UNIVERSIDAD SIMÓN BOLÍVAR | INSTITUTO DE POSGRADOS

DISEÑO DE UN MODELO DE AUTENTICACIÓN PARA FORTALECER LA SEGURIDAD A NIVEL DE ENRUTAMIENTO DEL PROTOCOLO OLSR EN UNA MANET

FEMNY JAVIER DIAZ JIMÉNEZ
femnydiaz@gmail.com
JOSE GREGORIO PALACIO VELÁSQUEZ
josepalacio@gmail.com

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de MAGISTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

RESUMEN

Las MANET (Mobile Adhoc Network) son redes sin infraestructura formadas por dispositivos móviles, estas redes se generan de forma espontánea, cuando los nodos, los cuales por lo general se encuentran en movimiento constante, se encuentran en el rango de distancia adecuado para poder unirse a la red, esta característica hace que la topología de la red sea muy variable y por lo tanto se requiere de algoritmos de enrutamiento que se adapten a dichos cambios, uno de estos algoritmos es el OLSR.

Uno de los problemas a los que se enfrentan estas redes, es el hecho de, que debido a sus características específicas, se vuelve un poco complicada la implementación de seguridad, ya que es muy difícil controlar la conexión de nodos maliciosos, debido al dinamismo de la misma. Teniendo en cuenta que en este tipo de redes cualquier nodo puede funcionar como enrutador para los otros nodos, es posible que un nodo malicioso, que se encuentre conectado a la MANET, intente inyectar tablas de enrutamiento falsificadas al resto de nodos, lo que afectaría el funcionamiento de la red. La finalidad de este proyecto es definir un mecanismo que permita asegurar dichas tablas de enrutamiento, a través de una técnica de autenticación.

Para dar solución a este problema, se realizó un diseño dividido en cuatro fases, la primera fase aborda el detalle de la conexión y autenticación del nodo, para lo cual se decidió por el uso de firma digital basada en algoritmos de cifrado asimétrico, para lo cual el nodo durante su fase de conexión a la red, le envíe su llave pública a todos sus vecinos, en la fase dos, se basa en un sistema de reputación, en el cual un nodo calcula la reputación de los diferentes nodos con los que ha tenido comunicación, definiendo si el mismo tiene mala o buena reputación, y generando un TLV de reputación, el cual es enviado al resto de nodos y calculando la misma según el esquema planteado basado en el Algoritmo de los generales bizantinos. La tercera fase se basa en la selección del nodo MPR, basado en la voluntad del

mismo para convertirse en MPR y el cálculo de la reputación realizado en la fase 2. Como última fase, para implementar autenticación y validar la integridad de las tablas de enrutamiento, se hará uso de la firma digital, basada en el hash del mensaje, del nodo junto con la tabla de enrutamiento.

Este diseño pretende disminuir en gran medida, no solo la conexión de nodos maliciosos a la red, sino que dado el caso, un nodo malicioso llegara a conectarse y se presentará pérdida de paquetes debido al mismo, el nodo terminaría siendo aislado de la red, ya que nunca haría parte del enrutamiento de paquetes, por su mala reputación.

El alcance de este proyecto llega hasta el diseño de la solución, la cual se basa en una combinación de técnicas que han demostrado ser eficientes en este tipo de redes, a futuro se podría trabajar en la implementación de la solución para medir su efectividad, y buscar algún otro mecanismo de medición de reputación para compararlo con el propuesto.

Antecedentes:

Las redes móviles, al igual que las redes convencionales, presentan una serie de problemas de seguridad, algunos generales, aplicables a diferentes tipos de redes otros muy puntuales de las MANETs, ataques como wormhole, blackhole, sybil, aislamiento de nodos, etc. Estos problemas han hecho que diferentes investigadores piensen en alternativas de solución para evitar que dichos ataques se puedan materializar, o por lo menos disminuir su impacto. Algunos de dichas soluciones van enfocadas a ataques particulares y otros a proteger contra múltiples ataques, teniendo claro que dichos ataques se concentran en alguna particularidad del funcionamiento de la red.

Algunas de dichas soluciones son:

(Sari, 2014) Presenta una evaluación de la seguridad en las MANET basadas en IEEE 802.11, a través de la propuesta de dos métodos; USM (Unified Security Mechanism) Mecanismo de Seguridad Unificado y RAS (Rate Adaptation Scheme) Esquema de Tasa de Adaptación, por medio del cual pretenden proteger las MANETs de ataques de denegación de servicio (DoS), dichos mecanismos fueron simulados utilizando simulador OPNET, generando ataques Jamming y comparando el rendimiento de cada mecanismo sobre la red específica.

(Honarbakhsh, Latif, Manaf, & Emami, 2014) Realizaron un estudio sobre mejoras de la seguridad en manets utilizando criptografía basada en identidad IBC, por sus siglas en inglés, en el cual se presenta un sistema de administración de llaves como una combinación de identificación de usuario, factor de tiempo de transmisión única y criptografía de umbral, basado en esquemas derivados del método de Shamir.

(Gharib & Belloulata, 2014) Presenta el artículo “Authentication Architecture Using Threshold Cryptography In Kerberos For Mobile Ad Hoc Networks”, en este los autores presenta una protección para Manet basado en un esquema de administración de llaves basados en criptografía de umbral, utilizando el protocolo de autenticación kerberos. El esquema implementa el método de criptografía de curva elíptica, el cual consume menos recursos y se encuentra bien adaptado para entornos inalámbricos.

