Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Análisis de la seguridad en redes 5G y propuesta de mejoras

Trabajo de Titulación previo a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Bolívar Rolando Quizhpe Vásquez.

DIRECTOR:

Ing. Juan Gabriel Ochoa Aldeán, Mg. Sc.

Portada

LOJA – ECUADOR

2023

Educamos para Transformar

Certificación

Loja, 20 de junio de 2023

Ing. Juan Gabriel Ochoa Aldeán Mg. Sc.

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis de la seguridad en redes 5G y propuesta de mejoras,** previo a la obtención del título **de Magíster en Telecomunicaciones,** de la autoría del estudiante **Bolívar Rolando Quizhpe Vásquez** , con **cédula de identidad N° 1104607120 ,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
JUAN GABRIEL OCHOA ALDEAN

Ing. Juan Gabriel Ochoa Aldeán Mg. Sc.

DIRECTOR DE TRABAJO DE INVESTIGACIÓN

Autoría

Yo, **Bolívar Rolando Quizhpe Vásquez**, declaro ser autor del Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: Firmado electrónicamente por: BOLIVAR ROLANDO QUIZHPE VASQUEZ

Cédula de Identidad: 1104607120

Fecha: 3 de julio de 2023

Correo electrónico: bolivar.quizhpe@unl.edu.ec

Teléfono o celular: 0986756385

Carta de autorización por parte del autor para la consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Titulación.

Yo, **Bolívar Rolando Quizhpe Vásquez**, declaro ser autor del Trabajo de Titulación denominado: **Análisis de la seguridad en redes 5G y propuesta de Mejoras**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los tres días del mes de julio de dos mil veintitrés.

Firma: Firmado electrónicamente por: BOLIVAR ROLANDO QUIZHPE VASQUEZ

Autor: Ing. Bolívar Rolando Quizhpe Vásquez

Cédula: 1104607120

Dirección: Loja-Ecuador

Correo Electrónico: bolivar.quizhpe@unl.edu.ec

Teléfono: 0986756385

DATOS COMPLEMENTARIOS:

Director de Trabajo de Titulación: Ing. Juan Gabriel Ochoa Aldeán Mg. Sc.

Dedicatoria

El presente Trabajo de Titulación está dedicado primeramente a Dios (Su voluntad es mi camino), a mi madre Luz María gracias por el amor y apoyo incondicional; a mis hermanos y sobrinos por acompañarme en cada uno de mis logros y ser parte de ellos.

Bolívar Rolando Quizhpe Vásquez

Agradecimiento

Deseo expresar mi sincero agradecimiento a la Universidad Nacional de Loja y su destacado cuerpo docente. Gracias a su amplia experiencia y vastos conocimientos, he adquirido valiosas herramientas que han contribuido significativamente al desarrollo de mi perfil profesional e intelectual. Su dedicación y compromiso con la enseñanza han sido fundamentales para mi formación académica y personal.

Bolívar Rolando Quizhpe Vásquez

Índice de Contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Titulo

Análisis de la seguridad en redes 5g y propuesta de mejoras

2. Resumen

En los últimos años, ha habido cierta confusión en torno a la definición precisa de la tecnología 5G. En esencia, el 5G es un conjunto de tecnologías avanzadas que se integran en una única estructura de red para conectar personas entre sí y con el mundo en general. Esta tecnología representa una evolución significativa en la conectividad móvil, ofreciendo mayores velocidades de transmisión de datos, menor latencia y mayor capacidad de conexión de dispositivos. A través del uso de tecnologías como el espectro de ondas milimétricas y la virtualización de redes, el 5G tiene el potencial de transformar la forma en que interactuamos y nos comunicamos.

El presente trabajo se enfoca en analizar la seguridad de las redes 5G, centrándose específicamente en la capa de aplicación. Para ello, se realizó un análisis detallado de casos de estudio que permitieron identificar posibles vulnerabilidades y amenazas en la infraestructura de estas redes. A partir de los resultados obtenidos, se propusieron mejoras y soluciones para aumentar la seguridad de la red y garantizar la privacidad de los datos de los usuarios. Entre las posibles soluciones se encuentran la implementación de protocolos de seguridad más robustos, la mejora de la autenticación de los usuarios y la implementación de medidas de protección adicionales.

Se espera que los resultados de esta investigación contribuyan a una red 5G más segura y confiable, lo que permitirá una mayor adopción y uso de la tecnología, fomentando el desarrollo tecnológico y la innovación en este ámbito.

Palabras Clave: *Seguridad, red, 5G, capa de aplicación, privacidad.*

2.1 Abstract

5G technology definition has been subject to some confusion in recent years. A 5G network consists of a set of advanced technologies integrated into one system. As a result, people are able to connect with each other and with the world at large. The technology represents a significant advancement in mobile connectivity, providing faster data transmission speeds, lower latency, and enhanced device connectivity. Through technologies such as millimeter wave spectrum and network virtualization, 5G has the potential to transform our interactions and communications. The purpose of this paper is to analyze the security of 5G networks, specifically at the application layer. In order to identify possible vulnerabilities and threats in the infrastructure of these networks, case studies were analyzed in detail. Based on the findings, improvements and solutions were proposed to increase network security and ensure user data privacy. Possible solutions include implementing more robust security protocols, improving user authentication and implementing additional protection measures. This research is expected to contribute to a more secure and reliable 5G network. This will enable increased adoption and use of the technology, fostering technological development and innovation in this area.

Keywords: *Security, network, 5G, application layer, privacy.*

3. Introducción

En la actualidad, la conectividad móvil es esencial para la vida cotidiana de las personas y las empresas. La red móvil de quinta generación (5G) se ha convertido en una de las tecnologías más prometedoras para la conectividad móvil y ha generado un gran interés en la industria de las telecomunicaciones.

La red 5G ofrece velocidades de datos más rápidas, mayor ancho de banda, menor latencia y mayor capacidad de conexión de dispositivos que las tecnologías móviles anteriores. Sin embargo, a medida que las redes 5G se implementan y se vuelven más comunes, también surgen preocupaciones sobre la seguridad de la red y la privacidad de los datos. En este contexto, el análisis de la seguridad en redes 5G se ha convertido en un tema crítico para garantizar una conectividad móvil segura y confiable.

El alcance del presente proyecto tiene objetivo analizar los desafíos de seguridad en las redes 5G y proponer mejoras para abordar estas preocupaciones de seguridad. Con este proyecto se espera contribuir al conocimiento sobre la seguridad en redes 5G y proporcionar recomendaciones para asegurar una conectividad móvil segura y confiable en el futuro.

Objetivo general

Realizar un análisis exhaustivo de la seguridad en redes 5G, identificando las vulnerabilidades y los riesgos asociados con esta tecnología, y proponer mejoras para fortalecer la seguridad de la red y proteger la privacidad de los usuarios.

Objetivos específicos

- Analizar las vulnerabilidades y riesgos específicos de la tecnología 5G, en comparación con las redes anteriores, para comprender mejor los desafíos de seguridad que presenta.
- Evaluar las medidas de seguridad actuales en la capa de aplicación de la red 5G , incluyendo la autenticación, la protección de la privacidad y la seguridad de la red, para identificar las áreas donde se necesitan mejoras.
- Proporcionar una propuesta integral de mejoras en la seguridad de la red 5G, que permita garantizar la seguridad y la privacidad de los usuarios y mantener la integridad de la red en el futuro.

4. Marco Teórico

4.1.Redes móviles 5G

Las redes móviles 5G son la última generación de tecnología de comunicación inalámbrica y se considera un avance significativo en comparación con las redes móviles 4G anteriores. La tecnología 5G ofrece mayores velocidades de datos, menor latencia y mayor capacidad de conexión de dispositivos en comparación con las redes 4G.

Figura 1

5G

Fuente: Ilustración: Istock

Las redes móviles 5G son la última generación de tecnología de comunicación inalámbrica y se considera un avance significativo en comparación con las redes móviles 4G anteriores. La tecnología 5G ofrece mayores velocidades de datos, menor latencia y mayor capacidad de conexión de dispositivos en comparación con las redes 4G.

Las redes móviles 5G se basan en una combinación de tecnologías, incluyendo espectro de radio de alta frecuencia, MIMO masivo (Múltiple Entrada Múltiple Salida), antenas inteligentes, virtualización de redes y computación en la nube. La tecnología 5G permite conexiones más rápidas y eficientes, lo que permite una mejor experiencia del usuario en aplicaciones como videoconferencias, realidad virtual y aumentada, y la Internet de las cosas (IoT).

Sin embargo, con la implementación de la tecnología 5G, también surgen nuevos desafíos de seguridad. Debido a su alta velocidad y capacidad de conexión de dispositivos, las redes 5G son más vulnerables a los ciberataques. Los ciberdelincuentes pueden explotar vulnerabilidades en la red 5G para robar datos confidenciales, interferir con la conexión del usuario y dañar la infraestructura crítica.

Por lo tanto, es esencial realizar un análisis exhaustivo de la seguridad en las redes 5G y proponer mejoras para garantizar que la tecnología sea segura y confiable para su uso a largo plazo.

4.1.1. Definicion y Caracteristicas

5G es la quinta generación de tecnología celular. Está diseñada para aumentar la velocidad, reducir la latencia y mejorar la flexibilidad de los servicios inalámbricos. La tecnología 5G ofrece una velocidad máxima teórica de 20 Gbps, mientras que la velocidad máxima de la tecnología 4G es solo de 1 Gbps.

5G también ofrece menor latencia, lo que puede mejorar el rendimiento de las aplicaciones comerciales y de otras experiencias digitales (como juegos en línea, videoconferencias y automóviles con piloto automático). (*¿Qué es 5G?*, s. f.)

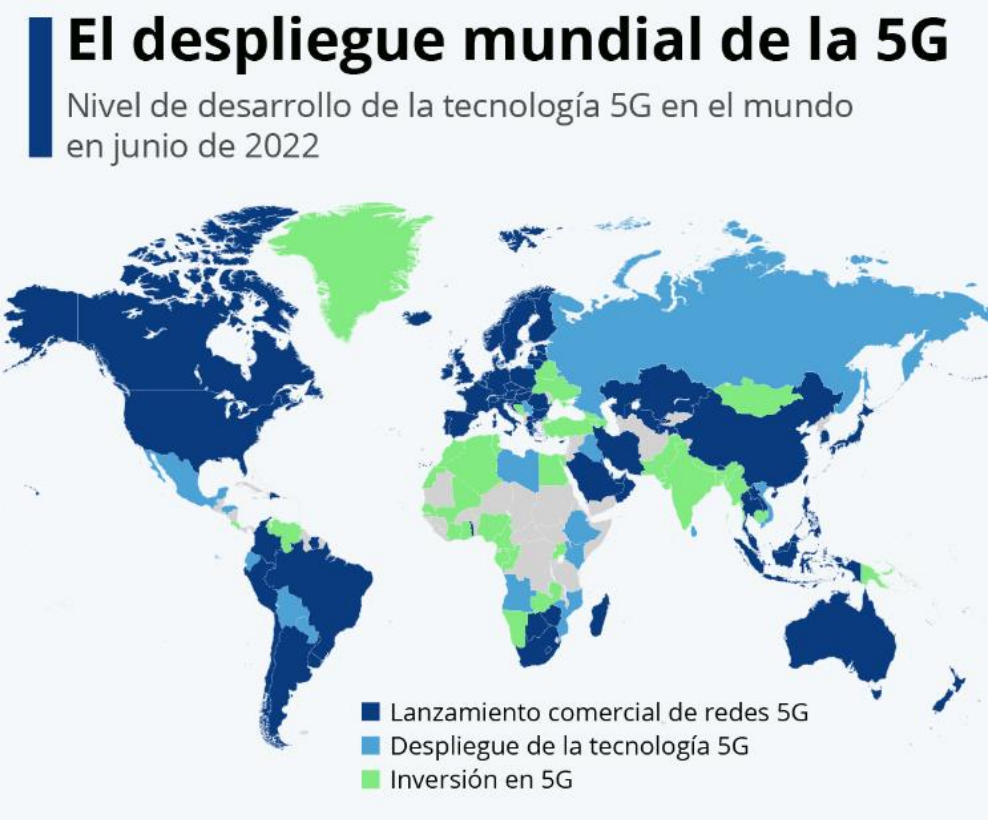
4.1.2. El Despliegue de la 5G en el Mundo

La tecnología 5G se está expandiendo rápidamente en todo el mundo. Según un informe de la Global Mobile Suppliers Association (GSA), la quinta generación de tecnologías móviles ya está disponible comercialmente en unos 70 países en junio de 2022, lo que supone un gran aumento respecto a los 38 países que la ofrecían en mediados de 2020. Además, otros quince países ya han desplegado parcialmente esta tecnología.

