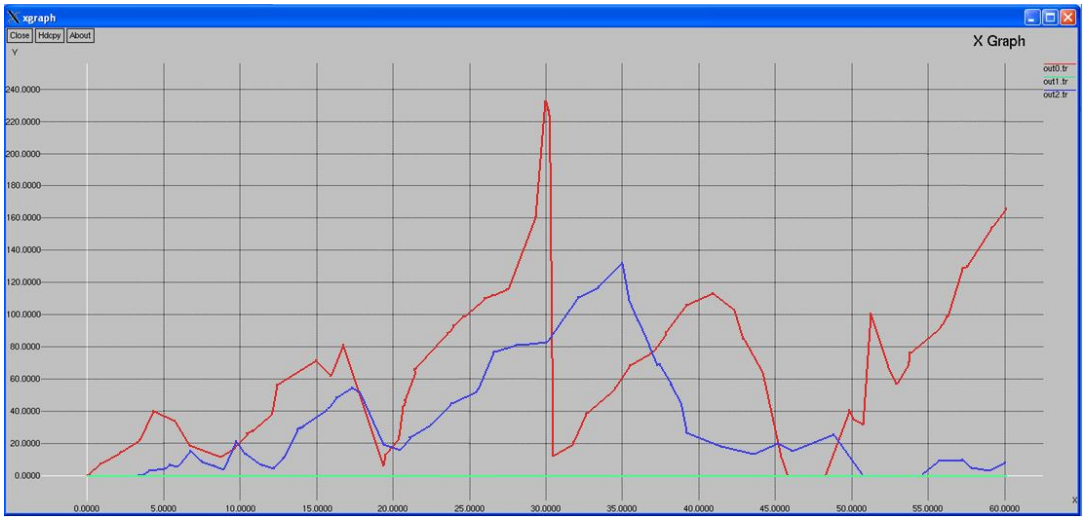
Pondering the results of the simulations with the active attack, and were not successful 81.34% of packets sent but only received the 11.72%. This shows the great amount of information that is lost when a wormhole attack occurs.

4.2 Results of the Detection and Evasion

This set of simulations includes two stages of implementation of safety, a protocol of the EC-S-AODV (mixing secure routing aspects and Key Management Service using ECC) and the other is the application of IDS agents for monitoring nodes.

Applying EC-S-AODV from the start in the default routing and assigning a key agreement private and public, the tunnel was totally void. This is because the simulation validation was included which asked for authentication and when a node does not answer simply is discarded from the routing process. This would simulate an environment where attackers are external to the network and do not know the key and it is impossible for them to authenticate to be able to pose as trusted nodes.

Figure 4-1: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a EC-S-AODV functional protocol.



However, this result should be reviewed further. Disabling communication with the attackers is made by S-AODV protocol using authentication by elliptic curves, notwithstanding this prohibition depends on the capture of the attacker's IP address. It is necessary to check that media can be used to completely disable the attack in order to mitigate the tunnel to where it is impossible to capture the IP address when an authentication request message cannot capture that direction. Another important aspect is to show that when the solution was applied to the amount of payload packets after receiving the RREP decreased by 18.56% compared to the non-implementation of the

