Aspectos de seguridad para sistemas de cómputo social-inspirados construidos sobre manets

Security aspects for social-inspired computing systems built on manets

Santiago José Molina Sanchez[*]
Jorge Eduardo Ortiz Triviño[**]
Henry Zarate Ceballos[***]

DOI: https://doi.org/10.18041/1909-2458/ingeniare.2.2884

RESUMEN

El presente artículo realiza una revisión literaria sobre el presente y los avances futuros que se esperan en temas relacionados con seguridad informática para sistemas de cómputo basados en MANETs (Mobile Ad hoc Network), además, expone las principales características que deberían tener los modelos de seguridad y cómo se podrían aplicar al modelo social-inspirado TLÖN. Se da una revisión a las redes definidas por software (SDN) y cómo se podrían aplicar a sistemas inalámbricos como las redes Ad hoc, el articulo describe los principales ataques sobre una red Ad hoc y cómo mediante los atributos de seguridad: confidencialidad, integridad y disponibilidad, se pueden resolver algunos de los problemas principales de seguridad.

Palabras claves: seguridad en redes, redes ad hoc, virtualización, redes definidas por software, redes inalámbricas, ataques en redes ad hoc.

ABSTRACT

The present paper makes a literary review about the present and future advances that are expected in security for Ad hoc networks, furthermore, it exposes the principal features that the security models should have it and how could the social-inspired model TLÖN have it. The Software Defined Network (SDN) are revised and how could they be applied to wireless systems like Ad hoc networks, the article describes the main attacks on an Ad hoc network and how could Through the attributes of security: Confidentiality, Integrity, Availability, resolve some of the main problems of security.

Keywords: network security, ad hoc network, virtualization, software defined network, wireless network, attacks on ad hoc networks.

Como citar:
Molina Sanchez S, Ortiz Triviño J, Zarate Ceballos H. Aspectos de seguridad para sistemas de cómputo social-inspirados construidos sobre manets. ingeniare [Internet]. 12sep.2017 [citado diames.año2018];23(2). Available from: http://revistas.unilibre.edu.co/index.php/ingeniare/article/view/2884

[*] *Ingeniero electrónico. Universidad Nacional de Colombia, facultad de ingeniería, estudiante de maestría en ingeniería de telecomunicaciones, grupo de investigación TLÖN. sjmolinas@unal.edu.co*
[**] *Doctor en ingeniería de sistemas y computación. Universidad Nacional de Colombia, facultad de ingeniería, profesor asociado, director del grupo de investigación TLÖN. jeortizt@unal.edu.co*
[***] *Magister en ingeniería de telecomunicaciones. Universidad Nacional de Colombia, estudiante de doctorado en ingeniería de sistemas y computación, grupo de investigación TLÖN. hzaratec@unal.edu.co*

Fecha de recepción: 16 de mayo de 2017 • Fecha de aceptación: 06 de septiembre de 2017 • Fecha de publicación: 12 de septiembre de 2017

1. INTRODUCCIÓN

Los modelos social- inspirados proponen controlar interacciones entre agentes e incluso controlar componentes éticos imposibles en sociedades reales pero posible en sociedades artificiales, los modelos social- inspirados idealizan los principios de justicia, inmanencia y da paso a principios derivados, como la equidad, la solidaridad y la aparición de virtudes como la verdad. Una característica de los sistemas social-inspirados es la cooperación entre los agentes de una comunidad, siendo una comunidad, una asociación más o menos autosuficiente de agentes que en sus relaciones reconocen ciertas reglas de conducta como obligatorias y que en su mayoría están de acuerdo con ellas [1].

Un rasgo de la comunidad de agentes es su movilidad y una racionalidad que no limita su régimen de comportamiento. Una idea para implementar estos modelos sociales en sistemas computacionales, nace con la analogía de un esquema que proporcione la movilidad y la autoorganización de una comunidad de agentes, para esto, las redes inalámbricas son de gran utilidad como solución para la operación de equipos que no pueden permanecer en un lugar estático, pero que deben cubrir las demandas de un entorno en el cual los dispositivos están en constante movimiento, como lo son los vehículos, celulares, redes de sensores, redes inalámbricas *Mesh*, entre otros [2]. Aquí es donde aparecen las redes MANET (*Mobile Ad hoc Network*), formalmente, las redes MANET son un grafo aleatorio con un conjunto de vértices, comúnmente llamados nodos, en este caso móviles, unidos por un conjunto de enlaces denominados aristas, que cambian de forma dinámica en función del tiempo y las condiciones del ambiente. Por ejemplo, las peticiones de los usuarios [3]. Es por esto que este tipo de sistemas pueden ser capaces de generar comportamientos pseudosociales desde el instante de su conformación hasta el fin de su operación. Adicionalmente, se hace necesario el uso de un modelo de virtualización inalámbrica para cubrir con las necesidades de un modelo social-inspirado, las redes SDN (*Software Defined Network*) mejoran su desempeño a través de la visión de red global ofrecida por un controlador centralizado, además prometen simplificar drásticamente su gestión [4].