Las últimas estimaciones indican que la 5G podría superar los mil millones de usuarios este año, apenas 3,5 años después de su entrada al mercado, en comparación con los cuatro años que tardó la 4G en alcanzar esta cifra y los doce años de la 3G.

América y Europa lideran la implementación de la 5G, tal como se muestra en nuestro mapa. En América Latina, Chile, Uruguay y República Dominicana han logrado importantes avances en los últimos doce meses, al lanzar comercialmente la 5G, según el monitoreo de la GSA. Además, México y Bolivia han evolucionado de la fase de inversión a la de despliegue en esta tecnología, en comparación con mediados de 2021. (Pasquali, 2022)

Figura 2
GSA 5G Snapshot



Fuente: Pasquali, 2022

4.1.3. Características de la tecnología 5G

La tecnología 5G está caracterizada por 9 especificaciones Latencia de un milisegundo, recordemos que la latencia es el tiempo que tarda en ir la información de origen hasta el destino, lo cual permitirá una mejora notable en la comunicación.

- 100% de cobertura para lo cual será necesario realizar millonarias inversiones a nivel de infraestructura física.
- Contará con un ancho de banda de 1.000 por unidad de área.
- Un dispositivo IoT (Internet de las cosas) contará con una vida útil de 10 años de baja potencia.
- Contará con velocidades, dependiendo el dispositivo, hasta de 10 GB por segundo.
- Reducirá el consumo de energía en la red hasta en un 90%.
- Aumentará el número de dispositivos conectados de 10 a 100x lo cual se calcula en un promedio de 50.000 millones de dispositivos conectados de forma simultánea.
- 99.99% de disponibilidad de la red.

- Las redes 5G usaran los estándares de seguridad SE, HSM, OTA y KMS con el fin de que la información enviada no sea atacada. (Castillo et al., 2022)

4.1.4. Aplicaciones.

El 5G permitirá muchas aplicaciones nuevas y será transformador, especialmente en áreas urbanas. A medida que se implemente, se verán nuevas aplicaciones de IoT y casos de uso con mayor ancho de banda y rendimiento más rápido. Sin embargo, habrá una división creciente entre áreas urbanas y rurales debido a la falta de implementación inmediata de 5G en todas partes. Para cumplir con la promesa de 5G, los operadores deben construir una red densa con una gran cantidad de nodos de red.

- **Telecomunicaciones**

Las empresas de telecomunicaciones necesitan redes escalables que puedan adaptarse de manera fluida para satisfacer las demandas cambiantes y deben prepararse para casos de uso florecientes con dispositivos conectados en casi todas las industrias. Si bien las arquitecturas tradicionales no han logrado satisfacer estas demandas, muchas de estas necesidades se abordan a través de sistemas 5G.

- **Vehículos autónomos**

Las redes 5G serán un habilitador importante para los vehículos autónomos debido a su latencia reducida, lo que permitirá a los vehículos responder de manera casi instantánea a los cambios en su entorno. El objetivo final es una red de comunicación del vehículo a todo, que permita que los vehículos respondan automáticamente a las señales de tráfico, peligros y peatones en milisegundos.

- **Ciudades inteligentes**

Hoy en día, muchas ciudades de todo el mundo están implementando sistemas de transporte inteligentes y planean respaldar la tecnología de vehículos conectados. Los aspectos de estos sistemas son relativamente fáciles de instalar utilizando los sistemas de comunicaciones actuales que respaldan la gestión inteligente del tráfico para manejar la congestión vehicular y enrutar los vehículos de emergencia.

La columna vertebral de las comunicaciones para respaldar la tecnología de los vehículos conectados puede implementarse gradualmente hoy, mucho antes de que se implemente por completo 5G, mejorando drásticamente la seguridad de los peatones y los vehículos.

- **Automatización industrial**

La automatización industrial está en uso hoy en día, y lo más probable es que hayas visto videos que muestran la robótica sincronizada en funcionamiento en fábricas y aplicaciones de la cadena de suministro. Hoy en día, estas aplicaciones requieren cables, ya que Wi-Fi no proporciona el alcance, la movilidad y la calidad de servicio requeridos para el control industrial, y la latencia de la tecnología celular actual es demasiado alta.

Con 5G, las aplicaciones de automatización industrial pueden cortar el cable y volverse completamente inalámbricas, lo que permite fábricas inteligentes más eficientes.

- **Realidad aumentada y realidad virtual**

La baja latencia de la tecnología 5G hará que las aplicaciones de realidad aumentada y realidad virtual sean tanto inmersivas como mucho más interactivas.

En aplicaciones industriales, por ejemplo, un técnico con gafas 5G AR podría ver una superposición de una máquina que identificaría piezas, proporcionaría instrucciones de reparación o mostraría piezas que no son seguras al tacto. Las oportunidades para aplicaciones industriales altamente receptivas que admiten tareas complejas serán amplias.

- **Drones**

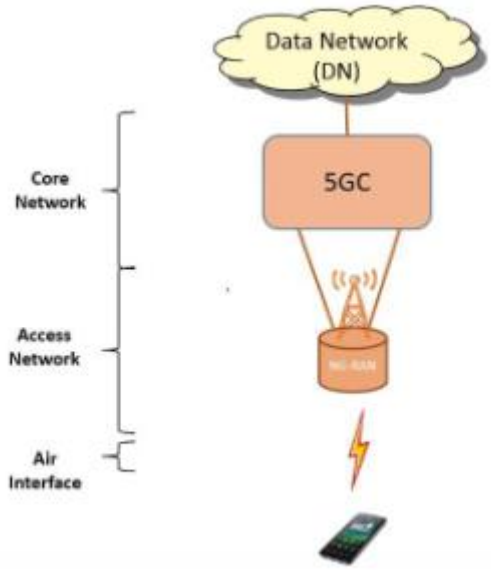
Los drones tienen un amplio y creciente conjunto de casos de uso en la actualidad más allá del uso del consumidor para filmar y fotografiar. Por ejemplo, las empresas de servicios públicos están utilizando drones en la actualidad para la inspección de equipos. Con el 5G, se superarán los límites de los drones actuales, especialmente en alcance e interactividad. La tecnología 5G permitirá una mayor latencia y video de alta resolución, lo que tendrá implicaciones en casos de uso como búsqueda y rescate, seguridad fronteriza, vigilancia y servicios de entrega de drones.(«Tecnología 5G, Características, usos y posibles peligros», 2020)

4.1.5. Arquitectura de la tecnología 5G

La tecnología 5G con su arquitectura de red avanzada, tiene el potencial de soportar muchas nuevas aplicaciones en diferentes sectores y mercados. Esto permitirá la automatización avanzada de la fabricación, vehículos autónomos, entre otras aplicaciones. Aunque el despliegue de la red 5G comenzó hace años, el proceso llevará tiempo y se desplegará primero en las grandes ciudades. (Montesinos Chano, 2018)

Las futuras redes de quinta generación deben ser capaces de soportar los servicios y aplicaciones que las nuevas demandas requieren, estas redes deben estar dotadas de mayor flexibilidad, agilidad y escalabilidad, por lo cual arquitectura de la red 5G está compuesta por varios habilitadores técnicos claves para cumplir con las necesidades de los usuarios.(Montesinos Chano, 2018)

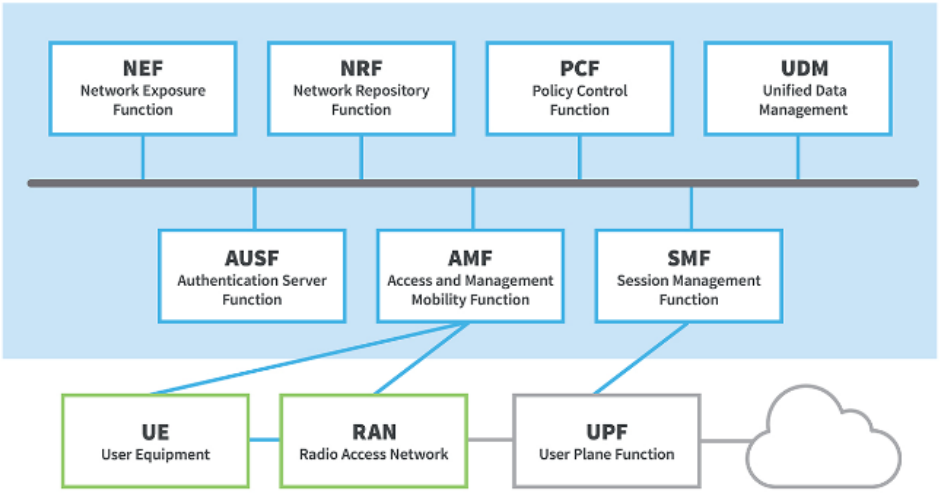
Figura 3
Sistema 5G



Fuente: (Wong, Schober, Ng, & Wang, 2017)

La arquitectura del sistema 5G, consiste de funciones de red (NF), con el fin de habilitar el acceso a los distintos tipos de servicios, estas funciones se han definido como software, con el fin de adaptarse a las necesidades.

Figura 4
Arquitectura 5G



Fuente: (*¿Qué es la arquitectura de red 5G?*, s. f.)

Así es como funciona:

- Los equipos de usuario (UE), como los smartphones 5G o los dispositivos celulares 5G, se conectan a través de la nueva red de acceso radioeléctrico 5G al núcleo 5G y, además, a las redes de datos (DN), como Internet.
- La función de gestión del acceso y la movilidad (AMF) actúa como punto de entrada único para la conexión del equipo de usuario.
- Basándose en el servicio solicitado por el UE, la AMF selecciona la respectiva función de gestión de sesión (SMF) para gestionar la sesión de usuario.
- La función de plano de usuario (UPF) transporta el tráfico de datos IP (plano de usuario) entre el equipo de usuario (UE) y las redes externas.
- La función de servidor de autenticación (AUSF) permite a la AMF autenticar al UE y acceder a los servicios del núcleo 5G.
- Otras funciones como la función de gestión de sesiones (SMF), la función de control de políticas (PCF), la función de aplicación (AF) y la función de gestión unificada de datos (UDM) proporcionan el marco de control de políticas, aplicando las decisiones de política y accediendo a la información de suscripción, para gobernar el comportamiento de la red.

Como se puede ver, la arquitectura de la red 5G es más compleja entre bastidores, pero esta complejidad es necesaria para ofrecer un mejor servicio que pueda adaptarse a la amplia gama de casos de uso del 5G.(*¿Qué es la arquitectura de red 5G?*, s. f.)

4.2.Estandares 5G

Los estándares 5G son especificaciones técnicas y protocolos desarrollados por organizaciones de estándares internacionales para garantizar la interoperabilidad, eficiencia y seguridad de las redes 5G. Estos estándares definen aspectos como la arquitectura de la red, la seguridad, la calidad del servicio y la administración del espectro.

Organizaciones que desarrollan estándares 5G:

4.2.1. 3GPP (3rd Generation Partnership Project)

3GPP es una colaboración entre siete organizaciones de estándares de telecomunicaciones que desarrolla especificaciones para tecnologías móviles, incluido el 5G. Sus principales contribuciones a los estándares 5G incluyen las versiones 15, 16 y 17 de sus especificaciones técnicas. Enlace: (*3GPP – The Mobile Broadband Standard*, s. f.)

4.2.2. ETSI (European Telecommunications Standards Institute)

ETSI es una organización europea que desarrolla estándares para las tecnologías de la información y las comunicaciones, incluido el 5G. ETSI ha trabajado en áreas clave como la seguridad, la calidad del servicio y la gestión del espectro en 5G. Enlace: (*ETSI - Welcome to the World of Standards!*, s. f.)