(Samreen & Hyderv, 2015) También se enfocaron en estudiar la criptografía de umbral para implementar autenticación en Manets. Los autores se encuentran con una serie de inconvenientes, como la administración de llaves, sobrecarga de programación, trabajar sin una autoridad central, etc.

(Sengathir & Manoharan, 2015) Proponen un mecanismo de reputación para los nodos de una MANET basado en un Coeficiente de Confiabilidad Exponencial (ERCRM) que permite aislar los nodos egoístas, el coeficiente se mide a través de la tasa de falla exponencial basada en el método de promedio móvil, que almacena el comportamiento más reciente del nodo.

(Wei, Tang, Yu, Wang, & Mason, 2014) Los autores proponen un sistema de gestión de confianza basados en inferencia utilizando el razonamiento incierto originado por la comunidad de inteligencia artificial. El esquema de gestión de confianza propuesto posee dos componentes fundamentales, la confianza basada en la observación directa y la basada en la observación indirecta, la primera se basa en obtener el valor de confianza mediante inferencia bayesiana, tipo de razonamiento incierto que puede ser utilizado cuando se puede definir un modelo de probabilidad total, la confianza basada en observación indirecta, la cual se obtiene de los nodos vecinos y la que también es llamada como información de segunda mano, se obtiene basado en la teoría de Dempster-Shafer, el cual plantea otro tipo de razonamiento indirecto cuando la proporción de interés puede ser derivado por un método indirecto.

(Ahmed, Abu Bakar, Channa, Haseeb, & Khan, 2015) En este documento se presenta una revisión bibliográfica de modelos basados en confianza y reputación en redes de sensores y MANET, clasificándolos en dos grupos, modelos de confianza basados en nodos y modelos de confianza basados en el sistema.

(Ashish Kumar, Tokekar, & Shrivastava, 2016) Presentan un enfoque basado en el modelo de confianza fuzzy relacional binaria ponderada, buscando mitigar los ataques de agujero negro, específicamente en el protocolo AODV. En este enfoque se plantea modelar la confianza como un valor probabilístico denotado como un valor entre 0 y 1. Los resultados mostrados por los autores, demuestran que se presentó una mejora en el rendimiento del protocolo AODV durante un ataque de agujero negro.

En este documento los autores plantean un nuevo enfoque de cifrado asimétrico y dinámico, que les permita asegurar adecuadamente el tráfico de red, cuando se utiliza el protocolo OLSR, contra posibles ataques sin disminuir el rendimiento de la red.

(Mohit & Pal, 2015) Los autores proponen una solución a la que llaman W-OLSR, como una extensión del protocolo OLSR, esta solución no se orienta el tema de seguridad dentro del protocolo, sino que se concentra en buscar una mejora en la selección de los nodos MPR, incluyendo parámetros como la intensidad de la señal del nodo y el retardo en la transmisión, al incluir estos parámetros los autores mostraron mejoras en términos de movilidad y pérdida de paquetes, dentro de un ambiente simulado.

Objetivos:

Objetivo General

Diseñar un modelo de sistema de autenticación para fortalecer la seguridad en el encaminamiento de redes MANET que hacen uso del protocolo OLSR, con el fin de disminuir el riesgo de que nodos maliciosos (nodos rogue) afecten el funcionamiento de la red.

Objetivos Específicos

- Identificar las características del protocolo OLSR y requerimientos de autenticación para el mismo.
- Evaluar algoritmos de autenticación e identificar de estos cuál es el que mejor se adapta al protocolo OLSR.
- Definir el mecanismo de autenticación a partir de la integración del algoritmo de autenticación seleccionado con el protocolo OLSR.
- Diseñar el modelo propuesto del mecanismo de autenticación.

Materiales y Métodos:

Para la realización del proyecto se hizo uso de dos computadores, teniendo en cuenta que este proyecto se planteó para el diseño de un modelo, no se hizo uso de herramientas de software no de hardware especiales.

Los equipos utilizados se utilizaron para realizar el estudio del estado del arte y el diseño del modelo planteado.

Para esto se utilizador dos computadores portátiles.

- MacBook Air:
  - Fabricante: Apple
  - CPU: Intel Core i5 de 1.4 GHz
  - RAM: 4 GB
  - Disco Duro: 120 GB
- Portatil HP ProBook 430 G2:
  - Fabricante: Hewlett Packard
  - CPU: Intel Core i5 de 2.20 GHz Quinta Generación
  - RAM: 4 GB
  - Disco Duro: 500 GB

Resultados:

Se diseñó un modelo basado en cuatro fases como lo muestra la siguiente figura:

Fase 1: Establecimiento de la conexión

Esta fase tiene como finalidad definir los parámetros para el establecimiento de la conexión de los nodos nuevos que necesiten unirse a la red. Antes del establecimiento de la conexión los nodos deberán generar un par de llaves privada o pública, esto con miras a poder firmar digitalmente las tablas de enrutamiento enviadas entre los nodos MPR.

Durante la fase de establecimiento de la conexión, los nodos deberán enviar en sus mensajes HELLO un TLV con su llave pública, la cual será utilizada para la autenticación de los mensajes enviados por el nodo.