Debido al tipo de sistemas computacionales en los que se pretenderían implementar los modelos social-inspirados, surgen nuevos retos en cuestiones de seguridad, por ejemplo, ¿cómo es posible alcanzar un nivel de seguridad optimo en una red que es altamente dinámica y descentralizada, donde ningún dispositivo de seguridad como un firewall, tradicional de una red cableada, funcionaria? o ¿cómo se proporciona seguridad a un sistema de virtualización inalámbrica?. Es importante resaltar que el número de amenazas que podrían afectar un sistema crece a diario y sin un sistema que contrarreste este tipo de amenazas, será imposible concebir un sistema social-inspirado. El presente artículo pretende hacer una revisión literaria de las soluciones actuales en cuestiones de seguridad para redes MANET y redes SDN, adicionalmente, presenta el modelo social-inspirado TLÖN.

2. FUNDAMENTACIÓN TEÓRICA Y METODOLOGÍA

El propósito del presente artículo se enmarca en la seguridad de sistemas de cómputo implementados sobre redes MANET y busca hacer una revisión literaria en los avances actuales que puedan dar un camino para solucionar las siguientes preguntas.

- ¿Existen amenazas que afecten las redes inalámbricas y las redes MANET?
- ¿Cómo es posible alcanzar un nivel de seguridad optimo en una red que es altamente dinámica y descentralizada, donde ningún dispositivo de seguridad como un firewall, tradicional de una red cableada, funcionaria?
- ¿Cómo se proporciona seguridad a un sistema de virtualización inalámbrica?
- ¿Existen amenazas que afecten los sistemas de redes definidas por software?

La búsqueda de información se basa en las preguntas anteriormente mencionadas y se tienen en cuenta artículos científicos, libros y estándares. El atributo principal para la selección e inclusión de los artículos científicos es que deben estar publicados en la plataforma de la IEEE, Springer Journal y Scopus. La búsqueda se realizó mediante las palabras claves mencionadas en este artículo. Se busca que la información esté relacionada con algún modelo computacional socio-inspirado o dé una solución en seguridad para redes MANET o redes SDN.

2.1. Redes inalámbricas definidas por software (WSDN).

Una variante de las redes SDN son las Wireless Software Defined Networking o por sus siglas WSDN, las cuales también tienen su fundamento en el software, pero introducen un número de nuevos elementos como, el medio inalámbrico, la funcionalidad de expandir el plano de datos y una estructura altamente dinámica [3]. WSDN asegura una simple y escalable arquitectura de red y una efectiva gestión de movilidad para áreas geográficamente extensas y un servicio estándar de proveedor de red [5]. Existen muchos requerimientos que debe satisfacer una red WSDN como la necesidad de soportar la movilidad de nodos y los cambios en una topología de red, o de solucionar la falta de disponibilidad característica de los enlaces inalámbricos [6]. En fig. 1 se ve la arquitectura clásica de una red SDN, la cual sirve de guía para agregar elementos como un medio inalámbrico basados en una efectiva gestión de movilidad. Las redes WSDN son una fuente de soluciones a problemas de la vida cotidiana, además de ser la tecnología con el crecimiento de mercado más alto tal como dicen [7, 8], para el año 2014 el mercado de las tecnologías SDN fue de 1.4 billones de dólares y se estima que para el año 2019 este crecimiento alcance los 4.6 billones de dólares.

Las aplicaciones de las redes WSDN son muy variadas en cualquier entorno y son un perfecto ejemplo de las tecnologías futuras, ya que se ha extendido a redes de sensores, SDN en redes vehiculares, SDN en Smart GRID, SDN en redes celulares, entre otro [9, 10]. El concepto de WSDN se ha ampliado

y ahora presenta una nueva arquitectura que elimina la necesidad de inundación multisalto para descubrir una ruta.

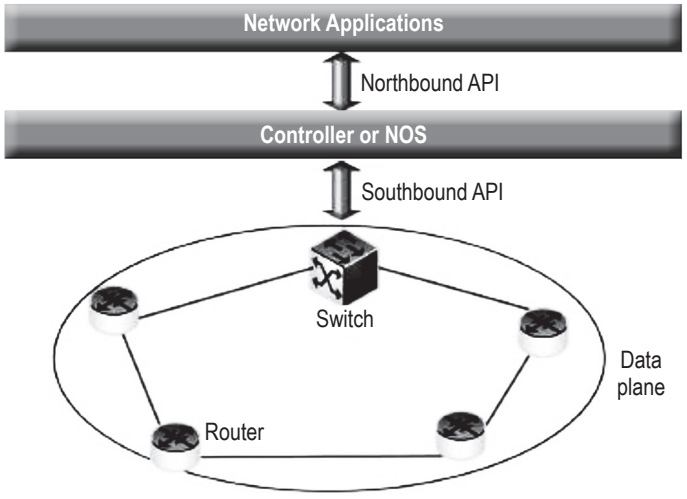

Figura 1. Arquitectura de una red definida por software.

Fuente: [11].