4.2.3. IEEE (Institute of Electrical and Electronics Engineers):

IEEE es una organización global que desarrolla estándares para varias áreas de tecnología, incluidas las comunicaciones inalámbricas. IEEE ha contribuido al desarrollo de tecnologías clave en 5G, como la comunicación de ondas milimétricas y la administración de la movilidad. Enlace: (*IEEE - The World's Largest Technical Professional Organization Dedicated to Advancing Technology for the Benefit of Humanity.*, s. f.)

El desarrollo del estándar 5G comenzó en la década de 2010, con la investigación y desarrollo de tecnologías clave y la identificación de los requisitos para la próxima generación de comunicaciones móviles. Organizaciones como 3GPP, ETSI e IEEE lideraron el proceso de estandarización.

Las especificaciones técnicas y protocolos de 5G se desarrollaron en varias fases. 3GPP, en particular, dividió el desarrollo del estándar 5G en tres versiones principales: Release 15, Release 16 y Release 17.

- Release 15: La primera versión de las especificaciones 5G, completada en junio de 2018, definió la arquitectura de la red 5G y las especificaciones para la nueva radio (NR) y el núcleo de la red 5G (5GC).
- Release 16: Completada en julio de 2020, esta versión mejoró y expandió las especificaciones iniciales, abordando temas como la segmentación de red, la comunicación V2X (vehículo a todo) y la Industria 4.0.
- Release 17: La finalización de esta versión estaba prevista inicialmente para 2021, pero se retrasó debido a la pandemia de COVID-19. Release 17 aborda aspectos adicionales como la mejora de la comunicación V2X y la integración de redes satelitales.

Dividir Rel-15 en varias gotas resultó ser un gran desafío, por ejemplo, NSA NR todavía tenía solicitudes de cambio no compatibles con versiones anteriores en septiembre 18 insertar ASN.1 en una especificación ya congelada requiere solicitudes de cambio de muy alta calidad, lo cual es difícil bajo mucha presión de tiempo

Los grupos de trabajo que requieren un trabajo previo estable de otros grupos de trabajo (como RAN4 para RF/RRM y RAN5 para pruebas) están trabajando en terrenos inestables y luchan aún más para mantenerse dentro del plan de tiempo.

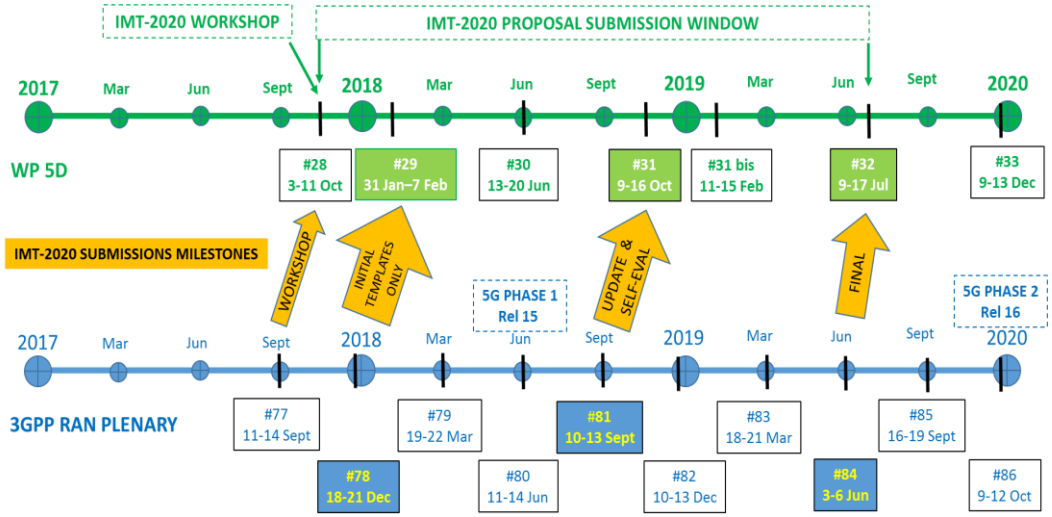
Sin embargo, 3GPP contribuyó a tiempo al cronograma IMT-2020 que se muestra a continuación:

- en enero de 2018 vía PCG40_11 con características iniciales de NR RIT y NR+LTE SRIT
- en sep./oct.2018 a través de PCG41_08 con las características del NR RIT y NR+LTE SRIT, los resultados preliminares de autoevaluación y presupuesto de enlace y las plantillas de cumplimiento
- en junio de 2019 a través de PCG43_07 con las presentaciones de candidatos 3GPP 5G de NR RIT y NR+LTE SRIT que incluyen características, plantillas de presupuesto de enlace y cumplimiento y la autoevaluación 3GPP TR 37.910 (esta presentación incluye más mejoras Rel-16) al paso 3 del IMT -Proceso 2020
  Nota: Las plantillas de características ofrecen una buena visión general de la tecnología considerada.
- en junio de 2020, las descripciones generales finales de las especificaciones 3GPP a través de PCG45_07 para NR+LTE SRIT y PCG45_08 para NR RIT y en julio de 2020,

los conjuntos de especificaciones finales de 2020-06 (Versión 15 y 16) para la transposición de los OP 3GPP(Dahmen-Lhuissier, s. f.)

Figura 5

Cronograma de las presentaciones de las tecnologías candidatas 3GPP para su inclusión.



Fuente: (Dahmen-Lhuissier, s. f.)

4.3.Seguridad en Redes 5G

4.3.1. Desafíos en el ámbito de la seguridad en las redes 5G

Las redes 5G ofrecen una amplia gama de características y avances técnicos que las distinguen y las sitúan por encima de las generaciones anteriores de redes móviles. A pesar de sus ventajas, diversas organizaciones y entidades europeas, incluyendo la Comisión Europea, la Agencia Europea de Ciberseguridad (ENISA) y el Grupo de Cooperación NIS, han expresado preocupaciones acerca de un aumento significativo en los riesgos de seguridad asociados con las redes 5G en comparación con las generaciones previas de redes móviles. Estos riesgos están estrechamente vinculados a la disponibilidad, integridad, privacidad, confidencialidad y accesibilidad de las redes.(Jiménez, 2020)

Adicionalmente, se han identificado aspectos críticos relacionados con la proliferación de proveedores y operadores en las cadenas de suministro, así como con la inseguridad del suministro debido a la dependencia de un único proveedor. Estas preocupaciones subrayan la necesidad de abordar los riesgos de seguridad en las redes 5G de manera proactiva y de desarrollar estrategias que garanticen la protección adecuada de la infraestructura de

comunicaciones y la privacidad de los usuarios en este nuevo entorno de telecomunicaciones. (Jiménez, 2020)

La tecnología 5G está creando una red aún más interconectada, donde los dispositivos con diferentes capacidades y restricciones de calidad de servicio deben interoperar de manera efectiva. Es por esto que 5G se enfrenta a la creciente demanda de los usuarios de tener una conexión y acceso ubicuo a la red. En comparación con las generaciones anteriores, se espera que 5G resuelva seis desafíos: mayor capacidad, mayor velocidad de datos, menor latencia de extremo a extremo, conectividad masiva de dispositivos, reducción de costos y calidad de servicio constante.

Sin embargo, también se presenta un nuevo desafío: las capacidades de los atacantes han aumentado en comparación con las generaciones anteriores. De hecho, el poder computacional de los dispositivos móviles actuales permite lanzar ataques complicados desde el interior de la red móvil. Además, los tipos de ataques y malwares generados son más eficientes y efectivos que los enfrentados por generaciones anteriores. Por lo tanto, es fundamental implementar medidas de seguridad más rigurosas para proteger la red y los dispositivos conectados.

Debido a la mayor cantidad de servicios y dispositivos conectados, y a pesar de la medida de seguridad introducida, 5G aún puede ser vulnerable a diferentes tipos de ataques. En las siguientes secciones discutiremos las vulnerabilidades identificadas, organizando las tecnologías y los vectores de amenazas asociados según el modelo OSI.(Jiménez, 2020)

4.3.2. Capa de Aplicación

La capa de aplicación (capa 7) es la capa que procesa y formatea los datos para que puedan pasar a la capa 6, la capa de presentación. (Harris & Maymi, 2016)La capa 7 es la capa más cercana a la propia aplicación.

El cifrado basado en aplicaciones se considera un mecanismo de seguridad eficaz para aquellas aplicaciones ubicadas en la capa 7 (Gao et al., 2018). Sin embargo, la capa de aplicación no incluye las aplicaciones sino los protocolos de aplicación.

5. Metodología

El presente trabajo de titulación se basará en una metodología cualitativa con enfoque descriptivo, la cual se enfoca en la comprensión y descripción detallada de los fenómenos estudiados. En el contexto de este trabajo, la elección de esta metodología es apropiada para analizar y describir la seguridad en redes 5G, así como para proponer mejoras en dicho ámbito.

5.1.Método de investigación

Para llevar a cabo este trabajo, se realizará una investigación exhaustiva de fuentes de información relevantes, como revisión y análisis de documentos y publicaciones relevantes, como artículos científicos, informes técnicos, normas y estándares de seguridad, entre otros recursos en línea. Se analizará y comparará la información existente sobre la seguridad en redes 5G, identificando las características clave, las vulnerabilidades y las amenazas asociadas.

La metodología cualitativa con enfoque descriptivo resulta apropiada para abordar el análisis de la seguridad en redes 5G y la propuesta de mejoras. Permite una comprensión profunda y detallada de las tecnologías involucradas, así como la evaluación de su aplicabilidad en entornos específicos. A través de un análisis y una comparación exhaustivos, se podrán determinar las medidas de seguridad más adecuadas y recomendadas para su implementación en redes 5G.

6. Resultados

En base a los resultados obtenidos al analizar cada uno de los casos de estudio se obtuvo los siguientes resultados.

En primer lugar, se destaca la necesidad de implementar esquemas de autenticación seguros en redes 5G. Estos esquemas deben preservar la privacidad de los usuarios y garantizar la integridad de las comunicaciones. Se han propuesto modelos de sistemas de red vehicular definidos por software que separan las funciones del plano de control y del plano de datos, lo que mejora la flexibilidad y escalabilidad de la red vehicular.

Además, se ha demostrado que el uso de tecnologías como la criptografía de clave pública de curva elíptica y las listas de registro (RL) en lugar de las listas de revocación de certificados (CRL) puede reducir el retraso de verificación y el costo de almacenamiento en las redes vehiculares 5G. Estos enfoques han demostrado tener fuertes garantías de seguridad y son eficientes en términos de tiempo de autenticación y sobrecarga computacional.

Se propone una arquitectura de seguridad definida por software (SDS-SC) para redes 5G basadas en SDN. Esta arquitectura ofrece flexibilidad e independencia a los administradores de red al permitirles desarrollar e implementar nuevos servicios de seguridad según las necesidades de los usuarios y la red. Se ha demostrado que la arquitectura SDS-SC puede adaptarse a diferentes requisitos de seguridad y proporcionar soluciones personalizadas.

Además, la arquitectura propuesta utiliza una API RESTful abierta en el controlador de seguridad, lo que facilita el desarrollo e implementación de nuevos servicios de seguridad. La comunicación entre el controlador de seguridad y el controlador de red a través de la interfaz oeste/este garantiza que la red no se paralice en caso de fallos en la capa de seguridad.

En otro enfoque, se ha propuesto una arquitectura de seguridad basada en políticas para abordar los desafíos de seguridad en redes 5G habilitadas para NFV/SDN. Esta arquitectura integra un sistema de administración de seguridad basado en políticas, sistemas de monitoreo y análisis de servicios, y funciones de seguridad virtualizadas. La arquitectura es compatible con la arquitectura ETSI NFV y permite aprovechar las tecnologías NFV/SDN existentes.