Fase 2: Cálculo de la Reputación del Nodo

El cálculo de la reputación es la base central del modelo, en este los nodos deberán determinar la reputación de sus nodos vecinos, este cálculo se realiza en dos subfases:

***Calculo de la reputación local del nodo*:** Cada nodo podrá calcular la reputación de sus nodos vecinos de manera local, haciendo uso del comportamiento de los mismos durante los procesos de retransmisión de los mensajes enviados por el nodo local, entre los procesos se cuentan mensajes no retransmitidos por el nodo vecino, paquetes mal formados, peticiones no respondidas y retraso en la transmisión.

***Calculo de la reputación final del nodo*:**

El cálculo de la reputación definitiva del nodo se realiza por consenso, para esto se hará uso de los valores de reputación enviados por los diferentes nodos, a través de los siguientes pasos:

1. Cada nodo envía a sus nodos vecinos las diferentes reputaciones calculadas a través de un TLV denominado NODES_REP, la reputación se enviará en el mismo orden en que se envían los bloques de direcciones.
2. Para el cálculo de la reputación final del nodo se usa el esquema de los Generales Bizantinos, basados en el siguiente algoritmo.

```
Si (Total_Nodos >= 3 * Nodos_Mala_Reputación + 1) Entonces
      Reputación = Entero(Promedio(Nodos_Buena_Reputación))
Sino
      Reputación = Entero(Promedio(Nodos_Mala_Reputación))
Fin Si
```

3. Se deberá crear una Base de Información de Reputación y almacenar en ella los valores calculados de reputación.

Fase 3: Selección de nodo MPR

La selección de nodos MPR sigue manteniendo el mismo concepto para su determinación, basado en el valor de MPR_WILLING, pero incluyendo un nuevo factor para determinar la selección, dicho factor es la reputación final del nodo, calculada según el algoritmo anterior.

1. Un nodo es un posible candidato a ser nodo MPR, ya que en el TLV MPR_WILLING, indicó una voluntad de 7 (WILL_ALWAYS) o un valor de voluntad válido.
2. El nodo verifica en la Base de Información de Reputación si el posible nodo MPR se encuentra registrado y si no se ha cumplido el tiempo de validez de la reputación, según los valores de INTERVAL_TIME y VALIDITY_TIME del mensaje.

```
Repetir
      Seleccionar Nodo con valor de voluntad válido
      Reputación = Reputación del Nodo
      Si (Reputación >= GOOD_REPUTATION) Entonces
            Nodo Seleccionado como MPR
      Fin Si
Hasta (Reputación >= GOOD_REPUTATION)
```

3. Se seleccionó nodo MPR.

Fase 4: Envío de información de enrutamiento

Las tablas de enrutamiento ya pueden ser enviadas por los nodos MPR que han sido seleccionados, para esto el nodo MPR deberá firmar el mensaje de enrutamiento haciendo uso de su llave privada, si se utilizó un algoritmo de cifrado asimétrico o de la llave generada si se utilizó un algoritmo simétrico, de esta manera el nodo MPR se encontrará autenticado, ya que el siguiente nodo MPR que reciba la tabla de enrutamiento, podrá validar la identidad del nodo, basado en su firma digital, la cual ya conoce de antemano.

Adicionalmente, los nodos deberán calcular el hash del mensaje de enrutamiento a enviar, lo que permitirá que los nodos puedan validar la integridad del mensaje al ejecutar el mismo algoritmo de hash utilizado por el emisor, de forma local, y comparar el hash enviado con el hash calculado localmente.

Conclusiones:

El resultado de este proyecto de investigación, plantea el diseño de una solución que permita garantizar que las tablas de enrutamiento que son intercambiadas por los diferentes nodos en una MANET, que implemente el protocolo OLSR, no sean alteradas, afectando el funcionamiento de la red.

Para llevar a cabo dicho diseño fue necesario hacer una investigación profunda sobre el funcionamiento del protocolo OLSR en su versión actual (versión 2), con la cual se trabajó, esta versión planteó muchos cambios en la forma como funcionaba el protocolo originalmente, haciendo uso de un elemento conocido como TLV que le agrega mucha versatilidad a OLSR y que sirvió de base para el diseño de la solución.

Durante el desarrollo del proyecto se plantearon y evaluaron varias alternativas de solución, y a través del estudio de un estado del arte, se encontraron diferentes enfoques para la implementación de seguridad en MANET. Todas las alternativas de solución analizadas se basaban en el uso de soluciones que han demostrado ser eficientes, en diferentes ambientes, no solo en el ambiente de las MANET. Uno de los inconvenientes más grandes fue buscar la manera de autenticar los nodos al inicio de la conexión a la red, teniendo en cuenta que los mecanismos de autenticación, utilizados por los diferentes autores, requieren de la interacción con el protocolo, por parte de elementos externos al mismo, lo que le quitaría parte de la espontaneidad del protocolo, por eso se optó por simplemente enviar en un TLV una llave, con el fin de utilizarla como herramienta para firmar los mensajes. Un problema que se puede llegar a presentar en esta parte de la solución, consiste en la selección del algoritmo de cifrado, para lo cual se recomiendan algunos detalles a tener en cuenta para la selección del mismo, como es seleccionar algoritmos de cifrado simétrico, si las características del nodo, a nivel de recursos de hardware, no permitirían usar cifrado asimétrico debido alto consumo de recursos del mismo, con respecto a los algoritmos simétricos

Una característica importante es que el diseño final se basó en el hecho de no incluir elementos adicionales, como agentes o herramientas de software externas al protocolo, se basó simplemente en incluir mejoras orientadas a la estructura

propia del protocolo, por lo cual la solución planteada se centró en el diseño de nuevos TLV.
Teniendo en cuenta todo esto se planteó la propuesta de diseño presentada, en la cual se propone un sistema de cuatro fases, conexión a la red, cálculo de reputación de nodos, selección de nodo MPR basado en la reputación calculada y firma digital de las tablas de enrutamiento para garantizar la integridad y autenticidad de las mismas.