La tecnología WSDN puede ser un gran aliado para los objetivos de una red MANET. Un análisis de la arquitectura de las redes móviles AD hoc, propone una organización jerárquica que está compuesta de un control centralizado, nodos regulares, y un conjunto de nodos de retardo para conectar esos nodos al controlador [11]. Algunos modelos de redes definidas por software móviles [12] permiten a los operadores el reenvió basado en flujo y fomentan un ambiente rico para la innovación de una red móvil. En la tabla 1 se ve una comparación entre algunas de las características de una red cableada tradicional y una red definida por software, de la tabla se puede deducir que las redes SDN tiene ventajas considerables en la escalabilidad y en una gestión más optima, características que son fundamentales en un entorno que demande alta movilidad y dinamismo.

Tabla 1. Comparación entre Networking tradicional y SDN/WSDN

	Networking tradicional	Red definida por software (SDN/WSDN)
Planos de control y transporte	Ambos situados en elementos de la red	Plano de control separado del de transporte y situado en el controlador
Control	Distribuida por los elementos de la red	Centralizada en el controlador SDN
Gestión de la red	Cada elemento de la red se configura por separado	El controlador puede exponer interfaces de aplicación para la manipulación de la red.
Políticas y seguridad	La aplicación de políticas necesita cambios en los dispositivos de nivel	La aplicación de políticas se vuelve simplificada y consistente
Escalabilidad	La escalabilidad es insostenible después de un tiempo debido a la alta complejidad	La escalabilidad es fácil debido al ágil control centralizado

Fuente: adaptado de [11].

2.2. Seguridad en redes inalámbricas

Existen diferentes vectores de amenaza que pueden afectar el funcionamiento de una red inalámbrica, tales como, ataques de negación de servicio, virus, ataques de hombre en el medio, entre otros [13]. Los ataques de negación de servicio afectan la disponibilidad de las redes, ya que un atacante o varios realizan un envío de paquetes hasta saturar un servidor y dejar sin servicio la red, en [14] se propone una detección de ataques en la capa MAC (*Medium Access Control*) para redes inalámbricas, y de esta forma evitar ataques de negación de servicio. En [15] discuten lo critico que es la seguridad en una red de sensores inalámbricos y resaltan varias técnicas para detectar y prevenir ataques de agujero negro, proponiendo un modelo para conservar la energía, en [16] también se propone un modelo para prevenir ataques de agujero negro en redes de sensores inalámbricos, pero basan el modelo en la técnica de aprendizaje basada en conocimiento para detectar y mitigar nodos dañinos. Los ataques de hombre en el medio afectan la confidencialidad de la red, ya que los mensajes enviados pueden ser leído y espiados por intrusos [17]. Los ataques de manipulación de mensajes afectan la integridad de la red, un atacante puede manipular el mensaje y entregar al recibidor un mensaje alterado y por lo tanto incorrecto [18]. En fig. 2 se encuentra un resumen de los ataques más comunes en una red Ad hoc vehicular.

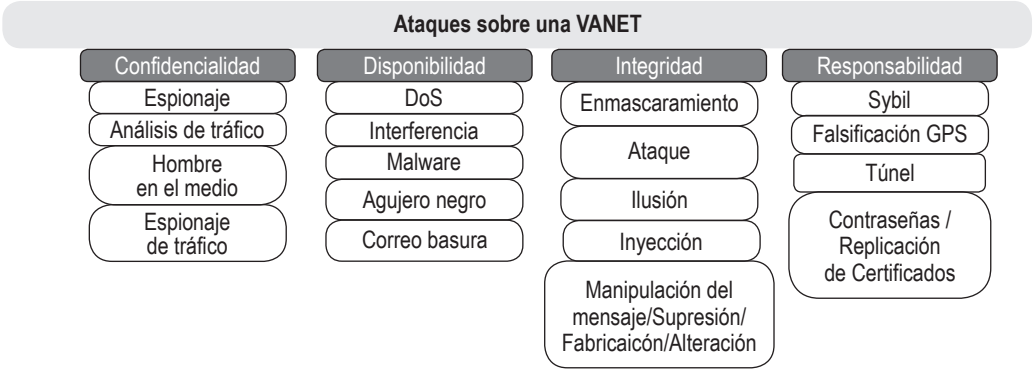

Figura 2. Ataques sobre una VANET.

Fuente: Adaptado de [14][11].

2.3. Seguridad definida por software.

El campo más fuerte en el desarrollo de la seguridad en las redes Ad hoc es el automotor con las redes VANET (Vehicular Ad hoc Network).Como se ve en [17, 18, 2] , se ofrecen soluciones para ciberataques. Uno de estos estudios, ha estado basado en un sistema de “Seguridad Definida por Software” (SDS), donde la información de seguridad es implementada, controlada y manejada por un software. En resumen, SDS es un software controlador, un dirigente de políticas, donde la mayoría de controles de seguridad, tales como la detección de intrusos, la segmentación de la red y los controles de acceso, son automatizados y monitoreados [10, 19, 20]. SDS introduce simplicidad al mundo de la seguridad en redes, pues en este modelo la protección está basada en políticas lógicas y, no depende de ningún

servidor o dispositivo especializado en seguridad. Además, es adaptativa, ya que la virtualización de la seguridad es alcanzada por la abstracción y agrupación de recursos de seguridad a través de límites [21]. El punto principal es que la capa de control se separa de la capa de datos y protege el ambiente SDN a través del controlador SDS. En esta arquitectura general, las SDN están siempre divididas en tres niveles principales, la capa física (ejecuta las estrategias generadas en la capa de control superior), la capa de control (ordena a la capa de seguridad qué es lo que debe hacer) y capa de aplicación (es la única visible al usuario, pues todas las aplicaciones son desplegadas en esta capa) [19]. Estudios recientes [15] usan un modelo SDS para detectar y prevenir ataques de espionaje sobre la red, en [22] sugiere ser empleado SDS para ofrecer control de acceso programable para VANET.