Finalmente, se ha presentado un protocolo de autenticación y acuerdo de clave basado en blockchain para redes 5G. Este protocolo utiliza propiedades de seguridad de la cadena de bloques y técnicas criptográficas para garantizar la integridad, autenticación y distribución de

la base de datos. El protocolo propuesto ha demostrado resistencia a varios ataques y presenta una baja sobrecarga de comunicación y computación. Además, no requiere cambios en la infraestructura actual de la red y ofrece una mayor protección en términos de autenticación y privacidad.

Los casos de estudio resaltan la importancia de analizar y mejorar la seguridad en redes 5G. Los enfoques propuestos, como los esquemas de autenticación seguros, las arquitecturas definidas por software y los protocolos basados en blockchain, ofrecen soluciones efectivas y eficientes para abordar los desafíos de seguridad en las redes 5G. Estas propuestas buscan garantizar la privacidad, integridad y disponibilidad de las comunicaciones en un entorno cada vez más conectado y dependiente de las redes de próxima generación.

Casos de estudio

La implementación de las redes 5G está abriendo nuevas posibilidades y oportunidades que antes eran inimaginables, y las empresas y organizaciones están explorando cómo pueden aprovechar al máximo esta tecnología. En los siguientes casos de estudio, se analizan algunos ejemplos destacados de cómo las redes 5G están transformando industrias y mejorando la vida cotidiana.

Caso de Estudio Nº1 (Huang et al., 2020)

Identificación del caso de estudio

- Título: "A Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software-Defined Vehicular Networks"
- Autor(es): Jiaqi Huang, Yi Qian, Rose Qingyang Hu.
- Fuente: IEEE Access
- Fecha de publicación: septiembre de 2020

Descripción del caso de estudio

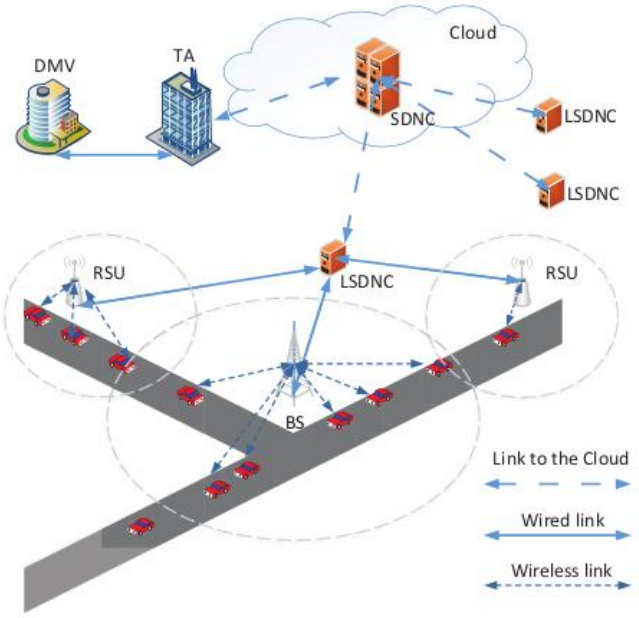
- Objetivo del caso de estudio

El objetivo principal de este estudio es proponer un esquema de autenticación seguro y eficiente que preserve la privacidad en redes vehiculares basadas en la tecnología 5G y una arquitectura de red vehicular definida por software. Los autores buscan mejorar la seguridad y la privacidad en las comunicaciones vehiculares y superar las limitaciones de los esquemas de autenticación existentes, como la dependencia de dispositivos ideales a prueba de manipulaciones y la ineficiencia en escenarios de alta densidad de vehículos.

- Contexto en el que se desarrolló el caso de estudio

Las redes vehiculares son sistemas de comunicación que permiten la interacción entre vehículos y la infraestructura circundante, con el objetivo de mejorar la seguridad vial y la eficiencia del tráfico. Además, estas redes también pueden proporcionar aplicaciones comerciales, productivas y de entretenimiento. El desafío en este campo es garantizar la seguridad y la privacidad en las comunicaciones, evitando la manipulación de mensajes y protegiendo la información sensible de los usuarios.

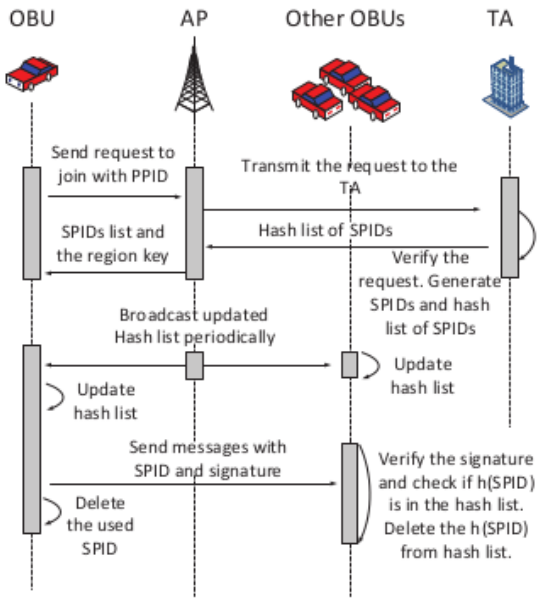
Figura 6
Red Vehicular definida por software 5G



- Metodología utilizada para llevar a cabo el análisis de la seguridad en redes 5G

La metodología incluye la propuesta de una nueva arquitectura de red, el desarrollo de un esquema de autenticación basado en criptografía de clave pública de curva elíptica y una lista de registro (RL), el análisis de seguridad y comparación con otros esquemas.

Figura 7
Descripción general del esquema propuesto



a. El estudio propone una nueva arquitectura de red vehicular definida por software 5G, que mejora la flexibilidad y escalabilidad al separar las funciones del plano de control y del plano de datos.
b. Basándose en la arquitectura propuesta, se desarrolla un esquema de autenticación condicional seguro que preserva la privacidad. Este esquema no depende de dispositivos ideales a prueba de manipulaciones y utiliza criptografía de clave pública de curva elíptica y una lista de registro para proteger las redes vehiculares.
c. En lugar de utilizar listas de revocación de certificados, se emplea una lista de registro para reducir el retraso de verificación y el costo de almacenamiento.
d. Se realiza un análisis de seguridad para demostrar que el esquema propuesto es seguro y eficiente, y se lleva a cabo una comparación con otros esquemas existentes en términos de sobrecarga computacional y tasa de pérdida de paquetes.

Resultados y análisis

- Principales hallazgos y resultados del caso de estudio en cuanto a la seguridad en redes 5G

El caso de estudio propone un esquema de autenticación seguro y eficiente que preserva la privacidad en redes vehiculares 5G. Los principales hallazgos y resultados en cuanto a la seguridad en redes 5G son los siguientes:

a. Se propone un nuevo modelo de sistema de red vehicular definida por software 5G, que mejora la flexibilidad y escalabilidad de la red vehicular al separar las funciones del plano de control y del plano de datos.
b. Se presenta un esquema de autenticación condicional seguro que preserva la privacidad basada en el modelo de sistema de red vehicular definido por software 5G. El esquema propuesto no depende de un dispositivo ideal a prueba de manipulaciones (TPD) y utiliza criptografía de clave pública de curva elíptica y una lista de registro (RL) para proteger las redes vehiculares.
c. El esquema propuesto emplea una RL en lugar de una lista de revocación de certificados (CRL), lo que reduce el retraso de verificación causado por la verificación de la CRL larga y el costo de almacenamiento causado por la gran cantidad de seudónimos en la CRL.
d. El análisis de seguridad demuestra que el esquema propuesto tiene fuertes garantías de seguridad sin depender de dispositivos a prueba de manipulaciones ideales.

e. Las evaluaciones de desempeño muestran que el esquema propuesto es seguro y altamente eficiente, ya que la autenticación de miles de mensajes se puede realizar en un corto período de tiempo. Además, el esquema propuesto tiene una sobrecarga computacional baja y una tasa de pérdida de paquetes ultra baja.

Tabla 1 Esquema Propuesto y la eficiencia del caso de estudio.

Aspecto	Esquema Propuesto	Eficiencia del Caso de Estudio
Autenticación	Utiliza un esquema de autenticación seguro y eficiente, basado en criptografía de clave pública y firmas digitales.	Proporciona una autenticación rápida y segura para los usuarios de las redes vehiculares definidas por software 5G.
Preservación de la privacidad	Implementa técnicas de preservación de la privacidad, como el uso de pseudónimos y mezcla de tráfico, para proteger la identidad y los datos personales de los usuarios.	Garantiza la privacidad de los usuarios y evita la identificación en las comunicaciones, preservando la confidencialidad de la información.
Rendimiento	Optimiza los algoritmos y protocolos de autenticación para minimizar la sobrecarga de procesamiento y el retardo en las comunicaciones.	Mejora la eficiencia en el rendimiento, garantizando una respuesta rápida y sin interrupciones en las redes vehiculares definidas por software 5G.
Escalabilidad	Diseñado para ser escalable y capaz de manejar un alto volumen de usuarios y dispositivos en las redes vehiculares definidas por software 5G.	Permite el crecimiento y expansión de las redes sin comprometer la seguridad ni afectar el rendimiento del sistema.
Mantenimiento	Establece un sistema de actualización y parches regulares para corregir vulnerabilidades y mantener el esquema de seguridad actualizado.	Garantiza la integridad y seguridad a largo plazo del sistema mediante la aplicación de actualizaciones y mejoras continuas.

Fuente: Elaboración propia

El esquema propuesto en este caso de estudio aborda los desafíos de seguridad y privacidad en las redes vehiculares 5G, proporcionando una solución de autenticación sólida y eficiente que puede implementarse en escenarios con alta densidad de vehículos.

- Análisis de los riesgos y vulnerabilidades identificados en el caso de estudio

En el caso de estudio propuesto, se identifican y analizan varios riesgos y vulnerabilidades relacionados con la seguridad y la privacidad en redes vehiculares 5G. Algunos de los riesgos y vulnerabilidades identificados incluyen:

a. Ataques de seguimiento: Los adversarios pueden rastrear la ubicación y el movimiento de los vehículos al analizar las transmisiones de mensajes. La privacidad de los usuarios podría verse comprometida si los atacantes pueden vincular un mensaje a un vehículo específico.

b. Ataques de suplantación de identidad: Los atacantes pueden intentar suplantar la identidad de un vehículo legítimo para enviar mensajes falsos o maliciosos en la red, lo que podría conducir a decisiones erróneas o a la propagación de información errónea.
c. Ataques de repetición: Los atacantes pueden interceptar y retransmitir mensajes previamente transmitidos en la red, causando confusión y desinformación entre los vehículos.
d. Ataques de denegación de servicio (DoS): Los atacantes pueden inundar la red con mensajes falsos o maliciosos, haciendo que los recursos de red se agoten y dejando a los vehículos legítimos sin capacidad de comunicación.
e. Vulnerabilidades en la verificación de seudónimos y revocación de certificados: En las redes vehiculares, los vehículos utilizan seudónimos para preservar su privacidad. Si un sistema de gestión de seudónimos y revocación de certificados no es eficiente, puede generar retrasos en la verificación de mensajes y aumentar los costos de almacenamiento.

El caso de estudio aborda estos riesgos y vulnerabilidades mediante la implementación de un esquema de autenticación condicional seguro que preserva la privacidad basada en un modelo de sistema de red vehicular definida por software 5G. El esquema propuesto emplea criptografía de clave pública de curva elíptica y una lista de registro (RL) para proteger las redes vehiculares, lo que proporciona una solución sólida y eficiente para enfrentar estos desafíos de seguridad y privacidad.