Palabras clave:
OLSR, MPR, Criptografía, Firma Digital, Generales Bizantinos. Reputación.

ABSTRACT

The MANET (Mobile Adhoc Network) are networks without infrastructure formed by mobile devices, these networks are generated spontaneously, when the nodes, which are usually in constant movement, are in the right distance range to be able to join to the network, this feature makes the topology of the network very variable and therefore requires routing algorithms that adapt to these changes, one of these algorithms is the OLSR.
One of the problems faced by these networks is the fact that due to their specific characteristics, the implementation of security becomes a bit complicated, since it is very difficult to control the connection of malicious nodes, due to the dynamism of the same. Taking into account that in this type of networks any node can function as a router for the other nodes, it is possible that a malicious node, which is connected to the MANET, tries to inject falsified routing tables to the rest of the nodes, which would affect the operation of the network. The purpose of this project is to define a mechanism to ensure these routing tables, through an authentication technique.
To solve this problem, a design was divided into four phases, the first phase addresses the detail of the connection and authentication of the node, for which it was decided to use a digital signature based on asymmetric encryption algorithms, specifically RSA , for which the node during its phase of connection to the network, sends its public key to all its neighbors, in phase two, it is based on a reputation system, in which a node calculates the reputation of the different nodes with which it has had communication, defining if it has bad or good reputation, and generating a TLV of reputation, which is sent to the rest of the nodes and calculating the same according to the proposed scheme based on the Algorithm of the Byzantine generals. The third phase is based on the selection of the MPR node, based on the will of the same to become MPR and the calculation of the reputation performed in phase 2. As a last phase, to implement authentication and validate the integrity of the routing tables, use will be made of the digital signature, based on the hash of the message, of the node together with the routing table.
This design aims to reduce to a large extent, not only the connection of malicious nodes to the network, but if necessary, a malicious node will connect and there will

be packet loss due to it, the node would end up being isolated from the network, since it would never be part of packet routing, because of its bad reputation.
The scope of this project goes to the design of the solution, which is based on a combination of techniques that have proven to be efficient in this type of networks, in the future we could work on the implementation of the solution to measure its effectiveness, and look for some other mechanism of reputation measurement to compare it with the proposed one.

Background:
Mobile networks, like conventional networks, present a series of security problems, some general, applicable to different types of networks, others very specific to MANETs, attacks such as wormhole, blackhole, sybil, node isolation, etc. These problems have led different researchers to think of alternative solutions to prevent such attacks from materializing, or at least lessen their impact. Some of these solutions are focused on particular attacks and others to protect against multiple attacks, being clear that these attacks focus on some particularity of the operation of the network.
Some of these solutions are:
(Sari, 2014) Presents an evaluation of the security in the MANET based on IEEE 802.11, through the proposal of two methods; USM (Unified Security Mechanism) Unified Security Mechanism and RAS (Rate Adaptation Scheme) Adaptation Rate Scheme, by means of which they intend to protect MANETs from denial of service (DoS) attacks, said mechanisms were simulated using OPNET simulator, generating Jamming attacks and comparing the performance of each mechanism on the specific network.
(Honarbakhsh, Latif, Manaf, & Emami, 2014) Conducted a study on security improvements in manets using IBC identity-based cryptography, in which a key management system is presented as a combination of User identification, unique transmission time factor and threshold cryptography, based on schemes derived from the Shamir method.
(Gharib & Belloulata, 2014) Presents the article “Authentication Architecture Using Threshold Cryptography In Kerberos For Mobile Ad Hoc Networks”, in this the authors presents a protection for Manet based on a key management scheme based on threshold cryptography, using the Kerberos authentication protocol The scheme implements the elliptic curve cryptography method, which consumes less resources and is well adapted for wireless environments.
(Samreen & Hyderv, 2015) They also focused on studying threshold cryptography to implement authentication in Manets. The authors are faced with a series of drawbacks, such as key management, programming overhead, working without a central authority, etc.
(Sengathir & Manoharan, 2015) Propose a reputation mechanism for the nodes of a MANET based on an Exponential Reliability Coefficient (ERCRM) that allows to isolate the selfish nodes, the coefficient is measured through the exponential failure rate based on the moving average method, which stores the most recent node behavior.

(Wei, Tang, Yu, Wang, & Mason, 2014) The authors propose a trust management system based on inference using uncertain reasoning originated by the artificial intelligence community. The proposed trust management scheme has two fundamental components, the trust based on direct observation and the one based on indirect observation, the first is based on obtaining the value of trust through Bayesian inference, type of uncertain reasoning that can be used when a total probability model can be defined, the confidence based on indirect observation, which is obtained from the neighboring nodes and which is also called as second-hand information, is obtained based on the Dempster-Shafer theory, which raises Another type of indirect reasoning when the interest rate can be derived by an indirect method.