2.4. Seguridad en redes móviles Ad hoc

En las redes Ad hoc existen ataques que afectan la confidencialidad, como en el conocido *man-in-the-middle*, donde la información es interceptada o escuchada por terceras personas [2, 23]. Algunas soluciones para este tipo de ataques involucran la criptografía y análisis de tráfico, como en [24], el cual proporciona un novedoso enfoque anti-espía basado en criptografía, o en [25], donde se desarrolla un nuevo esquema de gestión de llaves auto-organizable que usa criptografía basada en identidad. Otro tipo de ataque involucra la disponibilidad de los recursos de la red, su principal objetivo es tener los dispositivos de red ocupados para que en el momento de ser requeridos no estén disponibles. Como en el caso, de los ataques de negación de servicio o DoS, en los cuales un intruso inunda la red con paquetes basura que la congestionan y evitan que los dispositivos se puedan comunicar entre sí [26]. Existen diferentes ataques que pueden afectar la integridad de la información en una red Ad hoc, entre ellos están los ataques de agujero negro, en [27] utilizan un algoritmo con uso de *blockchain* para detectar ataques y remover nodos maliciosos en una red VANET. En [28] se propone un modelo de respuesta que identifica rutas maliciosas en nodos fuente e intermedios que estén sufriendo ataques de agujero negro y gris, y busca el camino más corto en una red MANET. En la tabla 2 se generalizan algunos de los tipos de ataques que pueden afectar una red Ad hoc.

Tabla 2 Ataques en redes Ad hoc

Ataque de fabricación	En esta situación el atacante crea un falso mensaje, en el cual miente acerca de la identidad y la localización del tráfico. El atacante prácticamente fabrica su propio anuncio de localización.
Ataque de alteración	En este caso los atacantes modifican la localización de otros nodos en la red
Ataque de pérdida de paquete	Los atacantes en forma de routers pueden botar los paquetes, ya sea en un agujero negro o un agujero gris
Replicación	Un atacante se comporta como un nodo que dejó de existir hace un tiempo.

2.5. Atributos de seguridad en una red móvil Ad hoc

Una red, realiza un intercambio de información muy sensible y debe usar algunos modelos para controlar los problemas de ataques. Diferente a otras comunicaciones tradicionales, donde los nodos debían tener acceso físico a la red o comunicarse a través de muchos perímetros de defensa como firewalls

y Gateway, los atacantes pueden usar el medio inalámbrico para atacar sobre una red inalámbrica, los ataques pueden venir de cualquier dirección y atacar cualquier nodo. Esto da como resultado una gama de ataques disponibles que pueden ser utilizados en la red [29].

En una red Ad hoc los atributos de seguridad se pueden enmarcar en [30] :

- Confidencialidad: es la propiedad en la cual cada aplicación o nodo tiene permiso para acceder a un conjunto específico de servicios y asegura la localización de la información y el almacenamiento de los datos, privacidad significa ocultar la identidad y la locación de los nodos de entes externos, en [31, 32] se hace una revisión literaria sobre las técnicas de detección de intrusos en una MANET.
- Autentificación: debe manejar la comunicación confiable entre dos o más nodos, es esencial verificar la identidad de todo nodo en la MANET y su elegibilidad para acceder a la red. En [33] se propone un robusto mecanismo para la autentificación de los nodos en MANETs, basado en el intercambio de certificados entre nodos.
- Disponibilidad: el nodo debe estar siempre disponible para proveer servicios y datos, incluso en la presencia de fallas o ataques maliciosos, tal como, un ataque DoS. En [34] se propone una estrategia para mejorar la disponibilidad basados en una replicación de datos tolerante a fallos de nodo.
- Integridad: los datos transmitidos entre los nodos de una MANET deberían ser recibidos en el nodo correspondiente sin que hayan sido estropeados o cambiados por modificaciones no autorizadas [35].

3. SEGURIDAD EN EL PROYECTO TLÖN

3.1. Sistema de cómputo sobre redes Ad hoc

Los sistemas de cómputo son un conjunto de elementos que interactúan entre sí, un sistema de cómputo puede tener la capacidad de compartir un sistema central de almacenamiento, bases de datos, entre otros periféricos y propiedades. Cada nodo conectado al sistema puede operar independientemente, pero tiene la posibilidad de comunicarse con otros dispositivos y computadores externos [36]. La capacidad que tiene el sistema para realizar la correcta interacción entre los dispositivos requiere de una robusta red que proporcione las características necesarias para el correcto funcionamiento del sistema. Las redes Ad hoc por sus propiedades dinámicas y de autoorganización proponen ser una buena herramienta para el buen funcionamiento de un sistema de cómputo.