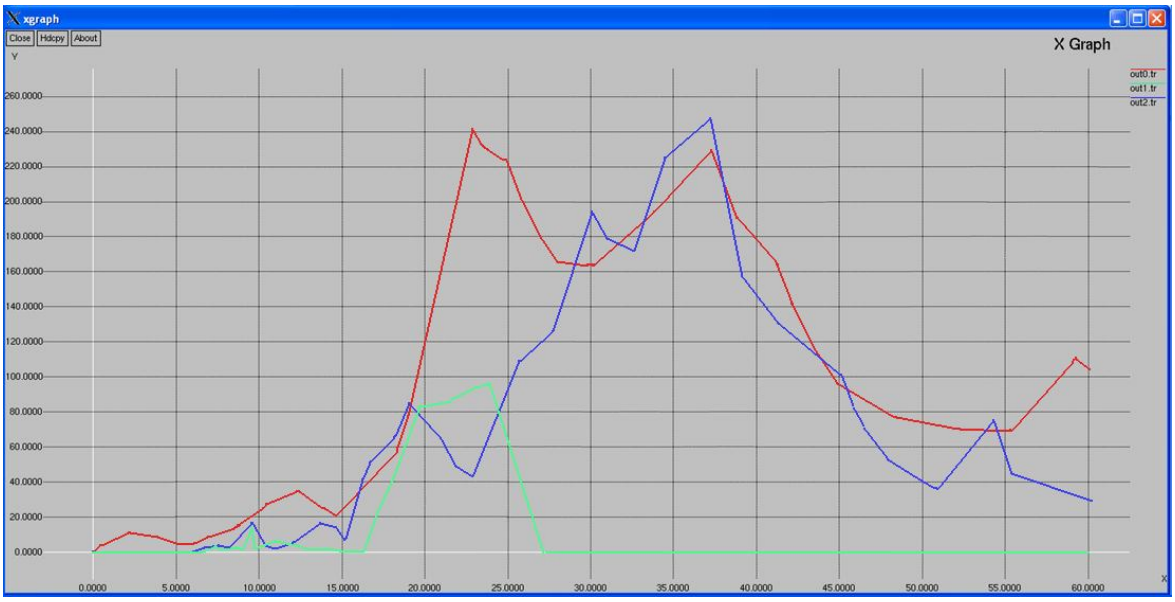
solution and when the attack does not hurt. That is, the authentication process lowers the rate of flow of messages in the network. Still, there is a very high value even more considering that the implementation of an ECC saves network resources compared to other solutions based on cryptography.

Table 4-3: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a EC-S-AODV functional protocol.

Test 26	PACKAGES		
TIEMPO ti	**ENVIADOS**	**A TRAVÉS DEL TÚNEL**	**RECIBIDOS**
t1	2	0	0
t2	1	0	1
t3	34	0	0
t4	21	0	31
t5	32	3	4
t6	34	3	45
t7	61	7	9
t8	89	34	18
t9	102	45	34
t10	98	34	67
t11	65	45	25
t12	72	56	36
t13	56	65	47
t14	34	12	87
t15	97	1	23
t16	67	23	32
t17	43	34	3
t18	19	56	2
t19	61	12	37
t20	31	26	12

The other simulation that was carried out in a second phase was to apply the security system where the attackers are part of the network and create a tunnel to generate a denial of service. In this case the nodes know the keys necessary to authenticate and can form a tunnel protocol mocking EC-S-AODV. That's where we evaluate the implementation of IDS monitoring nodes. The result was as follows.

Figure 4-2: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a Distributed and Cooperative IDS.



The IDS Agent running received information from other nodes belonging to other irregularity in the number RERR message generation. Note that the attack was present at one time online doing damage until the alarm is raised to detect the intruder. The intruder is identified with the routes monitored and the punishment given to IP addresses that generate an error message number greater than allowed (the number of messages is 20 messages RERR every 40 seconds, however this parameter can be varied and is under study to find the optimal limit). After lifting the alarm sends a broadcast message informing nodes eliminating routes that are considered attackers. This process takes some time which is what can be displayed on the graph where the action is fast but not immediate.

Table 4-4: Number of packets sent / received in total in a simulation and number of packets that pass through the tunnel with an active denial of service attack and a Distributed and Cooperative IDS.

Test 29	PACKAGES		
TIEMPO ti	**ENVIADOS**	**A TRAVÉS DEL TÚNEL**	**RECIBIDOS**
t1	3	0	0
t2	6	0	5
t3	52	0	7
t4	12	0	23
t5	10	0	35
t6	7	12	15
t7	61	18	4
t8	48	11	15
t9	72	0	23
t10	94	0	51
t11	81	0	24
t12	79	0	57
t13	54	0	69
t14	23	0	26
t15	83	0	29
t16	47	0	41
t17	46	0	32
t18	24	0	21
t19	73	0	22
t20	42	0	71

5. Chapter 5

5.1 Conclusions

Elliptic Curve Cryptography (ECC) is a good choice to implement authentication and information security in MANET, since it has features that make it viable when used in networks with limited resources. However, the implementation of an ECC is not enough to counter the Wormhole attack. It is necessary to combine these security and authentication methods with other approaches like: intrusion detection systems and secure routing algorithms. Such combinations will make not only to counter an attack as complex and dangerous as the Wormhole, but should be set very high levels of security against other attacks. In this thesis, we have done a very broad survey about the Wormhole attack and the application of ECC in MANET in order to conclude that, in terms of ensuring security in MANET, ECC is not sufficient but necessary.

References

[1] S. Corson, J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF RFC 2501, January 1999.