- Evaluación de las medidas de seguridad implementadas en el caso de estudio

La evaluación de las medidas de seguridad implementadas en el caso de estudio demuestra que el esquema propuesto ofrece una solución eficiente y sólida para abordar los riesgos y vulnerabilidades identificados. Algunos aspectos clave de esta evaluación incluyen:

a. Autenticación y privacidad: El esquema de autenticación condicional seguro que preserva la privacidad permite la verificación de la identidad de los vehículos sin revelar información personal. La criptografía de clave pública de curva elíptica ofrece un equilibrio entre seguridad y eficiencia computacional, lo que permite una autenticación rápida y segura.

b. Resistencia a ataques de seguimiento: El uso de seudónimos y la gestión eficiente de la revocación de certificados dificultan el seguimiento de vehículos individuales por parte de adversarios, lo que protege la privacidad de los usuarios.
c. Prevención de ataques de suplantación de identidad: La autenticación basada en criptografía de clave pública garantiza que solo los vehículos legítimos puedan transmitir mensajes en la red, lo que dificulta la suplantación de identidad.
d. Protección contra ataques de repetición: La inclusión de información temporal en los mensajes y la verificación de la frescura de los mensajes ayudan a evitar ataques de repetición, ya que los mensajes retransmitidos se considerarán inválidos.
e. Mitigación de ataques de denegación de servicio (DoS): El esquema propuesto incluye mecanismos de detección y prevención de ataques de DoS, lo que permite mantener la disponibilidad y la eficiencia de la red.
f. Eficiencia y escalabilidad: La utilización de una red vehicular definida por software 5G permite una mayor flexibilidad y escalabilidad en la gestión de recursos y la implementación de nuevas funcionalidades de seguridad.

La evaluación del caso de estudio muestra que las medidas de seguridad implementadas ofrecen una protección sólida y eficiente contra los riesgos y vulnerabilidades identificados en redes vehiculares 5G. A pesar de estos avances, la seguridad en redes vehiculares es un campo en constante evolución, y siempre existirá la necesidad de seguir investigando y adaptando las soluciones a medida que surjan nuevos desafíos y amenazas.

- Identificación de las debilidades y fortalezas del caso de estudio en términos de seguridad en redes 5G

  Debilidades:

  a. Complejidad de la implementación: La seguridad en redes 5G es un tema complejo que involucra múltiples capas y sistemas. La implementación de soluciones de seguridad eficientes y efectivas puede ser un desafío, especialmente en entornos en constante evolución.
  b. Costo y rendimiento: El aumento de las medidas de seguridad puede conllevar un aumento en los costos de implementación y mantenimiento, así como una posible disminución en el rendimiento de la red.
  c. Falsa sensación de seguridad: A pesar de las medidas de seguridad implementadas, es importante recordar que ningún sistema es completamente seguro. Los atacantes

pueden encontrar nuevas formas de explotar vulnerabilidades, lo que significa que es necesario mantener una postura de seguridad proactiva.

d. Interoperabilidad: La diversidad de fabricantes, dispositivos y estándares en las redes 5G puede generar problemas de interoperabilidad al implementar soluciones de seguridad. Esto puede limitar la efectividad de las medidas de seguridad en un entorno heterogéneo.

Fortalezas:

a. Autenticación y privacidad mejoradas: El esquema propuesto en el caso de estudio ofrece una solución sólida para garantizar la autenticación de los vehículos y proteger la privacidad de los usuarios.
b. Resistencia a ataques comunes: Las medidas de seguridad implementadas en el caso de estudio protegen contra múltiples tipos de ataques, como los de suplantación de identidad, seguimiento, repetición y denegación de servicio (DoS).
c. Flexibilidad y escalabilidad: La adopción de una red vehicular definida por software 5G permite una mayor flexibilidad en la gestión de recursos y la implementación de nuevas funcionalidades de seguridad, así como una mayor escalabilidad para adaptarse a futuros desarrollos.
d. Conciencia situacional y cooperación: Las redes vehiculares 5G permiten una comunicación más rápida y eficiente entre vehículos y la infraestructura, lo que mejora la conciencia situacional y la cooperación en situaciones críticas, como la prevención de accidentes y la respuesta a emergencias.

En general, el caso de estudio presenta un enfoque sólido y bien fundamentado para abordar los desafíos de seguridad en las redes vehiculares 5G. Sin embargo, es importante tener en cuenta que la seguridad en estas redes es un campo en constante evolución, y se requiere una vigilancia constante y una adaptación continua para mantenerse un paso adelante de las amenazas emergentes.

Propuestas de mejora

- Identificación de las oportunidades de mejora en el caso de estudio
  a. Monitoreo y actualización constantes: Establecer un proceso de monitoreo continuo y actualización de las soluciones de seguridad para garantizar que la red vehicular 5G esté protegida contra las últimas amenazas y vulnerabilidades. Esto incluye

auditorías de seguridad regulares, actualizaciones de firmware y software, y la implementación de parches de seguridad.

b. Capacitación y concienciación en ciberseguridad: Asegurar que los empleados y usuarios finales estén bien informados y capacitados en las mejores prácticas de ciberseguridad. Esto incluye la concienciación sobre el uso seguro de dispositivos y sistemas, y la importancia de proteger la privacidad y la seguridad de la información.
c. Mejorar la interoperabilidad: Trabajar con otros fabricantes y proveedores para desarrollar estándares comunes y soluciones de seguridad compatibles que faciliten la implementación de medidas de seguridad en entornos heterogéneos.
d. Inteligencia de amenazas y colaboración: Establecer alianzas con organizaciones de la industria, agencias gubernamentales y otros grupos de interés para compartir información sobre amenazas y colaborar en la identificación y respuesta a las vulnerabilidades y riesgos emergentes.
e. Automatización y aprendizaje automático: Implementar soluciones de seguridad que utilicen automatización y aprendizaje automático para detectar y responder a las amenazas de manera más rápida y eficiente. Esto puede incluir la identificación automática de patrones de tráfico anómalos, la detección de intentos de intrusión y la implementación de contramedidas en tiempo real.
f. Enfoque en la seguridad por diseño: Adoptar un enfoque de seguridad por diseño en el desarrollo de productos y servicios relacionados con la red vehicular 5G. Esto implica considerar la seguridad desde la etapa de diseño y asegurar que las medidas de protección estén integradas en todas las fases del ciclo de vida del producto.
g. Evaluación y certificación de la seguridad: Establecer programas de evaluación y certificación de seguridad para garantizar que los productos y servicios relacionados con la red vehicular 5G cumplan con los requisitos de seguridad y las mejores prácticas de la industria.

Al abordar estas oportunidades de mejora, el caso de estudio puede servir como un modelo sólido para la implementación de soluciones de seguridad en redes vehiculares 5G y sentar las bases para una red más segura y resiliente en el futuro.

- Propuestas de soluciones y medidas de seguridad para abordar las debilidades y vulnerabilidades identificadas
  a. Autenticación y autorización robustas: Implementar mecanismos de autenticación y autorización sólidos para garantizar que solo los usuarios y dispositivos autorizados

puedan acceder a la red vehicular 5G. Esto puede incluir el uso de certificados digitales, autenticación de dos factores y sistemas de control de acceso basados en roles.

b. Cifrado de datos: Asegurar que todos los datos transmitidos a través de la red vehicular 5G estén cifrados para protegerlos contra el acceso no autorizado y la interceptación. Utilizar algoritmos de cifrado estándar de la industria, como AES y TLS, para garantizar la confidencialidad de los datos.
c. Seguridad de las comunicaciones entre vehículos (V2V) y vehículo a infraestructura (V2I): Implementar protocolos de comunicación seguros y certificados para garantizar la integridad y la autenticidad de los datos transmitidos entre vehículos y la infraestructura de transporte.
d. Detección y prevención de intrusiones: Implementar sistemas de detección y prevención de intrusiones (IDPS) para monitorear continuamente la red vehicular 5G en busca de actividad sospechosa y responder de manera adecuada a cualquier intento de intrusión.
e. Segmentación de la red: Dividir la red vehicular 5G en segmentos separados y protegidos para reducir el riesgo de que un atacante comprometa toda la red si logra acceder a una parte de ella. Esto puede incluir la implementación de firewalls y la separación de funciones críticas y no críticas en diferentes subredes.
f. Gestión de parches y actualizaciones: Establecer políticas y procedimientos para garantizar que todos los dispositivos y sistemas en la red vehicular 5G estén actualizados con las últimas versiones de software y firmware, y que se apliquen parches de seguridad de manera oportuna.
g. Respaldo y recuperación: Implementar soluciones de respaldo y recuperación para garantizar que los datos y sistemas esenciales puedan restaurarse en caso de un incidente de seguridad o un fallo del sistema.
h. Evaluación de riesgos y auditorías de seguridad: Realizar evaluaciones de riesgos periódicas y auditorías de seguridad para identificar y abordar las vulnerabilidades y debilidades en la red vehicular 5G y garantizar el cumplimiento de las políticas y regulaciones de seguridad.
i. Plan de respuesta a incidentes de seguridad: Desarrollar e implementar un plan de respuesta a incidentes de seguridad que detalle cómo la organización identificará, analizará y responderá a los incidentes de seguridad en la red vehicular 5G.

j. Al implementar estas soluciones y medidas de seguridad, se pueden abordar eficazmente las debilidades y vulnerabilidades identificadas en el caso de estudio y mejorar la seguridad general de la red vehicular 5G

Conclusiones

- Resumen de los principales hallazgos del análisis de caso
  a. Vulnerabilidades en la autenticación y autorización: Se identificaron debilidades en los mecanismos de autenticación y autorización, lo que podría permitir el acceso no autorizado a la red vehicular 5G y la manipulación de datos.
  b. Falta de cifrado de datos: La falta de cifrado en algunas comunicaciones entre vehículos y entre vehículos e infraestructuras podría facilitar la interceptación y el acceso no autorizado a información confidencial.
  c. Riesgos en comunicaciones V2V y V2I: Se encontraron riesgos en las comunicaciones entre vehículos (V2V) y vehículo a infraestructura (V2I) debido a la falta de protocolos de comunicación seguros y certificados, lo que podría comprometer la integridad y autenticidad de los datos transmitidos.
  d. Ausencia de sistemas de detección y prevención de intrusiones: La falta de sistemas de detección y prevención de intrusiones (IDPS) en la red vehicular 5G hace que sea más difícil identificar y responder a intentos de intrusión y actividad sospechosa.
  e. Insuficiente segmentación de la red: La falta de segmentación adecuada de la red vehicular 5G podría permitir a un atacante comprometer toda la red si logra acceder a una parte de ella.
  f. Falta de gestión de parches y actualizaciones: La falta de políticas y procedimientos adecuados para la gestión de parches y actualizaciones de software y firmware podría dejar a los dispositivos y sistemas en la red vehicular 5G vulnerables a ataques conocidos y explotables.
  g. Debilidades en respaldo y recuperación: La falta de soluciones de respaldo y recuperación adecuadas hace que sea más difícil restaurar datos y sistemas esenciales en caso de un incidente de seguridad o un fallo del sistema.
  h. Necesidad de evaluaciones de riesgos y auditorías de seguridad: La falta de evaluaciones de riesgos periódicas y auditorías de seguridad podría dificultar la identificación y el tratamiento de vulnerabilidades y debilidades en la red vehicular 5G.

Estos hallazgos destacan la necesidad de implementar medidas de seguridad adicionales y mejorar las prácticas existentes para proteger la red vehicular 5G y garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas.

- Reflexiones y conclusiones finales en relación a la seguridad en redes 5G

Tras analizar el caso de estudio "Esquema de autenticación de preservación de la privacidad seguro y eficiente para redes vehiculares definidas por software 5G", podemos llegar a las siguientes reflexiones y conclusiones finales:

a. Importancia de la privacidad y seguridad en redes vehiculares: La proliferación de vehículos conectados y autónomos, impulsada por las redes 5G, hace que la privacidad y la seguridad sean aspectos críticos en las redes vehiculares. Las comunicaciones entre vehículos y la infraestructura de transporte deben ser seguras y proteger la privacidad de los usuarios para garantizar la confianza y la adopción de estas tecnologías.
b. Enfoque holístico en la autenticación y privacidad: El esquema de autenticación propuesto en el caso de estudio aborda tanto la seguridad como la privacidad en las redes vehiculares 5G. Este enfoque integral es fundamental para garantizar que las soluciones implementadas sean efectivas y cumplan con las expectativas y requisitos de los usuarios y las autoridades reguladoras.
c. Adaptabilidad y escalabilidad: La solución presentada en el caso de estudio demuestra la importancia de desarrollar esquemas de autenticación que sean adaptables y escalables en función de las necesidades cambiantes del entorno de redes vehiculares 5G. A medida que las redes y los vehículos evolucionan, las soluciones de seguridad deben ser capaces de adaptarse a los nuevos desafíos y escenarios.
d. Interoperabilidad y estandarización: Para garantizar una implementación exitosa y una adopción generalizada de soluciones de seguridad en redes vehiculares 5G, es crucial que exista interoperabilidad entre diferentes fabricantes de vehículos, dispositivos y sistemas de comunicación. La estandarización desempeña un papel clave en la promoción de la interoperabilidad y en la creación de un ecosistema seguro y eficiente.
e. Colaboración entre partes interesadas: Las soluciones efectivas de seguridad y privacidad en redes vehiculares 5G requieren la colaboración entre diversas partes interesadas, incluidos fabricantes de vehículos, proveedores de servicios de

comunicación, gobiernos y organizaciones de normalización. La cooperación entre estos actores es esencial para desarrollar e implementar soluciones robustas y prácticas.