3.2. Proyecto TLÖN

El proyecto del Grupo de investigación en redes de Telecomunicaciones Dinámicas & Lenguajes de Programación Distribuidos –TLÖN, propone un esquema de computación inspirado en modelos Sociales, inviables en la práctica pero muy posibles en entornos artificiales controlados, este sistema basado en los conceptos de Justicia de Jhon Rawls, inmanencia de Baruch de Spinoza, paradigma Thomas Kuhn, Estado Thomas Hobbes y las concepciones de existencia y esencia de Jean Paul Sartre, generan una

analogía completa de un esquema de virtualización inalámbrica, necesaria para implementar estos modelos sociales en sistemas computacionales, este modelo social inspirado, es una abstracción superior a los modelo bio-inspirados. El cyber espacio y sus dinámicas pueden ser conceptualizadas como una manifestación de acciones humanas en una abstracción y un alto espacio dimensional [37]. En fig. 3 se pueden observar los componentes del modelo propuesto el cual además funcionará sobre una red Ad hoc móvil con todas sus condiciones dinámicas, estocásticas e inalámbricas [38].

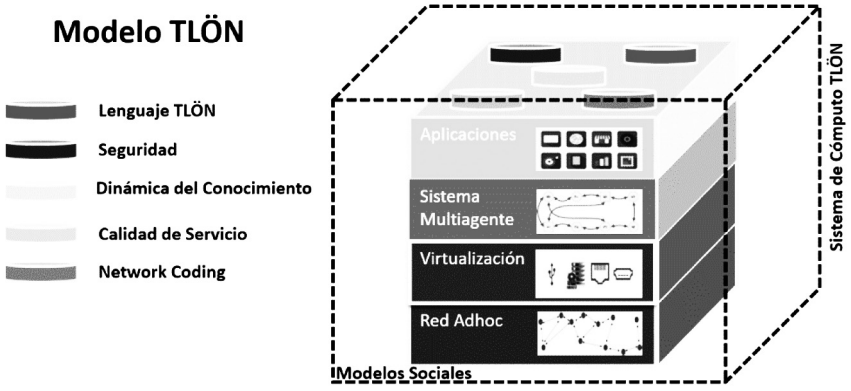

Figura 3. Sistema de cómputo TLÖN.

Fuente: Grupo de investigación TLÖN, Universidad Nacional de Colombia.

3.2.1. Capa de red Ad hoc

La movilidad en dispositivos móviles es crítica porque se debe proteger los nodos y no comprometerlos a ataques los cuales podrían desencadenar en perdida de información. Varias formas de protección son construidas como parte del sistema operativo, tales como, encriptación del dispositivo, políticas de claves, control remoto, entre otros. Algunos atributos de la capa de red Ad hoc son:

- Enrutamiento**:** El objetivo principal de un protocolo de enrutamiento es encontrar y establecer una correcta y eficiente ruta entre los nodos. Si una ruta es mal direccionada puede paralizar la red, por lo tanto, el rol de la seguridad es importante. En [39] evalúan el desempeño de varios protocolos de enrutamiento que están sufriendo un ataque de ruptura. La seguridad implica la identificación de las vulnerabilidades y ataques potenciales que puedan suceder. Los ataques en las redes MANET están clasificados en dos categorías, activos y pasivos. Los ataques pasivos son difíciles de identificar ya que son ataques que no afectan el funcionamiento de la red, su objetivo principal es ver el tráfico de la red y obtener información valiosa. Los ataques activos se dividen en dos grupos: ataques externos y ataques internos. Los ataques externos son causados por nodos que no pertenecen a la red. Un ataque interno es más peligroso ya que puede secuestrar o comprometer los nodos que pertenecen a la red, por lo tanto, cada nodo debe estar protegido con los mecanismos de seguridad de red [40].

- Red distribuida**:** es una topología de red caracterizada por la ausencia de un centro individual o colectivo. Los nodos se vinculan unos a otros de modo que ninguno de ellos, ni siquiera un grupo estable de ellos, tiene poder de filtro sobre la información que se transmite en la red. Desaparece por tanto la divisoria entre centro y periferia, característica de las redes centralizadas y descentralizadas [41].

3.2.2. Capa de virtualización

La evaluación en seguridad de contenedores, o una arquitectura de microservicios, requieren entender los diferentes modelos de amenaza, estos modelos dependen de muchas circunstancias individuales, aunque tienen muchas cosas en común. Algunos atributos de la capa de virtualización son:

- Docker: Docker es una opción de herramienta base de la primera abstracción de virtualización, es una plataforma de software compartida usada por desarrolladores y administradores de sistemas para operar aplicaciones sobre Contenedores, el concepto está ligado a la Virtualización Ligera, es decir no es necesario tener todo un sistema operativo para operar las abstracciones computacionales, traducidas en aplicaciones, al momento lo único necesario es operar sobre la aplicación de Docker los scripts y funciones desarrolladas [25, 42]. Las soluciones de contenedores proveen un ambiente con más flexibilidad que las máquinas virtuales e incluso ofrece infraestructuras basadas en cloud, sin embargo, los Docker y sus actuales escenarios de uso implican vulnerabilidades de seguridad que deben ser direccionadas. Los contenedores integran el sistema operativo del host, reduciendo la sobrecarga de software impuesta por máquinas virtuales, sin embargo, esta integración incrementa la superficie de ataque, elevando las preocupaciones de seguridad [43]. Existe trabajo sobre seguridad en contenedores como [44] que discute los principales retos y trabajos relacionados en esta área, y propone un algoritmo para mitigar los ataques de negación de servicio.
- Orquestador: los contenedores pueden ser consultados por una entidad superior denominada orquestador, este puede estar en uno o varios nodos haciendo tareas de control y validando los cambios de los recursos, este elemento toma decisiones con base en las políticas pseudo-sociales programadas en él y opera los recursos para generar la siguiente abstracción de la capa de virtualización [42].

3.2.3. Sistema multiagente

Un agente es cualquier cosa capaz de percibir su medioambiente con la ayuda de sensores y actuar en ese medio utilizando actuadores. Cada agente puede percibir sus propias acciones (pero no sus efectos). La percepción es la muestra de que el agente puede recibir alguna entrada. Un agente tomara alguna decisión dependiendo la cantidad de percepciones que reciba en su entrada [45]. Algunos atributos del sistema multiagente son:

- Entorno del agente: El entorno sobre el cual los agentes se sitúan representa al conjunto de problemas para los cuales la existencia de estos pretende dar solución. La arquitectura de un agente está definida por algún tipo de sensor físico que en algunas ocasiones implementa un actuador, esta parte física está gobernada por un programa que implementa la función del agente y proyecta las

precepciones en las acciones. La representación de conceptos abstractos como las acciones, el tiempo, los objetos físicos, las creencias y la posible representación de todo en el mundo se suelen denominar ingeniería ontológica [46].

3.3. Modelo CIA en el sistema TLÖN

El módulo de seguridad para el sistema TLÖN debería tener las principales características de seguridad (confidencialidad, integridad y disponibilidad), expresadas en cada capa del sistema como se ve en fig. 4. Por ser un sistema social inspirado tiene atributos de cooperación para la solución de problemas, el compartir información, entre otras cosas. Puede generar distintos problemas de seguridad y vulnerabilidades, las cuales podrían ser solucionadas tomando como referencia la construcción de un módulo de seguridad presente en cada nodo de la red que realice las tareas de confidencialidad, integridad y disponibilidad.

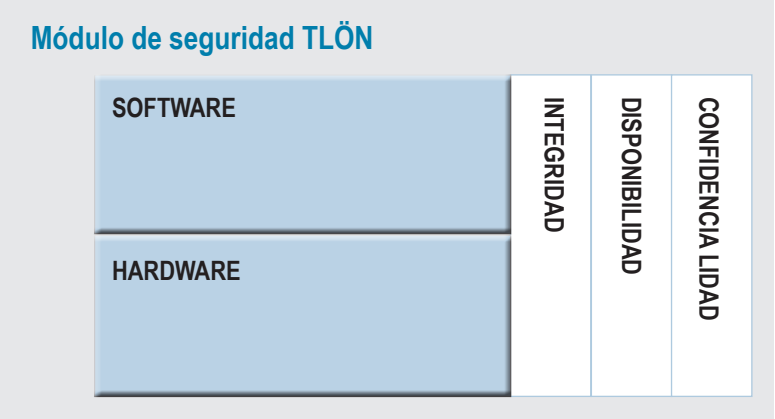

Figura 4. Sistema de cómputo TLÖN.

Fuente: Elaborado por Santiago José Molina Sanchez

3.3.1. Características de disponibilidad para el modelo TLÖN

Históricamente, alrededor del 90% de las investigaciones en seguridad de la información fueron acerca de la confidencialidad, 9% sobre autenticidad y solo un 1% sobre disponibilidad, pero debido a los ataques actuales y las expectativas de las compañías, actualmente se están gastando más esfuerzos en disponibilidad [47]. Una red militar o una red bancaria seguramente necesitarían de una confidencialidad alta, y por otro lado, una aplicación de *streaming* video, necesitaría de una alta integridad, adicionalmente, todas estas aplicaciones requieren que la red esté disponible: cuando el sistema o los datos sean solicitados, puedan ser accedidos por el personal apropiado [48].

En [49] presentan un control adaptativo de crucero el cual funciona en un red vehicular para prevenir los ataques de negación de servicio, y en [50] para la comunicación *Vehicle to Vehicle* (V2V) y *Vehicle to infrastructure* (V2I), se desarrolla un esquema resiliente para un esquema de vehículos conectados equipados con un *Cooperative Adaptive Cruise Control* (CACC), para mitigar los ataques de negación de servicio.

3.3.2. Característica de confidencialidad para el modelo TLÖN

La criptografía es la ciencia o estudio de proteger la información, usando técnicas para convertir la información a un formato ilegible, para que nadie excepto quien posea la clave de des-encriptación pueda acceder a ella. El proceso es simple, tomar el texto plano (algo que se puede leer) y aplicando un método criptográfico, convertirlo en un texto cifrado(algo que no se puede leer), para convertir de nuevo el mensaje a texto plano se utiliza un método de des-encriptación [48].