[2] Mahajan, V.; Natu, M.; Sethi, A.; , "Analysis of wormhole intrusion attacks in MANETS," *Military Communications Conference, 2008. MILCOM 2008. IEEE* , vol., no., pp.1-7, 16-19 Nov. 2008.

[3] Hu, Y.-C.; Perrig, A.; Johnson, D.B.; , "Packet leashes: a defense against wormhole attacks in wireless networks," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies* , vol.3, no., pp. 1976- 1986 vol.3, 30 March-3 April 2003.

[4] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks”, in: Proceedings of NDSS (Feb. 2004).

[5] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W.; , "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," *Wireless Communications and Networking Conference, 2005 IEEE* , vol.2, no., pp. 1193- 1199 Vol. 2, 13-17 March 2005.

[6] M. Natu and A.S. Sethi, “Intrusion detection system to detect wormhole using fault localization techniques.” In WORLDCOMP SAM'07, International Conference on Security and Management, Las Vegas, NV, June 2007.

[7] Gorlatova, M.A.; Mason, P.C.; Wang, M.; Lamont, L.; Liscano, R.; , "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," *Military Communications Conference, 2006. MILCOM 2006. IEEE* , vol., no., pp.1-7, 23-25 Oct. 2006.

[8] Sun Choi; Doo-young Kim; Do-hyeon Lee; Jae-il Jung; , "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," *Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08. IEEE International Conference on* , vol., no., pp.343-348, 11-13 June 2008.

[9] Nait-Abdesselam, F.; , "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *Communications Magazine, IEEE* , vol.46, no.4, pp.127-133, April 2008.

[10] S. Capkun, L. Buttyan, and J. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks”, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp.1-12, Washington, USA, Oct 2003.

[11] V. Katiyar, K. Dutta, S. Gupta; “A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment.” *International Journal of Computer Applications* 11(10):41–46, December 2010.

[12] Vanstone, S.A., “Next generation security for wireless: elliptic curve cryptography”, Elsevier, Computers and Security“, Vol. 22, No. 5, July 2003, 412-415.

[13] Kruus, Peter; Sterne, Dan; Gopaul, Richard; Heyman, Michael; Rivera, Brian; Budulas, Peter; Luu, Brian; Johnson, Tommy; Ivanic, Natalie; Lawler, Geoff; , "In-Band Wormholes and Countermeasures in OLSR Networks," *Securecomm and Workshops, 2006* , vol., no., pp.1-11, Aug. 28 2006-Sept. 1 2006.

[14] M. Azer, S. El-Kassas, and M.M.S. El-Soudani, "A Full Image of the Wormhole Attacks - Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", presented at CoRR, 2009.

[15] Xia Wang; Wong, J.; , "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks," *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International* , vol.1, no., pp.39-48, 24-27 July 2007.

[16] C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, D. Raffo, "Securing the OLSR routing protocol with or without compromised nodes in the network", Institut National de Recherche en Informatique et en Automatique", ISRN INRIAR/RR-54-94, February 2005.

[17] Khalil, I.; Saurabh Bagchi; Shroff, N.B.; , "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on* , vol., no., pp. 612- 621, 28 June-1 July 2005.

[18] R. Gopaul, P. Kruus, D. Sterne, and B. Rivera, "Gravitational analysis of the in-band wormhole phenomenon", Proc. 25th Army Science Conference, Orlando, FL, Nov. 2007.

[19] Eriksson, J.; Krishnamurthy, S.V.; Faloutsos, M.; , "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks," *Network Protocols, 2006. ICNP '06. Proceedings of the 2006 14th IEEE International Conference on* , vol., no., pp.75-84, 12-15 Nov. 2006.

[20] Gunhee Lee; Dong-kyoo Kim; Jungtaek Seo; , "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks," *Information Security and Assurance, 2008. ISA 2008. International Conference on* , vol., no., pp.220-225, 24-26 April 2008.

[21] Pires, W.R., Jr.; de Paula Figueiredo, T.H.; Wong, H.C.; Loureiro, A.A.F.; , "Malicious node detection in wireless sensor networks," *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International* , vol., no., pp. 24, 26-30 April 2004.

[22] Xia Wang; , "Intrusion Detection Techniques in Wireless Ad Hoc Networks," *Computer Software and Applications Conference, 2006. COMPSAC '06. 30th Annual International* , vol.2, no., pp.347-349, 17-21 Sept. 2006.