(Ahmed, Abu Bakar, Channa, Haseeb, & Khan, 2015) This document presents a bibliographic review of models based on trust and reputation in sensor networks and MANET, classifying them into two groups, trust models based on nodes and models Trusted based on the system.

(Ashish Kumar, Tokekar, & Shrivastava, 2016) Present an approach based on the weighted binary relational fuzzy confidence model, seeking to mitigate black hole attacks, specifically in the AODV protocol. In this approach it is proposed to model confidence as a probabilistic value denoted as a value between 0 and 1. The results shown by the authors show that there was an improvement in the performance of the AODV protocol during a black hole attack.

In this document, the authors propose a new approach to asymmetric and dynamic encryption, which allows them to adequately secure network traffic, when using the OLSR protocol, against possible attacks without decreasing network performance.

(Mohit & Pal, 2015) The authors propose a solution that they call W-OLSR, as an extension of the OLSR protocol, this solution does not address the issue of security within the protocol, but instead focuses on seeking an improvement in the MPR node selection, including parameters such as node signal strength and transmission delay, by including these parameters the authors showed improvements in terms of mobility and packet loss, within a simulated environment.

Objective:

General objective

Design an authentication system model to strengthen security in routing MANET networks that use the OLSR protocol, in order to reduce the risk of malicious nodes (rogue nodes) affecting the operation of the network.

Specific objectives

- Identify the characteristics of the OLSR protocol and authentication requirements for it.
- Evaluate authentication algorithms and identify which one best suits the OLSR protocol.
- Define the authentication mechanism based on the integration of the selected authentication algorithm with the OLSR protocol.
- Design the proposed model of the authentication mechanism.

Materials and Methods:

For the realization of the project, two computers were used, taking into account that this project was proposed for the design of a model, no special non-hardware software tools were used.

The equipment used was used to carry out the study of the state of the art and the design of the proposed model.

For this, two portable computers were used.

- MacBook Air:
  - Manufacturer: Apple
  - CPU: Intel Core i5 1.4 GHz
  - RAM: 4 GB
  - Hard Disk: 120 GB
- HP ProBook 430 G2 notebook:
  - Manufacturer: Hewlett Packard
  - CPU: Intel Core i5 2.20 GHz Fifth Generation
  - RAM: 4 GB
  - Hard Disk: 500 GB

Results:

A model based on four phases was designed as shown in the following figure:

Phase 1: Connection establishment

This phase aims to define the parameters for establishing the connection of the new nodes that need to join the network. Before the connection is established, the nodes must generate a private or public pair of keys, in order to be able to digitally sign the routing tables sent between the MPR nodes.

During the connection establishment phase, the nodes must send in their HELLO messages a TLV with their public key, which will be used for the authentication of the messages sent by the node.

Phase 2: Calculation of Node Reputation

The calculation of the reputation is the central base of the model, in this the nodes must determine the reputation of their neighboring nodes, this calculation is carried out in two subphases:

Calculation of the local reputation of the node: Each node can calculate the reputation of its neighboring nodes locally, making use of their behavior during the retransmission processes of the messages sent by the local node, among the processes are not retransmitted by the neighboring node, badly formed packets, unanswered requests and transmission delay.

Calculation of the node's final reputation:

The calculation of the definitive reputation of the node is done by consensus, for this purpose the reputation values sent by the different nodes will be used, through the following steps:

1. Each node sends to its neighboring nodes the different reputations calculated through a TLV called NODES_REP, the reputation will be sent in the same order in which the address blocks are sent.
2. The Byzantine Generals scheme, based on the following algorithm, is used to calculate the final reputation of the node.

```
If (Total_Nodes >= 3 * Bad_Reputation_Nodes + 1) Then
      Reputation = Integer (Average (Good_Nodes_Reputation))
Else
      Reputation = Integer (Average (Bad_Reputation_Nodes))
End If
```

3. A Reputation Information Base must be created and stored in it the calculated reputation values.

Phase 3: MPR node selection

The selection of MPR nodes continues to maintain the same concept for its determination, based on the value of MPR_WILLING, but including a new factor to determine the selection, said factor is the final reputation of the node, calculated according to the previous algorithm.

1. A node is a possible candidate to be an MPR node, since in the TLV MPR_WILLING, it indicated a will of 7 (WILL_ALWAYS) or a valid will value.
2. The node verifies in the Reputation Information Base if the possible MPR node is registered and if the validity time of the reputation has not been met, according to the values of INTERVAL_TIME and VALIDITY_TIME of the message.

```
Repeat
      Select Node with valid will value
      Reputation = Node Reputation
      If (Reputation> = GOOD_REPUTATION) Then
            Node Selected as MPR
      End If
Until (Reputation > = GOOD_REPUTATION)
```

3. MPR node was selected.

Phase 4: Sending routing information

The routing tables can already be sent by the MPR nodes that have been selected, for this the MPR node must sign the routing message using its private key, if an asymmetric encryption algorithm or the generated key was used if used a symmetric algorithm, in this way the MPR node will be authenticated, since the next MPR node that receives the routing table, can validate the identity of the node, based on its digital signature, which you already know in advance.

Additionally, the nodes must calculate the hash of the routing message to be sent, which will allow the nodes to validate the integrity of the message by executing the same hash algorithm used by the sender, locally, and compare the hash sent with the hash calculated locally.