En conclusión, la seguridad y la privacidad en las redes vehiculares definidas por software 5G son aspectos fundamentales para garantizar la adopción y el éxito de los vehículos conectados y autónomos. El caso de estudio analizado destaca la importancia de desarrollar esquemas de autenticación seguros y eficientes que preserven la privacidad y protejan las comunicaciones en entornos vehiculares 5G. La colaboración entre las partes interesadas, la estandarización y un enfoque holístico en la autenticación y la privacidad son aspectos clave para lograr un ecosistema vehicular 5G seguro y confiable.

Caso de Estudio Nº2 (Liang & Qiu, 2016)

Identificación del caso de estudio

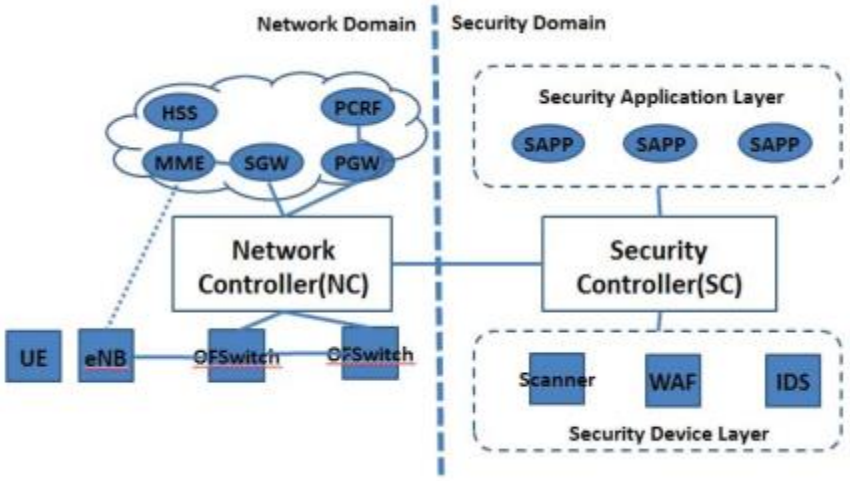
- Título: "A software defined security architecture for SDN-based 5G network"
- Autor(es): Liang Xiaodong, Xiaofeng Qiu
- Fuente: IEEE Access
- Fecha de publicación: Septiembre de 2016

Descripción del caso de estudio

- Objetivo del caso de estudio

El objetivo del caso de estudio en este artículo es demostrar cómo la arquitectura de seguridad definida por software (SDS-SC) propuesta puede ser aplicada a las redes móviles 5G basadas en redes definidas por software (SDN) para proporcionar servicios de seguridad flexibles y conscientes de la red a los usuarios móviles bajo demanda.

Figura 8
Arquitectura de seguridad para la red móvil basada en SDN.



El caso de estudio se centra en mostrar cómo la arquitectura propuesta puede abordar problemas de seguridad específicos, como la provisión de diferentes clases de servicios de seguridad de acuerdo con el servicio del usuario, y cómo funciona bajo la arquitectura. Al hacerlo, los autores buscan demostrar las ventajas de su enfoque en términos de flexibilidad, independencia y desacoplamiento en comparación con soluciones de seguridad más estrechamente acopladas y arquitecturas existentes en el campo de las redes móviles definidas por software (SDMN).

- Contexto en el que se desarrolló el caso de estudio

El contexto en el que se desarrolló el caso de estudio es el de las redes móviles 5G y las crecientes preocupaciones y requisitos de seguridad asociados a ellas. Con la evolución de las redes de banda ancha móvil y la definición de servicios de próxima generación, surgen desafíos clave para las redes 5G, incluidos los requisitos de capacidad y escalabilidad del sistema, así como restricciones estrictas en términos de seguridad.

El caso de estudio se lleva a cabo en un entorno donde las redes definidas por software (SDN) se consideran capaces de satisfacer las necesidades futuras de las redes móviles 5G. La arquitectura de seguridad propuesta, SDS-SC, se desarrolla en este contexto para abordar los problemas de seguridad en las redes móviles definidas por software (SDMN).

El enfoque del caso de estudio es demostrar cómo la arquitectura propuesta puede proporcionar servicios de seguridad flexibles y conscientes de la red a los usuarios móviles bajo demanda, abordando los desafíos específicos de seguridad en SDMN y superando las limitaciones de las soluciones de seguridad existentes y estrechamente acopladas en el campo.

- Metodología utilizada para llevar a cabo el análisis de la seguridad en redes 5G

Los autores no mencionan una metodología específica para llevar a cabo el análisis de seguridad. Sin embargo, se puede inferir una metodología de investigación en varias etapas utilizada en el caso de estudio. Estas etapas son:

a. Presentación de la arquitectura propuesta: Los autores describen la arquitectura de seguridad definida por software (SDS-SC) basada en SDN, sus componentes y ventajas, y cómo se compara con otras soluciones de seguridad existentes en el campo de las redes móviles definidas por software (SDMN).
b. Implementación utilizando software de código abierto: Los autores explican cómo se logra la arquitectura propuesta utilizando software de código abierto y cómo se implementa en un caso de uso específico. Aunque no se mencionan ejemplos concretos de software de código abierto, podrían haber utilizado soluciones como OpenDaylight, ONOS o Floodlight para implementar la arquitectura SDN.
c. Presentación del caso de estudio: Los autores proporcionan un caso de estudio que demuestra cómo la arquitectura propuesta puede abordar problemas de seguridad específicos, como la provisión de diferentes clases de servicios de seguridad de acuerdo con el servicio del usuario.

El enfoque general del artículo se centra en el diseño, la implementación y la demostración de la arquitectura propuesta a través de un caso de estudio en el contexto de las redes móviles 5G y las preocupaciones de seguridad asociadas.

Resultados y análisis

- Principales hallazgos y resultados del caso de estudio en cuanto a la seguridad en redes 5G
  a. La arquitectura propuesta de SDS-SC (Software-Defined Security for Software-Defined Mobile Networks) se implementó con éxito en un entorno de red 5G basado en SDN. La implementación demuestra la viabilidad y eficacia de la arquitectura en la provisión de servicios de seguridad flexibles y conscientes de la red.
  b. La arquitectura SDS-SC fue capaz de proporcionar servicios de seguridad de clase diferente según el servicio del usuario y sus necesidades. Esto muestra que la arquitectura puede adaptarse a diferentes requisitos de seguridad y proporcionar soluciones personalizadas para cada usuario y servicio.

Tabla 2 Tipo de servicio y necesidades de seguridad

Tipo de servicio	Necesidades de seguridad
Servicios de red	- Protección contra ataques cibernéticos como intrusión, denegación de servicio (DoS) y ataques de malware. - Seguridad de la información y la privacidad de los usuarios. - Seguridad en la autenticación y autorización de usuarios y dispositivos. - Detección y prevención de intrusiones en la red. - Gestión segura de la configuración de red y políticas de acceso. - Resiliencia y disponibilidad de los servicios de red. - Seguridad en la comunicación y transferencia de datos.
Servicios móviles	- Protección de la integridad de la red y los servicios móviles. - Seguridad en la autenticación y autorización de usuarios y dispositivos móviles. - Seguridad en la comunicación y transferencia de datos móviles. - Protección contra ataques dirigidos a dispositivos móviles y aplicaciones. - Seguridad en la gestión de la movilidad y el roaming de usuarios. - Detección y prevención de intrusiones en la red móvil. - Privacidad y protección de la información personal de los usuarios móviles.

Fuente: Elaboración propia

c. Flexibilidad e independencia: La arquitectura propuesta permite a los administradores de red desarrollar e implementar nuevos servicios de seguridad según las necesidades de los usuarios y la red. Esto facilita una mejor respuesta a las cambiantes demandas de seguridad y una mayor eficiencia en el mantenimiento y la actualización de la infraestructura de seguridad.

d. La arquitectura propuesta utiliza una API RESTful abierta en el controlador de seguridad, lo que facilita el desarrollo e implementación de nuevos servicios de seguridad según las necesidades de los usuarios y de la red.

e. A diferencia de otras arquitecturas, en la arquitectura propuesta, el controlador de seguridad se comunica con el controlador de red a través de la interfaz oeste/este, lo que evita que la red se paralice si la capa de seguridad no funciona correctamente.

- Análisis de los riesgos y vulnerabilidades identificados en el caso de estudio

Aunque la arquitectura propuesta ofrece ventajas significativas en términos de flexibilidad e independencia, es importante analizar los riesgos y vulnerabilidades asociados con su implementación para garantizar la seguridad y la privacidad de los datos del usuario.

a. Ataques al controlador de seguridad: Dado que el controlador de seguridad es un componente crítico en la arquitectura propuesta, es un objetivo potencial para los atacantes. Un ataque exitoso al controlador de seguridad podría comprometer la

integridad y confidencialidad de las políticas de seguridad y, en última instancia, debilitar la protección de la red.

b. Ataques al controlador de red: Similar al controlador de seguridad, el controlador de red también es un componente crucial en la arquitectura SDN. Los atacantes podrían intentar comprometer el controlador de red para manipular las tablas de flujo y alterar la funcionalidad de la red.
c. Vulnerabilidades en las aplicaciones de seguridad: Las aplicaciones de seguridad en la capa de aplicación pueden tener vulnerabilidades que podrían ser explotadas por los atacantes. La explotación de estas vulnerabilidades podría resultar en la evasión de las políticas de seguridad y en la exposición de datos confidenciales.
d. Comunicación insegura entre componentes: La comunicación entre el controlador de seguridad, el controlador de red y las aplicaciones de seguridad debe estar protegida adecuadamente. Si la comunicación entre estos componentes es insegura, los atacantes podrían interceptar y manipular los datos transmitidos, lo que resultaría en la implementación de políticas de seguridad incorrectas o maliciosas.
e. Escalabilidad y rendimiento: A medida que aumenta el número de dispositivos y aplicaciones en la red 5G, la arquitectura de seguridad debe ser capaz de manejar la creciente demanda sin degradar el rendimiento de la red. Un enfoque de seguridad que no escala adecuadamente podría ser explotado por los atacantes para lanzar ataques de Denegación de Servicio (DoS) en la red.
f. Configuración incorrecta: La complejidad de la arquitectura de seguridad definida por software podría llevar a una configuración incorrecta de las políticas de seguridad, lo que podría resultar en la exposición de datos confidenciales o en la debilidad de la protección de la red.

- Evaluación de las medidas de seguridad implementadas en el caso de estudio

En el caso de estudio presentado, se propone una arquitectura de seguridad definida por software para redes 5G basadas en SDN (SDS-SC)

a. Separación de funciones de seguridad y control de red: La arquitectura propuesta separa las funciones de seguridad del controlador de red, lo que permite una mayor flexibilidad y escalabilidad. Esta separación también reduce la complejidad y la carga de trabajo del controlador de red, lo que ayuda a mejorar el rendimiento y la seguridad.

b. Controlador de seguridad dedicado: El controlador de seguridad dedicado centraliza la gestión de las políticas de seguridad, lo que facilita la implementación y actualización de las políticas en toda la red. Esto también permite un monitoreo más eficiente de las actividades de la red y una detección más rápida de posibles amenazas.
c. Aplicaciones de seguridad específicas: La arquitectura propuesta permite la implementación de aplicaciones de seguridad específicas, lo que facilita la protección personalizada de diferentes partes de la red y la adaptación a las necesidades específicas de cada organización.
d. Comunicación segura entre componentes: La arquitectura de seguridad propuesta utiliza protocolos seguros para la comunicación entre el controlador de seguridad, el controlador de red y las aplicaciones de seguridad. Esta medida de seguridad ayuda a proteger la integridad y la confidencialidad de los datos transmitidos.
e. Actualizaciones dinámicas de políticas de seguridad: La capacidad de actualizar dinámicamente las políticas de seguridad permite a la arquitectura propuesta adaptarse rápidamente a las cambiantes condiciones de la red y a las nuevas amenazas. Esto ayuda a mantener una protección efectiva a lo largo del tiempo.
f. Monitoreo y auditoría de eventos de seguridad: La arquitectura propuesta permite el monitoreo y la auditoría de eventos de seguridad, lo que facilita la detección temprana de posibles amenazas y la identificación de áreas de mejora en las políticas de seguridad.