[23] Khurana, S.; Gupta, N.; , "FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks," *Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on* , vol., no., pp.74-79, 25-31 Aug. 2008.

[24] C. Honglong, L. Wei, W. Zhi: “A Consistency-Based Secure Localization Scheme against Wormhole Attacks in WSNs.” WASA 2009: 368-377.

[25] Azer, M.A.; El-Kassas, S.M.; El-Soudani, M.S.; , "Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks," *Systems and Networks Communications, 2009. ICSNC '09. Fourth International Conference on* , vol., no., pp.30-36, 20-25 Sept. 2009.

[26] Qiu Xiu-feng; Liu Jian-wei; Sangi, A.R.; , "MTSR: Wormhole attack resistant secure routing for Ad hoc network," *Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference on* , vol., no., pp.419-422, 28-30 Nov. 2010.

[27] Maheshwari, R.; Jie Gao; Das, S.R.; , "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE* , vol., no., pp.107-115, 6-12 May 2007.

[28] Jen, S. M., Laih,. C.S., and KuoW,. C. “A hop-count analysis scheme for avoiding wormhole attacks in MANET”. In Sensors2009.

[29] Zeng, Yingpei; Zhang, Shigeng; Guo, Shanqing; Li, Xie; , "Secure Hop-Count Based Localization in Wireless Sensor Networks," *Computational Intelligence and Security, 2007 International Conference on* , vol., no., pp.907-911, 15-19 Dec. 2007.

[30] W. Wang, B. K. Bhargava. “Visualization of wormholes in sensor networks”. In Proceedings of Workshop on Wireless Security'2004. pp.51~60

[31] Azer M., El-Kassas S., El-Soudani M. M. S.; “Using Attack Graphs in Ad Hoc Networks - For Intrusion Prediction Correlation and Detection”. In Proceedings of SECRYPT'2006. pp.63~68

[32] R. Poovendran and L. Lazos, “A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks”, Wireless Networks, vol. 13(1), pp. 27-59, 2007.

[33] D. Dong, M. Li, Y. Liu, X. Liao., “Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks”. J. Inf. Sci. Eng., 2011: 65~78

[34] KhinSandar Win, “Analysis of Detecting Wormhole Attack in Wireless Networks”, World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008

[35] F. Kong, C. Li, Q. Ding, G. Cui, B. Cui, "WAPN: A Distributed Wormhole Attack Detection Approach for Wireless Sensor Networks," Journal of Zhejiang University SCIENCE A, vol.10, p. 279~289, February 2009.

[36] Yun Wang; Zhongke Zhang; Jie Wu; , "A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information," *Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on* , vol., no., pp.63-72, 15-17 July 2010.

[37] Nguyen, D.Q.; Lamont, L.; , "A Simple and Efficient Detection of Wormhole Attacks," *New Technologies, Mobility and Security, 2008. NTMS '08.* , vol., no., pp.1-5, 5-7 Nov. 2008.

[38] Song, N.; Qian, L.; Li, X.; , "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," *Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International* , vol., no., pp. 8 pp., 4-8 April 2005.

[39] L. Buttyán, L. Dóra, I. Vajda, "Statistical Wormhole Detection in Sensor Networks", Second European Workshop on Security and Privacy in AdHoc and Sensor Networks (ESAS 2005), Visegrád, Hungary, July 13-14,2005,pp. 128-141.

[40] Yanchao Zhang; Wei Liu; Wenjing Lou; Yuguang Fang; , "Securing sensor networks with location-based keys," *Wireless Communications and Networking Conference, 2005 IEEE* , vol.4, no., pp. 1909- 1914 Vol. 4, 13-17 March 2005.

[41] Xu Huang; Shah, P.G.; Sharma, D.; , "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," *Network and System Security (NSS), 2010 4th International Conference on* , vol., no., pp.588-593, 1-3 Sept. 2010.

[42] Jia Xiangyu; Wang Chao; , "The application of elliptic curve cryptosystem in wireless communication," *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005. MAPE 2005. IEEE International Symposium on* , vol.2, no., pp. 1602- 1605 Vol. 2, 8-12 Aug. 2005.

[43] Yong Wang; Ramamurthy, B.; Xukai Zou; , "The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," *Communications, 2006. ICC '06. IEEE International Conference on* , vol.5, no., pp.2243-2248, June 2006.