3.3.3. Característica de integridad para el modelo TLÖN

La integridad como atributo permite solo a los usuarios autorizados modificar los datos en el cyber espacio [37]. Cuando los datos son intercambiados entre los actores, a menudo pasan por áreas compartidas donde otros actores tienen la posibilidad de alterar los datos antes que lleguen a su destino. Algunos algoritmos y métodos de encriptación también proveen integridad, la no repudiación es el medio por el cual un recipiente puede asegurar la identidad del mensaje enviado y ninguna persona puede enviar o recibir el mensaje [48]. El objetivo principal de la integridad de la información es la no alteración e interceptación del mensaje por parte de terceros [51].

4. CONCLUSIONES Y RETOS DE INVESTIGACIÓN

Tecnologías como SDN ya han sido implementadas con éxito en muchas empresas a nivel mundial y apuntan a convertirse en una tecnología dominante en algunos años. Las redes inalámbricas Ad hoc adoptan tecnologías como SDN para mejorar su eficiencia energética además de optimizar la utilización de espacios físicos. Los diseños del sistema de cómputo TLÖN se han desarrollado bajo la idea de una SDN como se ve en la figura 4, ello impone un gran reto de ingeniería debido a que éstas aun no incorporan aspectos avanzados de seguridad, los campos de investigación en redes inalámbricas Ad hoc crecen rápidamente, por esta razón es importante la investigación en seguridad, además las aplicaciones de las redes Ad hoc y de los sistemas de cómputo montados sobre ellos están en constante interacción con datos muy sensibles. Proyectos de investigación como TLÖN el cual funciona sobre una red Ad hoc, toma muy enserio la seguridad y propone desarrollar un módulo de seguridad el cual proporcione disponibilidad, integridad y confidencialidad, los cuales son los atributos principales de cualquier sistema de seguridad. La seguridad de un sistema debe responder a los desafíos de sistemas altamente distribuidos y escalables como el internet de las cosas o las ciudades inteligentes. El comienzo del desarrollo del módulo se enfocará en la disponibilidad, ya que todo sistema de telecomunicaciones debe proporcionar comunicación entre los nodos de la red.

REFERENCIAS

[1] Y. Hayel, E. Hart, R. El-Azouzi, I. Carrera, and E. Altman, *Bioinspired Models of Network, Information, and Computing Systems: 4th International Conference, December 9-11, 2009, Revised Selected Papers*. Springer Berlin Heidelberg, 2010.

[2] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3. pp. 2027–2051, 2016.

[3] B. R. Al-Kaseem and H. S. Al-Raweshidy, "Enabling wireless Software Defined Networking in cloud based Machine-to-Machine gateway," *2016 8th Computer Science and Electronic Engineering (CEEC)*. pp. 24–29, 2016.

[4] A. Kumari, J. Chandra, and A. S. Sairam, "Optimizing flow setup time in software defined network," in *10th International Conference on Communication Systems Networks (COMSNETS)*, pp. 543–545.

[5] A. I. Swapna, M. R. Huda, and M. K. Aion, "Comparative security analysis of software defined wireless networking (SDWN)-BGP and NETCONF protocols," *2016 19th International Conference on Computer and Information Technology (ICCIT)*. pp. 282–287, 2016.

[6] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, "Software Defined Wireless Network (SDWN): An evolvable architecture for W-PANs," *2015 IEEE 1st International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. pp. 23–28, 2015.

[7] I. T. Haque and N. Abu-Ghazaleh, "Wireless Software Defined Networking: A Survey and Taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4. pp. 2713–2737, 2016.

[8] G. Karagiannis *et al.*, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4. pp. 584–616, 2011.

[9] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected Vehicles: Solutions and Challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4. pp. 289–299, 2014.

[10] C. V Neu, A. F. Zorzo, A. M. S. Orozco, and R. A. Michelin, "An approach for detecting encrypted insider attacks on OpenFlow SDN Networks," *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. pp. 210–215, 2016.

[11] M. Dong, H. Li, K. Ota, and J. Xiao, "Rule caching in SDN-enabled mobile access networks," *IEEE Network*, vol. 29, no. 4. pp. 40–45, 2015.

[12] K. Pentikousis, Y. Wang, and W. Hu, "Mobileflow: Toward software-defined mobile networks," *IEEE Communications Magazine*, vol. 51, no. 7. pp. 44–53, 2013.

[13] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," in *2017 International Conference on Signal Processing and Communication (ICSPC)*, 2017, pp. 288–293.

[14] M. Dasari, "Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks," in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2017, pp. 939–944.

[15] M. U. Farooq, X. Wang, R. Yasrab, and S. Qaisar, "Energy Preserving Detection Model for Collaborative Black Hole Attacks in Wireless Sensor Networks," in *2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, 2016, pp. 395–399.

[16] H. Kaur and A. Singh, "Identification and Mitigation of Black Hole Attack in Wireless Sensor Networks," in *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, 2016, pp. 616–619.

[17] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking #x2014; A review," in *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*, 2017, pp. 1–6.