Conclusions:

The result of this research project, proposes the design of a solution that ensures that the routing tables that are exchanged by the different nodes in a MANET, that implements the OLSR protocol, are not altered, affecting the operation of the network.

To carry out this design it was necessary to make a thorough investigation on the operation of the OLSR protocol in its current version (version 2), with which it worked, this version raised many changes in the way the protocol originally

worked, making use of an element known as TLV that adds a lot of versatility to OLSR and that served as the basis for the design of the solution.
During the development of the project, several solution alternatives were raised and evaluated, and through the study of a state of the art, different approaches were found for the implementation of security in MANET. All the solution alternatives analyzed were based on the use of solutions that have proven to be efficient, in different environments, not only in the MANET environment. One of the biggest drawbacks was to look for ways to authenticate the nodes at the beginning of the network connection, taking into account that the authentication mechanisms, used by the different authors, require interaction with the protocol, by elements external to it, which would take away part of the spontaneity of the protocol, so it was decided to simply send a key in a TLV, in order to use it as a tool to sign the messages. A problem that can be presented in this part of the solution is the selection of the encryption algorithm, for which some details are recommended to be taken into account for the selection of the same, such as selecting symmetric encryption algorithms, if the characteristics of the node, at the level of hardware resources, would not allow the use of asymmetric encryption due to its high consumption of resources, with respect to symmetric algorithms
An important feature is that the final design was based on the fact that it did not include additional elements, such as agents or software tools external to the protocol, it was based simply on including improvements oriented to the protocol's own structure, so that the proposed solution was focused on the design of new TLVs.
Taking all this into account, the design proposal presented was proposed, in which a four-phase system, network connection, node reputation calculation, MPR node selection based on the calculated reputation and digital signature of the tables are proposed of routing to guarantee their integrity and authenticity.

KeyWords:
OLSR, MPR, Cryptography, Digital Signature, Byzantine Generals. Reputation.

REFERENCIAS

1. Advanced Network Technologies Division Wireless Ad Hoc Network (s.f.) Recuperado 14 de julio de 2016, de http://www.antd.nist.gov/wahn_mahn.shtml.
2. Ahir, S. A., Marathe, N., & Padiya, P. (2014). IAMTT - New method for resisting network layer denial of service attack on MANET. Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT, 2016, 762–766. https://doi.org/10.1109/CSNT.2014.160
3. Ahmad, M., Chen, Q., Najam-Ul-Islam, M., Iqbal, M. A., & Hussain, S. (2018). On the secure optimized link state routing (SOLSR) protocol for MANETs. Proceedings of the 2017 12th International Conference on Intelligent Systems and Knowledge Engineering, ISKE 2017, 2018-Janua, 1–8. https://doi.org/10.1109/ISKE.2017.8258757
4. Ahmed, A., Abu Bakar, K., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Frontiers of Computer Science, 9(2), 280–296. https://doi.org/10.1007/s11704-014-4212-5
5. Álvarez, S., & Rios, M. (2013). Estudio Comparativo de las Soluciones Frente al Ataque Wormhole dentro de una MANET. Universidad SImón Bolívar.
6. Amraoui, H., Habbani, A., Hajami, A., & Bilal, E. (2016). Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model. Mobile Information Systems, 2016. https://doi.org/10.1155/2016/5653010
7. Aneiba, A., & Melad, M. (2016). Performance Evaluation of AODV, DSR, OLSR, and GRP MANET Routing Protocols Using OPNET. International Journal of Future Computer and Communication. https://doi.org/10.18178/ijfcc.2016.5.1.444
8. Bhuvaneswari, R., & Ramachandran, R. (2018a). Comparative Analysis of E-OLSR Algorithm in the Presence of Routing Attacks in MANET. International Journal of Sensors, Wireless Communications and Control, 8(1), 65–71. https://doi.org/10.2174/2210327908666180328163219
9. Bhuvaneswari, R., & Ramachandran, R. (2018b). Denial of service attack solution in OLSR based manet by varying number of fictitious nodes. Cluster Computing, 1–11. https://doi.org/10.1007/s10586-018-1723-0
10. Chang, J., Tsou, P., Woungang, I., Chao, H., & Lai, C. (2014). Defending Against Collaborative Attacks by Malicious Nodes in MANETs : A Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1), 65–75. https://doi.org/10.1109/JSYST.2013.2296197
11. Chiejina, E., Xiao, H., & Christianson, B. (2015). A dynamic reputation management system for mobile ad hoc networks. 6th Computer Science and Electronic Engineering Conference, CEEC 2014 - Conference Proceedings, 133–138. https://doi.org/10.1109/CEEC.2014.6958568
12. Chowdari, R., & Srinivas, K. (2017). A Survey on Detection of Blackhole and Grayhole Attacks in Mobile Ad-hoc Networks. International Research

Journal of Engineering and Technology (IRJET), 4(5), 1375–1378. https://doi.org/10.15680/IJIRCCE.2017.