[44] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation,vol. 48, no.177, pp.203-209, Jan 1987.

[45] A. Jurisic and A.J. Menezes, “Elliptic curves and cryptography”, Dr. Dobb’s Journal, pages 26-35, April 1997.

[46] D. Hakerson, A. Menezes, and S. Vanston, "Guide to Elliptic Curve Cryptography," Springer-Verlag New York, Inc., Secaucus, NJ, USA, (2004).

[47] H. Cohen, A Miyaji and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates," Lectures Notes in Computer Science, 1514, 51-65 (1998).

[48] D. Johnson and A. Menezes, “The elliptic curve digital signature algorithm (ECDSA)”, Technical report CORR 99-34, University of Waterloo, 2000.

[49] Nippon Telephone and Telegraph Corporation; “SEC X.1 Supplemental Document for Odd Characteristic Extension Fields”, June, 2008.

[50] Standards for Efficient Cryptography Group, "SEC 1: EllipticCurve Cryptography", May 2009, <http://www.secg.org/download/aid-780/sec1-v2.pdf>.

[51] Standards for Efficient Cryptography Group; "SEC 2: Recommended Elliptic Curve Domain Parameters"; September 2000. V1.0; <http://www.secg.org/download/aid-386/sec2_final.pdf>.

[52] National Institute of Standards and Technology; “Digital Signature Standard (DSS)”, FIPS Publication 186-2, 2000.

[53] National Institute of Standards and Technology; “Secure Hash Standard”, FIPS Publication 180-1, 1995.

[54] A. Menezes, “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic Publishers, Dordrecht, 1993.

[55] "IEEE Standard Specifications for Public-Key Cryptography," *IEEE Std 1363-2000* , vol., no., pp.i, 2000.

[56] J. Lopez, R. Dahab, “Improved algorithms for elliptic curve arithmetic in GF(2n)”, in: Selected Areas in Cryptography, Proc. SAC’98, Lecture Notes in Comput. Sci., Vol. 1556, Springer, Berlin, 1998, pp. 201–212.

[57] H. K. Kwang, N. Christophe; "Point Multiplication on Supersingular Elliptic Curves Defined over Fields of Characteristic 2 and 3", SECRYPT 2008, Proceedings of the International Conference on Security and Cryptography, Porto, Portugal, 2008.

[58] S. Blake-Wilson, A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol.", Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, Proceedings, pages: 154-170, 1999.

[59] P. Szczechowiak, L.B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks", in Proc. EWSN, 2008, pp.305-320.

[60] Ngai, E.C.H.; Jiangchuan Liu; Lyu, M.R.; , "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *Communications, 2006. ICC '06. IEEE International Conference on* , vol.8, no., pp.3383-3389, June 2006.

[61] Hoang Lan Nguyen; Uyen Trang Nguyen; , "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on* , vol., no., pp. 149, 23-29 April 2006.

[62] Pohlig, S.; Hellman, M.; , "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.)," *Information Theory, IEEE Transactions on* , vol.24, no.1, pp. 106- 110, Jan 1978.

[63] An Liu; Peng Ning; , "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on* , vol., no., pp.245-256, 22-24 April 2008.

[64] Kumar, K.; Begum, J.N.; Sumathy, V.; , "A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks," *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference on* , vol., no., pp.470-475, 23-25 July 2009.

[65] Jing-feng Li; Ya-juan Zhang; Yue-fei Zhu; , "A secure elliptic curve communication scheme for the cluster-based ad hoc networks," *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on* , vol., no., pp.1-4, 6-9 Nov. 2006.

[66] Hamed, A.I.; El-Khamy, S.E.; , "New low complexity key exchange and encryption protocols for wireless sensor networks clusters based on Elliptic Curve Cryptography," *Radio Science Conference, 2009. NRSC 2009. National* , vol., no., pp.1-13, 17-19 March 2009.

[67] V. Vijayalakshmi and T.G. Palanivelu, “Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography”, Journal of Computer Science, Vol. 3, No. 12, 2007, 939-943.

[68] Shouyun Song; Junpeng Xu; Shuai Yang; Qing Cong; , "Completely self-organization Ad hoc networks key management scheme based on elliptic curve," *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on* , vol.6, no., pp.271-274, 9-11 July 2010.

[69] E. Levent, C. Nitu, “Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs”, IJCSNS, Vol.7, No.4, April 2007.