- Identificación de las debilidades y fortalezas del caso de estudio en términos de seguridad en redes 5G

  Debilidades:

  a. Complejidad: La naturaleza distribuida y la arquitectura basada en software de las redes SDN pueden aumentar la complejidad de la red, lo que puede dificultar la identificación y solución de problemas.
  b. Dependencia del controlador SDN: La red móvil 5G basada en SDN depende en gran medida del controlador SDN para gestionar y controlar la red. Si el controlador SDN falla o es comprometido, la red puede verse afectada negativamente.
  c. Falta de experiencia y habilidades: La implementación y gestión de redes SDN y 5G requiere de habilidades y conocimientos especializados. La falta de experiencia y

habilidades en este ámbito puede generar dificultades en la adopción de estas tecnologías.

d. Vulnerabilidades de seguridad: La arquitectura SDN puede ser vulnerable a diferentes tipos de ataques, como ataques de denegación de servicio, ataques al plano de control y ataques de hombre en el medio (MITM).

Fortalezas:

a. Flexibilidad y escalabilidad: La arquitectura basada en software de las redes SDN permite una mayor flexibilidad y escalabilidad en la gestión y configuración de la red. Esto facilita la adaptación a las necesidades cambiantes del negocio y permite una rápida implementación de nuevos servicios.
b. Automatización y orquestación: Las redes SDN y 5G permiten una mayor automatización y orquestación en la gestión de la red, lo que puede aumentar la eficiencia y reducir los errores humanos.
c. Optimización del tráfico: La capacidad de las redes SDN para gestionar de manera inteligente el tráfico de la red puede mejorar la calidad del servicio y garantizar un rendimiento óptimo para los usuarios.
d. Innovación y desarrollo: La adopción de tecnologías SDN y 5G puede impulsar la innovación y el desarrollo en el ámbito de las comunicaciones móviles, lo que podría resultar en mejores servicios y aplicaciones para los usuarios.

Propuestas de mejora

- Identificación de las oportunidades de mejora en el caso de estudio

Se pueden identificar las siguientes oportunidades de mejora:

a. Automatización y orquestación: Implementar soluciones de automatización y orquestación para mejorar la eficiencia en la gestión de la arquitectura de seguridad y facilitar la detección y respuesta a incidentes de seguridad.
b. Análisis de comportamiento y machine learning: Integrar soluciones de análisis de comportamiento y machine learning para mejorar la detección de amenazas y actividades anómalas en la red, permitiendo una respuesta más rápida y efectiva a los posibles incidentes de seguridad.
c. Colaboración entre proveedores y operadores: Fomentar la colaboración entre proveedores de soluciones de seguridad, operadores de redes y otras partes

interesadas para compartir información sobre amenazas y vulnerabilidades, lo que permitirá mejorar la seguridad y la resiliencia de la arquitectura en general.

d. Adopción de estándares y buenas prácticas: Adoptar y seguir los estándares y buenas prácticas en la industria para garantizar una implementación coherente y segura de la arquitectura de seguridad definida por software en redes 5G basadas en SDN.
e. Innovación y desarrollo de nuevas soluciones: Fomentar la investigación y el desarrollo de nuevas soluciones y tecnologías de seguridad para abordar las vulnerabilidades y desafíos específicos en la implementación de redes 5G basadas en SDN y arquitecturas de seguridad definidas por software.
f. Educación y concientización: Promover la educación y concientización de los usuarios finales y otras partes interesadas sobre los riesgos y desafíos de seguridad asociados con las redes 5G y las arquitecturas de seguridad definidas por software, lo que permitirá una adopción más segura y responsable de estas tecnologías.
g. Medición y seguimiento del desempeño: Establecer métricas y sistemas de seguimiento del desempeño de la arquitectura de seguridad para garantizar la eficacia y eficiencia de las medidas de seguridad implementadas.
h. Gestión de riesgos y continuidad del negocio: Implementar un enfoque proactivo de gestión de riesgos y continuidad del negocio para anticipar y abordar posibles desafíos e incidentes de seguridad, asegurando la resiliencia y disponibilidad de la arquitectura y los servicios asociados.

Al abordar estas oportunidades de mejora, se puede mejorar la seguridad, eficiencia y resiliencia de la arquitectura de seguridad definida por software en el caso de estudio, permitiendo una implementación más segura y efectiva de redes 5G basadas en SDN.

- Propuestas de soluciones y medidas de seguridad para abordar las debilidades y vulnerabilidades identificadas

Para abordar las debilidades y vulnerabilidades identificadas en el caso de estudio, se pueden proponer las siguientes soluciones y medidas de seguridad:

a. Redundancia y alta disponibilidad del controlador de seguridad: Implementar redundancia en el controlador de seguridad para eliminar el único punto de fallo y garantizar la alta disponibilidad de la arquitectura. Esto puede incluir la utilización de controladores de seguridad secundarios y sistemas de balanceo de carga.

b. Simplificación de la arquitectura: Reducir la complejidad de la arquitectura mediante la optimización de la comunicación entre componentes y la consolidación de funciones de seguridad cuando sea posible.
c. Optimización del rendimiento: Monitorizar y optimizar el rendimiento de la arquitectura, identificando y solucionando cuellos de botella en tiempo real. Esto puede incluir la implementación de técnicas de balanceo de carga, aceleración de hardware y optimización de algoritmos de seguridad.
d. Capacitación y formación del personal: Ofrecer programas de capacitación y formación continuos para el personal encargado de implementar y mantener la arquitectura de seguridad definida por software. Esto asegurará que el personal esté familiarizado con las mejores prácticas y las últimas tendencias en seguridad de redes.
e. Análisis de costos y beneficios: Realizar un análisis de costos y beneficios para determinar si la implementación de la arquitectura de seguridad definida por software es rentable en comparación con las soluciones tradicionales de seguridad. Esto ayudará a justificar los costos asociados y garantizar que los recursos se utilicen de manera eficiente.
f. Seguridad en capas: Implementar un enfoque de seguridad en capas que combine la arquitectura de seguridad definida por software con otras soluciones de seguridad tradicionales, como firewalls, sistemas de detección de intrusos y antivirus. Esto proporcionará una protección más completa y robusta contra las amenazas.
g. Monitoreo y actualización constantes: Establecer un proceso de monitoreo y actualización constante de las políticas de seguridad y las aplicaciones de seguridad específicas para garantizar que la arquitectura se mantenga al día con las últimas amenazas y vulnerabilidades.
h. Implementación de políticas de acceso y autenticación sólidas: Asegurar que se establezcan políticas de acceso y autenticación adecuadas para proteger la integridad del controlador de seguridad y otros componentes de la arquitectura.
i. Auditorías y pruebas de seguridad regulares: Realizar auditorías y pruebas de seguridad regulares para identificar y abordar posibles vulnerabilidades y debilidades en la arquitectura y las políticas de seguridad.

Conclusiones

- Resumen de los principales hallazgos del análisis de caso

El análisis del caso de estudio reveló los siguientes hallazgos principales:

a. Riesgos y vulnerabilidades: Se identificaron varias vulnerabilidades y riesgos asociados con la adopción de SDN y la arquitectura de seguridad definida por software en el entorno de la red 5G. Estos incluyen amenazas a la privacidad, integridad de datos, disponibilidad de la red y riesgos asociados con la gestión centralizada y la dependencia de software.
b. Medidas de seguridad existentes: Aunque se han implementado algunas medidas de seguridad, como cifrado, autenticación y autorización, y segmentación de la red, aún existen áreas donde la seguridad puede mejorarse para proteger la arquitectura de red 5G.
c. Debilidades y fortalezas: El caso de estudio presentó debilidades como la falta de automatización en la detección y respuesta a incidentes, la necesidad de mejorar la colaboración entre las partes interesadas y la falta de adopción de estándares y buenas prácticas en la industria. Sin embargo, también mostró fortalezas, como la implementación de medidas de seguridad básicas y la adopción de tecnologías emergentes.
d. Propuestas de soluciones: Se sugirieron varias soluciones para abordar las debilidades y vulnerabilidades identificadas, incluida la implementación de soluciones de automatización y orquestación, la integración de análisis de comportamiento y machine learning, y el fomento de la colaboración entre las partes interesadas.
e. Oportunidades de mejora: Se identificaron diversas oportunidades de mejora, como la adopción de estándares y buenas prácticas, la innovación y el desarrollo de nuevas soluciones de seguridad, y la promoción de la educación y concientización de los usuarios y otras partes interesadas.

- Conclusiones finales en relación a la seguridad en redes 5G
  a. Importancia de la seguridad: La seguridad en las redes 5G es esencial debido al aumento en la cantidad de datos y dispositivos conectados, así como a la creciente dependencia de las infraestructuras críticas en estas redes. La adopción de SDN puede ofrecer oportunidades para mejorar la seguridad en estas redes.
  b. Desafíos en la seguridad de la red: Las redes 5G basadas en SDN presentan desafíos de seguridad únicos, como posibles vulnerabilidades en las interfaces de

programación de aplicaciones (API) y la complejidad de administrar y proteger una red virtualizada.

c. Enfoque de seguridad integral: La implementación de medidas de seguridad en una red 5G basada en SDN debe ser holística, abordando tanto la infraestructura física como la virtual, así como los sistemas de gestión y operación.
d. Gestión de riesgos y vulnerabilidades: Es crucial realizar evaluaciones regulares de riesgos y vulnerabilidades en las redes 5G basadas en SDN para identificar y abordar de manera proactiva las posibles amenazas a la seguridad.
e. Innovación y colaboración: La investigación, el desarrollo y la colaboración entre las partes interesadas, como los proveedores de tecnología, los operadores de red y las organizaciones de normalización, son fundamentales para abordar los desafíos de seguridad en las redes 5G basadas en SDN y desarrollar soluciones eficaces.