13. Clausen, T., Dean, J., & Adjih, C. (2009). RFC 5444 - Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format. Internet Engineering Task Force (IETF). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC5444
14. Clausen, T., & Dearlove, C. (2009). RFC 5497 - Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC5497
15. Clausen, T., Dearlove, C., & Adamson, B. (2008). RFC 5148 - Jitter Considerations in Mobile Ad Hoc Networks. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC5148
16. Clausen, T., Dearlove, C., & Dean, J. (2011). RFC 6130 - Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP). Internet Engineering Task Force (IETF). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC6130
17. Clausen, T., Dearlove, C., Jacquet, P., & Herberg, U. (2014). RFC 7181 - The Optimized Link State Routing Protocol Version 2. Internet Engineering Task Force (IETF). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC7181
18. Clausen, T., Herberg, U., & Yi, J. (2017). RFC 8116 - Security Threats to the Optimized Link State Routing Protocol Version 2 (OLSRv2). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC8116
19. Clausen, T., & Jacquet, P. (2003). RFC 3626 - Optimized Link State Routing Protocol (OLSR). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC3626
20. Dearlove, C., & Clausen, T. (2014). RFC 7188 - Optimized Link State Routing Protocol Version 2 (OLSRv2) and MANET Neighborhood Discovery Protocol (NHDP) Extension TLVs. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC7188
21. Dearlove, C., & Clausen, T. (2015). RFC 7631 - TLV Naming in the Mobile Ad Hoc Network (MANET) Generalized Packet/Message Format. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC7631
22. Echchaachoui, A., Choukri, A., Habbani, A., & Elkoutbi, M. (2014). Asymmetric and dynamic encryption for routing security in MANETs. International Conference on Multimedia Computing and Systems - Proceedings, 0, 825–830. https://doi.org/10.1109/ICMCS.2014.6911237
23. Fernández-Bravo Peñuela, Francisco Javier; Bernabeu Aubán, J. M. (2018). Consenso Bizantino y Blockchain. Retrieved from https://riunet.upv.es/handle/10251/115369
24. Gadekar, M. S. (2017). Secure Optimized Link State Routing (OLSR) Protocol A gainst Node Isolation Attack. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 684–687.

25. Gharib, H., & Belloulata, K. (2014). AUTHENTICATION ARCHITECTURE USING THRESHOLD CRYPTOGRAPHY, 8(22), 12–18. https://doi.org/10.12913/22998624.1105141
26. Godwin, J., & Srinivasan, R. (2014). A Survey on MANET Security Challenges,, Attacks and its Countermeasures. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(1), 274–279.
27. Herberg, U. (Fujitsu L. of A., Clausen, T. (LIX, E. P., & Dearlove, C. (BAE S. A. (2014). RFC 7182 - Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs). Internet Engineering Task Force (IETF). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC7182
28. Herberg, U. (Fujitsu L. of A., Dearlove, C. (BAE S. A., & Clausen, T. (LIX, E. P. (2014). RFC 7183 - Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2). Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC7183
29. Honarbakhsh, S., Latif, L. B. A., Manaf, A. B. A., & Emami, B. (2014). Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography. International Journal of Computer and Communication Engineering, 3(1), 41–45. https://doi.org/10.7763/IJCCE.2014.V3.289
30. Hurley-Smith, D., Wetherall, J., & Adekunle, A. (2017). SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks. IEEE Transactions on Mobile Computing, 16(10), 2927–2940. https://doi.org/10.1109/TMC.2017.2649527
31. James, J. L., & Thomas, B. (2016). A Study on Preventing Node Isolation Attack in OLSR Protocol. Procedia Technology, 25(Raerest), 349–355. https://doi.org/10.1016/j.protcy.2016.08.117
32. Jaramillo, S. (2010). Servicios de Autenticación y Modelo de Seguridad en Redes Móviles Ad Hoc. La Universidad Católica de Loja.
33. Jubair, M. A., Khaleefah, S. H., Budiyono, A., Mostafa, S. A., & Mustapha, A. (2018). Performance Evaluation of AODV and OLSR Routing Protocols in MANET Environment, 8(4), 1277–1283.
34. Kaur, N., Joshi, M., & Nagar, Y. (2014). Implementing MANET Security using CBDS for Combating Sleep Deprivation & DOS Attack, 16(1), 6–11.
35. Kumar, Amit, & Singla, V. (2016). Detecting and Avoiding Sybil Attack in OLSR Protocol. International Journal of Control Theory and Applications, 5(5), 1905–1910.
36. Kumar, Ashish, Tokekar, V., & Shrivastava, S. (2016). Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. Information and Communication Technology, Proceeding of ICICT 2016, 625, 3–5. https://doi.org/10.1007/978-981-10-5508-9_4
37. Kumar Jha, R., & Kharga, P. (2015). A Comparative Performance Analysis of Routing Protocols in MANET using NS3 Simulator. International Journal

of Computer Network and Information Security. https://doi.org/10.5815/ijcnis.2015.04.08