[70] Dahshan, Hisham; Irvine, James; , "A Threshold Key Management Scheme for Mobile Ad Hoc Networks Using Elliptic Curve Dlog-Based Cryptosystem," *Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual* , vol., no., pp.130-137, 11-14 May 2010.

[71] Xiaojiang Du; Guizani, M.; Yang Xiao; Hsiao-Hwa Chen; , "A routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks," *Wireless Communications, IEEE Transactions on* , vol.8, no.3, pp.1223-1229, March 2009.

[72] Dahshan, H.; Irvine, J.; , "An Elliptic Curve Distributed Key Management for Mobile Ad Hoc Networks," *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st* , vol., no., pp.1-5, 16-19 May 2010.

[73] Holohan, E.; Schukat, M.; , "Authentication Using Virtual Certificate Authorities: A New Security Paradigm for Wireless Sensor Networks," *Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on* , vol., no., pp.92-99, 15-17 July 2010.

[74] C. Zouridaki, B.L. Mark, K. Gaj, R.K. Thomas, "Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography", in Proc. EuroPKI, 2004, pp.232-245.

[75] Jiang Jian-wei; Liu Jian-hui; , "Research on key management scheme for WSN based on elliptic curve cryptosystem," *Networked Digital Technologies, 2009. NDT '09. First International Conference on* , vol., no., pp.536-540, 28-31 July 2009.

[76] Huaqun Wang; Shuping Zhao; Guoxing Jiang; , "Key Management Based on Elliptic Curve Paillier Scheme in Ad Hoc Networks," *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on* , vol.1, no., pp.116-119, July 30 2007-Aug. 1 2007.

[77] W. Xiong, B. Tang, “A Secure and Highly Efficient Key Management Scheme for MANET”, AISS: Advances in Information Sciences and Service Sciences, Vol. 3, No. 2, pp. 12-22, 2011.

[78] Chin-Chen Chang; Shih-Chang Chang; , "An Improved Authentication Key Agreement Protocol Based on Elliptic Curve for Wireless Mobile Networks," *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on* , vol., no., pp.1375-1378, 15-17 Aug. 2008.

[79] Du Congwei; Li Rongsen; Dou Wenhua; , "An efficient key agreement protocol in cluster-based MANETs," *Computer Application and System Modeling (ICCASM), 2010 International Conference on* , vol.10, no., pp.V10-627-V10-630, 22-24 Oct. 2010.

[80] Zhang Li-Ping; Cui Guo-Hua; Yu Zhi-Gang; , "An Efficient Group Key Agreement Protocol for Ad Hoc Networks," *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-5, 12-14 Oct. 2008.

[81] Wang Wei-hong; Lin Yu-bing; Chen Tie-ming; , "The study and application of elliptic curve cryptography library on wireless sensor network," *Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on* , vol., no., pp.785-788, 10-12 Nov. 2008.

[82] Xu Huang; Sharma, D.; , "Fuzzy controller for a dynamic window in elliptic curve cryptography wireless networks for scalar multiplication," *Communications (APCC), 2010 16th Asia-Pacific Conference on* , vol., no., pp.458-463, Oct. 31 2010-Nov. 3 2010.

[83] B. Erik-Oliver, M. Zitterbart, “Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks”, Telematics Technical ReportsTM-2005-1, 2005.

[84] S. Blake-Wilson, D. Johnson, and A. Menezes, “Key Agreement Protocols and Their Security Analysis”, in Proc. IMA Int. Conf., 1997, pp.30-45.

[85] Abusalah, L.; Khokhar, A.; Guizani, M.; , "A survey of secure mobile Ad Hoc routing protocols," *Communications Surveys & Tutorials, IEEE* , vol.10, no.4, pp.78-93, Fourth Quarter 2008.

[86] Zheng Yan, “Security in Ad Hoc Networks,” Networking Laboratory, Helsinki University of Technology, 2002.

[87] Z. Yan, P. Zhang, and T. Virtanen, “Trust Evaluation Based Security Solution in Ad Hoc Networks”, The Seventh Nordic Workshop on Secure IT Systems, NordSec 2003, Gjovik, Norway, 10, 2003.

[88] Brutch, P.; Ko, C.; , "Challenges in intrusion detection for wireless ad-hoc networks," *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on* , vol., no., pp. 368- 373, 27-31 Jan. 2003.

