Behavior of Elliptic Curve Cryptosystems for the Wormhole Intrusion in MANET: A Survey and Analysis

Felipe Téllez[†] and Jorge Ortiz [††],

National University of Colombia, Bogotá D.C., Colombia

Summary
This article presents a study about the performance with different applications of Elliptic Curve Cryptography in Wireless Mobile Ad-Hoc Networks (MANET) to determine their effectiveness in security during the Wormhole intrusion. The aim is to provide answers to questions like: Is it an elliptic curve cryptosystem applied to Ad-Hoc networks sufficient to prevent, detect, evade and/or eliminate Wormhole attacks? If not, should it live with any of the proposals that have already been raised to counteract this attack?, What is the behavior of the various solutions of this type of cryptography, which claim to offer security, when are confronted with a Wormhole tunnel? We present a state of the art about Wormhole, the different types that exist, and the proposed solutions to counter it are classified. We review the various solutions based on Elliptic Curve Cryptography posed to security in Ad-Hoc networks and then analyze their performance against the requirements to be met when providing security against malicious tunnel. In the end, is expected to conclude as cryptography, and especially for this study, the elliptic curves, ensures security against Wormhole tunnel.

Key words:
Ad-Hoc, Wormhole Intrusion, Elliptic Curve Cryptography, Performance Analysis, State of the Art, MANET Security.

1. 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. 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.

Many 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], [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?.

Our contribution:

This study compiles a comprehensive state of the art on Wormhole and ECC in MANET, in order to further analyze the behavior of ECC against this 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 remainder of this paper is structured as follows: Section 2 presents a state of the art of Wormhole intrusion, the actions it can perform on Ad-Hoc networks, Wormhole

Manuscript received September 20, 2011
Manuscript revised September 25, 2011

types and classification of the proposed solutions to counter this attack. Section 3 introduces the concept of Elliptic Curve Cryptography. Section 4 lists the protocols and the different solutions that have been proposed based on ECC to ensure security as well as its advantages when applied in MANET. Section 5 lists the requirements to be satisfied by an ECC system to prevent, detect, evade and/or delete a wormhole attack and an analysis of compliance of these requirements in the ECC's proposed related work for countering the attack. Section 6 shows the conclusions. Section 7 lists possible directions for future work. Finally, Section 8 lists the references in this study.

2. Wormhole Attack

2.1 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.

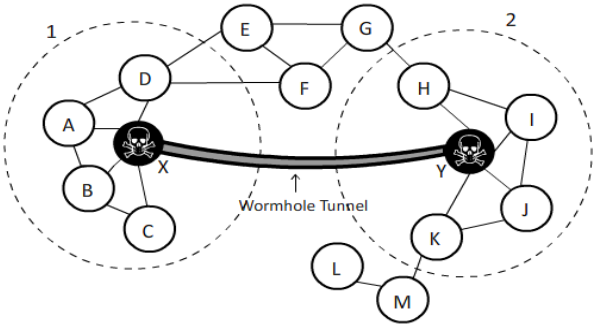

Fig 1. Intrusion in Ad-Hoc Network with Wormhole Tunnel: X and Y represent the Wormhole nodes connected through a tunnel that creates the illusion that region 1 and region 2 are directly connected, making believe that "A" is a neighbor node of "J".

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].

2.2 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 precisely the rationale for this article: Analyze these assertions and from them to study the recent implementation of the ECC to verify their behavior to an attack such as Wormhole.

2.3 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.

1. According to its mode of attack [14] Wormhole is classified as:

- *Wormhole using encapsulation*
- *Wormhole Out-of-Band Channel*
- *Wormhole with High Power Transmission*
- *Wormhole using Packet Relay*
- *Wormhole using Protocol Deviations*

2. Depending on whether the attackers are visible in the path [14] Wormhole is classified as:

- *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.

3. Depending on the resources used for the attack [2] Wormhole is classified as:

- *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.

2.4 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

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], [72].

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].

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].

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].

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].

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).

3. Elliptic Curve Cryptography (ECC)

3.1 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:

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

For example, a representation of an elliptic curve over the field of real numbers $\mathbb{R}$ would be as Figure 2.

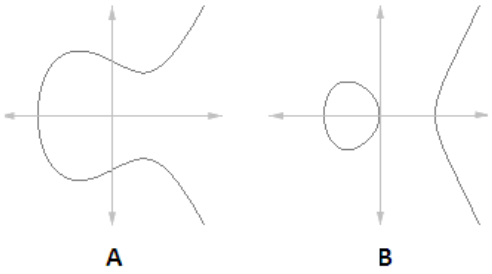

Fig 2. Elliptic curves over the field $\mathbb{R}$.

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 $a_1=a_2=a_3=a_5=0;\ a_4=-1$, i.e.:

$$\text{Curve A: } y^2 = x^3 - x + 1 \quad \text{Curve B: } y^2 = x^3 - x$$

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 $\mathbb{F}_{2^m}$). [45]
2. A Field representation (Polynomial or Normal Basis for $\mathbb{F}_{2^m}$) and the definition of the operations in computational levels (see figure 3).
3. A Type of elliptic curve E over $\mathbb{F}_q$ (Random curve or Koblitz curve) [52] and their Domain Parameters [49-51]
4. An Elliptic curve point representation (Affine Coordinates or Projective coordinates). [46], [54-57].