[18] A. Gupta and R. K. Jha, "Security threats of wireless networks: A survey," in *International Conference on Computing, Communication Automation*, 2015, pp. 389–395.

[19] M. Alqallaf and B. Wang, "Software defined collaborative secure ad hoc wireless networks," *2015 International Conference on Collaboration Technologies and Systems (CTS)*. pp. 196–203, 2015.

[20] M. Al-Zewairi, D. Suleiman, and S. Almajali, "An experimental Software Defined Security controller for Software Defined Network," *2017 Fourth International Conference on Software Defined Systems (SDS)*. pp. 32–36, 2017.

[21] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1. pp. 325–346, 2017.

[22] M. Kalinin, P. Zegzhda, D. Zegzhda, Y. Vasiliev, and V. Belenko, "Software defined security for vehicular ad hoc networks," *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. pp. 533–537, 2016.

[23] K. R. Ramkumar and A. Kaur, "A distributed method of key issue and revocation of mobile ad hoc networks using curve fitting," in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 2017, pp. 258–263.

[24] V. Kumar and R. Kumar, "Detection of phishing attack using visual cryptography in ad hoc network", in *2015 International Conference on Communications and Signal Processing (ICCSP)*, 2015, pp. 1021–1025.

[25] M. L. Pura and D. Buchs, "A self-organized key management scheme for ad hoc networks based on identity-based cryptography," in *2014 10th International Conference on Communications (COMM)*, 2014, pp. 1–4.

[26] K. D. Thilak and A. Amuthan, "DoS attack on VANET routing and possible defending solutions–A survey," *2016 International Conference on Information Communication and Embedded Systems (ICICES)*. pp. 1–7, 2016.

[27] J. Tobin, C. Thorpe, and L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–7.

[28] S. V Vasantha and A. Damodaram, "Bulwark AODV against Black hole and Gray hole attacks in MANET," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2015, pp. 1–5.

[29] Matt Walker, *CEH Certifed Ethical Hacker*. McGraw-Hill books, 2012.

[30] G. Kovacich, *information system security officer's guide*, First. united states: Butterworth Heinemann, 2003.

[31] M. Soni, M. Ahirwa, and S. Agrawal, "A Survey on Intrusion Detection Techniques in MANET," in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015, pp. 1027–1032.

[32] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[33] U. K. Verma, S. Kumar, and D. Sinha, "A secure and efficient certificate based authentication protocol for MANET," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, 2016, pp. 1–7.

[34] C. B. Chandrakala., K. V Prema., and K. S. Hareesha., "Improved data availability and fault tolerance in MANET by replication," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, 2013, pp. 324–329.

[35] T. Naik, F. Khatiwala, and A. Sakadasariya, "Search for secure data transmission in MANET: A review," in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017, pp. 573–575.

[36] M. Flynn and W. Luk, "Computer System Design." 2011.

[37] E. Thomas and D. Manz, *Research Methods for Cyber Security*, 1st ed. Syngress, 2017.

[38] A. Aho, M. Lam, R. Sethi, and J. Ullman, "compliers, principles, techniques & tools." p. 1038, 1986.

[39] R. J. Cai, X. J. Li, and P. H. J. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," *IEEE Trans. Mob. Comput. (en prensa)*, p. 1, 2018.

[40] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10. pp. 70–75, 2002.

[41] E. Gore, *El proximo management*, 1st ed. GRANICA, 2014.

[42] adrian Mouat, *Using docker developing and deploying software whit containers*, First. Gravenstein Highway North,: O'Reilly Media, Inc, 2016.

[43] T. Combe, A. Martin, and R. Di pietro, "to docker or not to docker: A Security Perspective," *IEEE Comput. Soc.*, p. 9, 2016.

[44] J. Chelladhurai, P. R. Chelliah, and S. A. Kumar, "Securing Docker Containers from Denial of Service (DoS) Attacks," in *2016 IEEE International Conference on Services Computing (SCC)*, 2016, pp. 856–859.

[45] S. Russell and P. Norving, *inteligencia artificial un enfoque moderno*, Segunda. Ribera del Loira: Pearson Education, 2004.

[46] A. Gómez, M. C. Suárez, E. Motta, and A. Gangemi, Eds., *Ontology Engineering in a Networked World*, First. Berlin: Springer-Verlag Berlin Heidelberg, 2012.

[47] ross Anderson, *Security Engineering*, Second. indianapolis, indiana: Wiley publishing.

[48] D. Regalado *et al.*, *Gray Hat Hacking*, Four. United States: McGraw-Hill Education, 2015.

[49] Q. Tianxiang, H. Defeng, L. Liangye, and S. Xiulan, "Adaptive cruise control of vehicles subject to Denial-of-Service," *2017 32nd Youth Academic Annual Conference of Chinese Association of Automation (YAC)*. pp. 382–386, 2017.

[50] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under Denial of Service in connected vehicles," *2017 American Control Conference (ACC)*. pp. 4971–4976, 2017.

[51] M. K. Verma, S. Joshi, and N. V Doohan, "A survey on: An analysis of secure routing of volatile nodes in MANET," in *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, 2012, pp. 1–3.