[89] Abi-Char, P.E.; Mhamed, A.; El-Hassan, B.; , "A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography," *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on* , vol., no., pp.89-94, 29-31 Aug. 2007.

[90] Senthilkumar G Cheetancheri.; , "Modelling a Computer Worm Defense System.", Master’s thesis for B.E. Computer Science & Engineering. Coimbatore Institute of Technology, Coimbatore, India. (1998).

[91] C. Perkins, E.Belding-Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, IETF RFC 3561, July 2003.

[92] R. Ramanathan, and J. Redi, “A brief overview of ad hoc networks: challenges and directions”, In: Communications Magazine, IEEE, Vol. 40 p. 20-22, 2002.

[93] M. N. Rooker and A. Birk, “Combining Exploration and Ad-Hoc Networking in RoboCup Rescue,” in RoboCup 2004: Robot Soccer World Cup VIII, ser. Lecture Notes in Artificial Intelligence (LNAI), D. Nardi, M. Riedmiller, and C. Sammut, Eds. Springer, vol. 3276, pp. 236–246, 2005.

[94] Hanzo-II, L.; Tafazolli, R.,"A Survey Of QoS Routing Solutions For Mobile Ad Hoc Networks", Communications Surveys & Tutorials, IEEE Volume 9, Issue 2, Page(s):50 - 70, 2007.

[95] B.L. Su, Y.M. Huang, and F. Lee, "Distributed Location-Aware Transmission for Ad Hoc Networks", 17th APAN Meetings & Joint Techs Workshop, Honolulu, USA, 2004.

[96] Charles E. Perkins. Addison-Wesley, “Ad Hoc Networking” , December 2000.

[97] Imrich Chlamtac, Marco Conti & Jennifer Liu. “Mobile Ad Hoc Networking: Imperatives and challenges”, Ad Hoc Networks Publication, Volume 1, Issue 1, 2003.

[98] L.M. Feeney: “A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks”, SICS Technical Report T99/07, October 1999.

[99] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, “The dynamic source routing protocol for mobile ad hoc networks,” Internet Draft, MANET Working Group, February 2002.

[100] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” Request for Comments 3626, MANET Working Group, October 2003.

[101] R.V. Boppana and S. Konduru, “An adaptive distance vector routing algorithm for mobile Ad Hoc Networks”, in: Proceedings of INFOCOM (April 2001) pp. 1753–1762.

[102] F. Bertocchi, P. Bergamo, G. Mazzini, M. Zorzi, “Performance comparison of routing protocols for ad hoc networks”; Global Telecommunications Conference. GLOBECOM '03. IEEE In GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489), Vol. 2 (2003), pp. 1033-1037, 2003.

[103] Enneya, El Koutbi, BERQIA, “Enhancing AODV Performance based on Statistical Mobility Quantification”. 2006, IEEE.

[104] Rafsanjani K., Movaghar A., and Koroupi F., “Investigating Intrusion Detection Systems in MANET and Comparing Idss for Detecting Misbehaving Nodes,” in Proceedings of World Academy of Science, Engineering and Technology, Canada, pp. 123-128, 2008.

[105] Pirzada, A.A.; McDonald, C.; , "Secure Routing with the AODV Protocol," *Communications, 2005 Asia-Pacific Conference on* , vol., no., pp.57-61, 5-5 Oct. 2005.

[106] The Network Simulator - ns-2: http://isi.edu/nsnam/ns/

[107] Manel Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector Routing”. ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106-107, July 2002.

[108] Manel Guerrero Zapata and N. Asokan: "Securing Ad hoc Routing Protocols". In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pages 1-10. September 2002. ISBN 1-58113-585-8.

[109] J. Ortiz, L. Bobadilla, "Simulación de Redes Ad hoc bajo diferentes modelos de movilidad" . En: Colombia Ingeniería E Investigación *ISSN:* 0120-5609 *ed:* Universidad Nacional de Colombia *v.*53 *fasc.* p.44 - 50 ,2003.

[110] F. Tellez, J. Ortiz, “Behavior of Elliptic Curve Cryptosystems for the Wormhole Intrusion in MANET: A Survey and Analysis”, IJCSNS International Journal of Computer Science and Network Security, Journal ISSN : 1738-7906, Vol. 11 No. 9 pp. 1-12, 2011.

[111] Law, A. L. & D. W. Kelton, (2000), Simulation Modeling and Analysis, 3rd Edition, McGraw-Hill, Boston, MA.