3.2 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 $A = (a_3a_2a_1a_0) \neq (0000)$.

3.3 Computational Levels and Field Representation

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

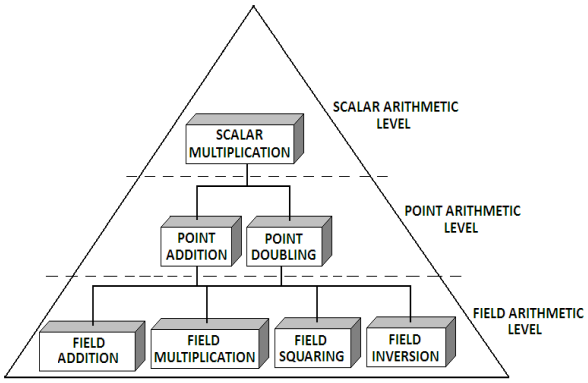

Fig 3. Computational levels of an ECC.

4. ECC Implementations for MANETs (Related Work)

4.1. 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: $Q = kG$. 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.

4.2. 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:

A. 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.

B. 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.

4.3. 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.

4.4. 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.

A. 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].

B. 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 paper (section 4.2). 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: [6], [53], [73 – 76]. Some proposals use Key Agreement Protocols as [47] that seeks resist the off-line password guessing attack, others simply apply ECDH in its Key Agreement Protocol as [37]. Other proposals applying ECC in MANET with Key Agreement are [64] and [36].

C. 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 [35]. In [34] 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 [33] 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.

5. ECC Implementation during Wormhole Attack in MANET

5.1. Security Requirements in MANETs

In order to combat passive and active attacks [32], according to [31] 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 [30] 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.

5.2. Key aspects to ensure security in MANET

In [30] and [24] 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 5.1:

Intrusion detection: Intrusion detection based on analysis of network behaviors.
Secure routing: Establishing a reliable and secure route between each pair of nodes.
Key management service: Generation of authentication, digital signature and encryption of information.

It is important to note that [30] and [23] 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.

5.3. Key Management Service Attributes

Returning to the Key Management Service aspect from the three previous Key aspects in section 5.2, when applying a security policy in MANET according to [32] a Key Management Service (For Example a: key agreement protocol) must conform to number of desirable attributes:
1. Known session keys. A protocol still achieves its goal in the face of an adversary who has learned some previous session keys.
2. Perfect forward secrecy. If long-term secrets of one or more entities are compromised, the secrecy of previous session keys is not affected.
3. 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.
4. 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.
5. Loss of information. Compromise of other information that would not ordinarily be available to an adversary does not affect the security of the protocol.
6. Message independence. Individual flows of a protocol run between two honest entities are unrelated.

Additionally, in [22] states that in terms of computation load a Key management service should fulfill:

-*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.

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

5.4. Levels of security against a Wormhole

Based on [9] and [21] 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:
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.
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.
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.
Analysing: 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.
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.
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.

5.5. Analysis

As we saw in section 2 of this paper, 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. As discussed in this paper (Section 5.2): in [30] and [24] 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 5.1?: 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 5.3) 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 2.2 of this paper 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 4.3, 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 5.4)? 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.

6. 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 paper, 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.

7. Future Work

Would be important to supplement the conclusions of this study, develop simulations of different ECC applications in MANET and analyze the behavior with a simulated Wormhole showing results that confirm this study. Also design and propose solutions that combine the three aspects of security in MANET: Intrusion Detection, Secure Routing and Key Management Service, implementing an ECC within the Key Management Service aspect to attack the Wormhole intrusion.

8. 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] 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.

[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] 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).

[22] 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.

[23] 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.

[24] 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.

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

[31] 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.

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

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

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[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] 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.

[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] 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.

[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] 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.

[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] 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.

Felipe Téllez earned a Computer Systems Engineer degree from the National University of Colombia in 2006. He is currently a M.Sc. (Candidate) in Computer Science from the National University of Colombia. Currently works as an IT Specialist at IBM Colombia. His research interests are mainly focused on Information Security, Cryptography, Ad-Hoc Networks, Simulations, Machine Learning among others.

Jorge Ortíz is an Associate Professor at the Department of Computer Systems and Industrial Engineering, National University of Colombia. He earned a Computer Systems Engineer degree, MSc in Statistics Degree, and MSc in Telecommunications Engineering degree from the National University of Colombia in 1995, 1999, and 2005 respectively. He earned a M. Phil. degree from the Javeriana University of Colombia in 2009. He is currently and PhD (candidate) in Computer Science from the National University of Colombia. His research work is mainly focused on Ad-Hoc Networks, Simulations, Artificial Intelligence, Probabilistic models, Theoretical Computer Science, Applied Computing among others. He has published more than 50 papers in different journals and international conferences.