38. Kumar, N., & Tripathi, K. (2017). Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26, 5(5), 194–205.
39. Litvinov, G. A. (2018). Applying Static Mobility Model in Relaying Network Organization in Mini-UAVs Based FANET. 2018Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 1–7.
40. Mishra, R., Kaur, I., & Sharma, S. (2010). New trust based security method for mobile ad-hoc networks Sanjeev sharma widely used in military and other scientific areas with nodes which can move. International Journal of Computer Science and Security, 4(3), 346–351.
41. Mohit, M., & Pal, S. (2015). Stable MPR Selection in OLSR for Mobile Ad-Hoc Networks. International Journal of Computer Science and Information Technologies, 6(6), 5121–5125.
42. Najafpour, B., Mahdavi, B., Soleimani, P., & Rahmani, R. (2016). Optimizing Security Issue Of OLSR Routing Protocol Based On Trust Method in Wireless Sensor Networks. International Journal of Research in Computer Applications and Robotics, 4(3), 27–37.
43. Narten, T., & Alvestrand, H. (2008). RFC 5226 - Guidelines for Writing an IANA Considerations Section in RFCs. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC5226
44. Patil, G. M., Kumar, A., & Shaligram, A. D. (n.d.). Performance Comparison of MANET Routing Protocols (OLSR, AODV, DSR, GRP and TORA) Considering Different Network Area Size. International Journal of Engineering and Management Research, (3). Retrieved from www.ijemr.net
45. Pérez-Solà, C., & Herrera-Joancomartí, J. (2014). Bitcoin y el problema de los generales bizantinos. Actas de La XIII Reunión Española de Criptología y Seguridad de La Información (RECSI 2014), 241–246. Retrieved from http://hdl.handle.net/10045/40444
46. Pouyan, A., & Yadollahzabeh, M. (2015). FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network. International Journal of Communication Systems, 31(2), 361–386. https://doi.org/10.1002/dac
47. Rajaram, A., & Palaniswami, S. (2010). Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol. International Journal of Computer Science Ans Information Technologies, 1(2), 130–137.
48. Rani, V. I., & Reddy, K. T. (2017). To Improve The Security Of OLSR Routing Protocol Based On Local Detection Of Link Spoofing, 5(6), 652–655.
49. Raza, N., Umar Aftab, M., Qasim Akbar, M., Ashraf, O., & Irfan, M. (2016). Mobile Ad-Hoc Networks Applications and Its Challenges. Communications and Network, 08(03), 131–136. https://doi.org/10.4236/cn.2016.83013
50. Rocabado, S. (2013). Caso de estudio de comunicaciones seguras sobre redes móviles Ad Hoc. Universidad Nacional de la Plata. https://doi.org/10.13140/RG.2.1.3336.4963

51. Sallam, G., & Mahmoud, A. (2015). Performance Evaluation of OLSR and AODV in VANET Cloud Computing Using Fading Model with SUMO and NS3. 2015 International Conference on Cloud Computing, ICCC 2015, 1–5. https://doi.org/10.1109/CLOUDCOMP.2015.7149649
52. Samreen, A., & Hyderv, S. I. (2015). Role of Threshold Cryptography in Securing MANETs, 15(1), 106–112.
53. Santiago, E. (2005). Posibilidades de las MANET (Mobile Ad-Hoc Networks) y Algunas otras Redes Inalámbricas. Prospectiva, 3(2), 44–46.
54. Santiago, E., & Sánchez, J. (2017). Riesgos de Ciberseguridad en las Empresas. Revista Tecnologí@ y Desarrollo, XV. Retrieved from http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas.pdf
55. Sari, A. (2014). Security Approaches in IEEE 802 . 11 MANET — Performance Evaluation of USM and RAS, (September), 365–372. https://doi.org/10.4236/ijcns.2014.79038
56. Sengathir, J. (2015). A Split Half Reliability Coefficient Based Mathematical Model for Miyigating Selfish Nodes in MANETs, (August).
57. Sengathir, J., & Manoharan, R. (2015). Exponential reliability factor based mitigation mechanism for selfish nodes in MANETs. Egyptian Informatics Journal, 4(1), 43–64. https://doi.org/10.7603/s40632-016-0003-5
58. Sharma, S., & Kumar, M. A. (2016). Performance Analysis of OLSR, AODV, DSR MANETs Routing Protocols. International Journal of Engineering Science and Computing. https://doi.org/10.4010/2016.1871
59. Shen, H., & Li, Z. (2015). A hierarchical account-aided reputation management system for MANETs. IEEE/ACM Transactions on Networking, 23(1), 70–84. https://doi.org/10.1109/TNET.2013.2290731
60. Singh, K., & Verma, A. K. (2015). Applying OLSR routing in FANETs. Proceedings of 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014, (May 2015), 1212–1215. https://doi.org/10.1109/ICACCCT.2014.7019290
61. Subba, B., Biswas, S., & Karmakar, S. (2016). Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal, 19(2), 782–799. https://doi.org/10.1016/j.jestch.2015.11.001
62. Tan, S., Li, X., & Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30(March), 84–98. https://doi.org/10.1016/j.adhoc.2015.03.004
63. Vellingiri, J., & Saravanan, K. (2017). Defending MANET Against Flooding Attack for Medical Application. 2nd International Conference on Comunication and Electronics Systems, (Icces), 486–489.
64. Wang, S., & Xia, H. (2018). A Reputation Management Framework for MANETs. 2018 IEEE Symposium on Privacy-Aware Computing (PAC), 119–120. https://doi.org/10.1109/PAC.2018.00019
65. Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using

uncertain reasoning. IEEE Transactions on Vehicular Technology, 63(9), 4647–4658. https://doi.org/10.1109/TVT.2014.2313865

66. Wu, Y., Xu, L., Lin, X., & Fang, J. (2017). A New Routing Protocol Based on OLSR Designed for UANET Maritime Search and Rescue. In S.-L. Peng, G.-L. Lee, R. Klette, & C.-H. Hsu (Eds.), Internet of Vehicles. Technologies and Services for Smart Cities (pp. 79–91). Cham: Springer International Publishing.