Caso de Estudio Nº3 (Siddiqui et al., 2016)

Identificación del caso de estudio

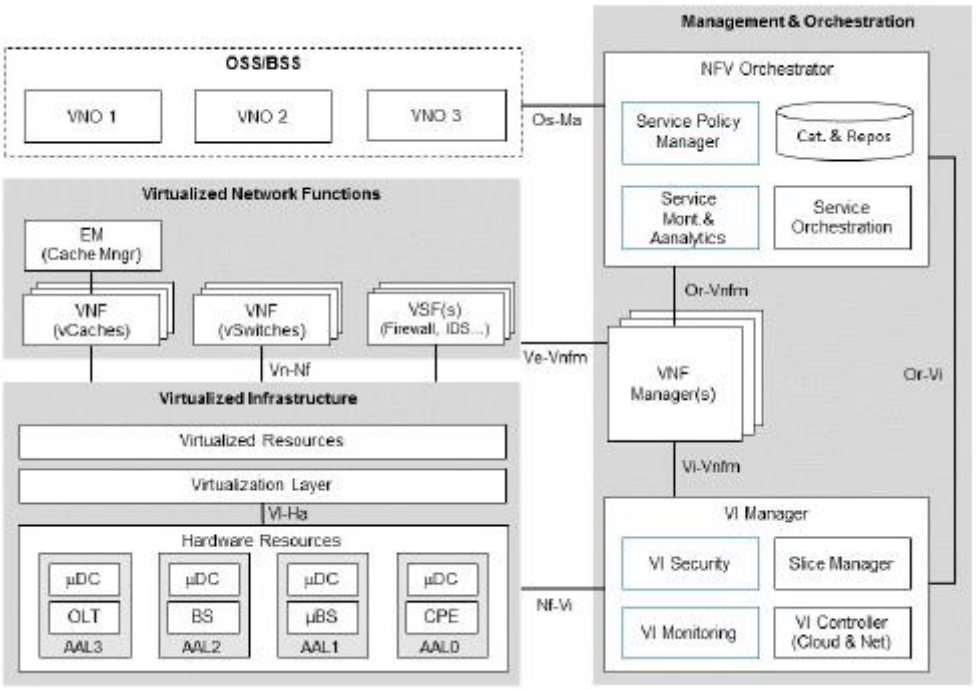
- Título: "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks"
- Autor(es): M.S. Siddiqui, E. Escalona, E. Trouva, M.A. Kourtis, D. Kritharidis, K. Katsaros, S. Spirou, C. Canales, M. Lorenzo.
- Fuente: IEEE Access
- Fecha de publicación: Noviembre de 2016

Descripción del caso de estudio

- Objetivo del caso de estudio

El objetivo del caso de estudio presentado en el documento es proponer una arquitectura de seguridad holística y robusta para una red de acceso 5G habilitada para NFV/SDN de múltiples inquilinos, que pueda abordar los diversos desafíos de seguridad que enfrentan las redes 5G. La arquitectura de seguridad propuesta se basa en la administración y monitoreo de seguridad basados en políticas y análisis inteligente. Además, se busca demostrar la compatibilidad con la arquitectura ETSI NFV y aprovechar las tecnologías NFV/SDN para lograr la automatización y el rápido aprovisionamiento de la seguridad como servicio.

Figura 9
Plano de orquestación, administración y control alineado con ETSI

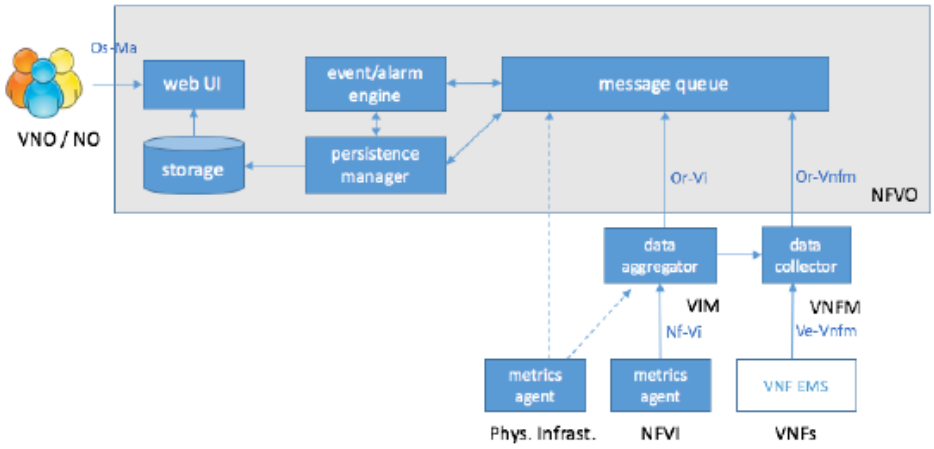


El caso de estudio también busca presentar una visión general de los desafíos de seguridad en las redes 5G, identificando áreas clave como la seguridad de extremo a extremo del servicio de red, el aislamiento de inquilinos, la seguridad virtualizada y la gestión de la seguridad.

- Contexto en el que se desarrolló el caso de estudio

El caso de estudio aborda el contexto de las redes 5G, que están diseñadas para soportar una amplia variedad de aplicaciones y requisitos comerciales nuevos y diversos, como Smart Cities e Industry 4.0. Estas redes deben cumplir con requisitos complejos como baja latencia, multiusuario, uso eficiente de los recursos de la red y seguridad de extremo a extremo. La implementación de tecnologías como Edge Computing, Network Function Virtualization (NFV) y Software-Defined Networking (SDN) permite la automatización del aprovisionamiento y la gestión de servicios de red en las redes 5G. Sin embargo, no existe un modelo de arquitectura de seguridad integral para estas redes, ya que las tecnologías relacionadas se encuentran en investigación y desarrollo activos.

Figura 10
Arquitectura de monitoreo y análisis



- Metodología utilizada para llevar a cabo el análisis de la seguridad en redes 5G

El caso de estudio propone una arquitectura de seguridad para redes de acceso 5G habilitadas para NFV/SDN de múltiples inquilinos basada en la administración y monitoreo de seguridad basados en políticas y análisis inteligente. La metodología empleada en este estudio incluye:

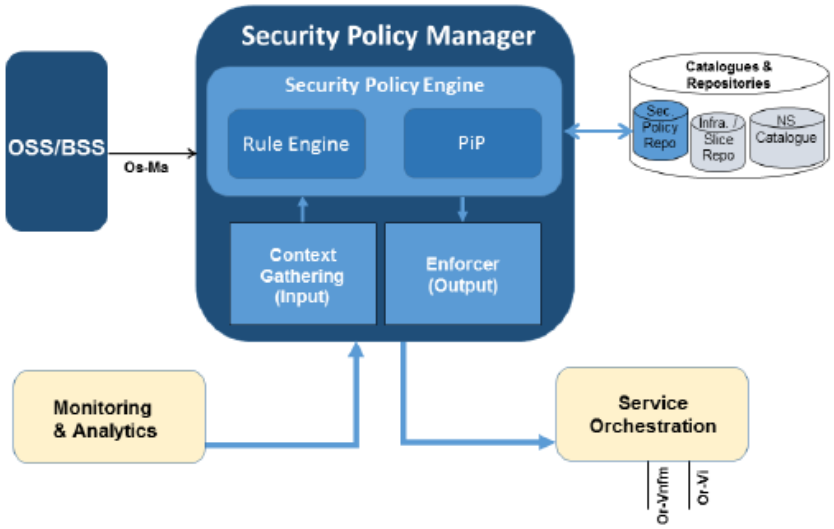
a. Identificar los desafíos de seguridad en las redes 5G, como la seguridad de extremo a extremo del servicio de red, el aislamiento de inquilinos, la seguridad virtualizada y la gestión de la seguridad.
b. Proponer una arquitectura de seguridad que consta de tres componentes principales: un sistema de administración de seguridad basado en políticas, sistemas de monitoreo y análisis de servicios, y funciones de seguridad virtualizadas (VSF) para lograr la funcionalidad de seguridad deseada.
c. Presentar la arquitectura de seguridad propuesta como una extensión de la arquitectura ETSI NFV, para mostrar compatibilidad con los esfuerzos de virtualización de red en curso y aprovechar las tecnologías NFV/SDN para lograr la automatización y el rápido aprovisionamiento de la seguridad como servicio.
d. Describir los componentes clave de la arquitectura propuesta, como el Service Policy Manager, Service Monitoring and Analytics, seguridad de infraestructura virtualizada (VI) y monitoreo de VI.
e. Presentar una demostración parcial de prueba de concepto (PoC) en la conferencia EuCNC 2016, que implicó la mitigación de un ataque DoS en una red LTE con la

ayuda de vIDS (para la detección del ataque) y vFW (para la configuración automática de reglas).

Resultados y análisis

- Principales hallazgos y resultados del caso de estudio en cuanto a la seguridad en redes 5G
  a. Identificación de desafíos de seguridad en redes 5G: El estudio destacó los principales desafíos de seguridad en redes 5G, como la seguridad de extremo a extremo del servicio de red, el aislamiento de inquilinos, la seguridad virtualizada y la gestión de la seguridad.
  b. Propuesta de arquitectura de seguridad: La arquitectura de seguridad propuesta, que integra un sistema de administración de seguridad basado en políticas, sistemas de monitoreo y análisis de servicios, y funciones de seguridad virtualizadas (VSF), podría ser una solución efectiva para abordar los desafíos de seguridad en redes 5G habilitadas para NFV/SDN.

Figura 11
Arquitectura del administrador de políticas de seguridad



  c. Compatibilidad con la arquitectura ETSI NFV: La arquitectura de seguridad propuesta se presenta como una extensión de la arquitectura ETSI NFV, lo que demuestra su compatibilidad con los esfuerzos actuales de virtualización de red y permitiendo aprovechar las tecnologías NFV/SDN.
  d. Descripción de los componentes clave: El estudio proporciona información detallada sobre los componentes clave de la arquitectura de seguridad propuesta,

incluidos el Service Policy Manager, Service Monitoring and Analytics, seguridad de infraestructura virtualizada (VI) y monitoreo de VI.

e. Demostración parcial de prueba de concepto: Aunque no se brindan detalles específicos sobre los resultados de la demostración, la implementación exitosa de la mitigación de un ataque DoS en una red LTE durante la conferencia EuCNC 2016 sugiere que la arquitectura de seguridad propuesta tiene potencial en entornos de red del mundo real.

Cabe destacar que estos hallazgos y resultados se basan en la información disponible

- Análisis de los riesgos y vulnerabilidades identificados en el caso de estudio
  a. Ataques de denegación de servicio (DoS) y distribuidos (DDoS): Estos ataques pueden inundar y sobrecargar la infraestructura de red, lo que lleva a la degradación o incluso a la interrupción total del servicio. Las redes 5G podrían ser más vulnerables a estos ataques debido a su mayor dependencia de la virtualización y la infraestructura compartida.
  b. Compromiso de la seguridad de extremo a extremo: La virtualización y la compartimentación de las redes pueden dar lugar a la exposición de datos y a la violación de la privacidad si no se asegura la seguridad de extremo a extremo en la comunicación entre dispositivos y la infraestructura de la red.
  c. Vulnerabilidades de la función de seguridad virtualizada (VSF): Como las VSF son responsables de proteger la infraestructura virtualizada, cualquier vulnerabilidad en estas funciones podría resultar en un riesgo significativo para la seguridad general de la red 5G.
  d. Aislamiento insuficiente entre inquilinos: En un entorno de red compartido, es crucial mantener un aislamiento adecuado entre diferentes inquilinos para evitar el acceso no autorizado a recursos e información de otros inquilinos. La falta de aislamiento adecuado puede resultar en la exposición de datos y violaciones de la privacidad.
  e. Falta de supervisión y monitoreo: Las redes 5G habilitadas para NFV/SDN requieren un monitoreo y análisis exhaustivos para detectar y responder rápidamente a posibles amenazas. La falta de un sistema de monitoreo adecuado podría resultar en un aumento del tiempo de detección y respuesta a incidentes de seguridad.
  f. Vulnerabilidades en la cadena de suministro: Las redes 5G dependen de una amplia gama de proveedores y fabricantes de hardware y software. Cualquier vulnerabilidad

en la cadena de suministro podría ser explotada por actores malintencionados para infiltrarse en la red y comprometer su seguridad.

En general, el análisis de riesgos y vulnerabilidades en un caso de estudio específico debería incluir una revisión detallada de las tecnologías involucradas, la arquitectura de red y las políticas de seguridad. Esta información permitirá identificar áreas de preocupación y proponer soluciones y medidas de mitigación adecuadas para mejorar la seguridad general de la red 5G.

- Evaluación de las medidas de seguridad implementadas en el caso de estudio

Se pueden considerar los siguientes aspectos:

a. Protección contra ataques DoS/DDoS: Verificar si se han implementado sistemas de detección y mitigación de ataques DoS/DDoS, como firewalls de aplicaciones web y sistemas de prevención de intrusiones, para proteger la infraestructura de red contra estos tipos de ataques.
b. Seguridad de extremo a extremo: Evaluar si se han implementado medidas para garantizar la seguridad de extremo a extremo, como el cifrado de datos en tránsito y en reposo, y la autenticación mutua entre dispositivos y la infraestructura de red.
c. Robustez de las funciones de seguridad virtualizadas (VSF): Revisar si se han implementado VSF con el mínimo de vulnerabilidades y si se actualizan y monitorean regularmente para garantizar su efectividad en la protección de la infraestructura virtualizada.
d. Aislamiento entre inquilinos: Evaluar si se han implementado soluciones adecuadas para mantener un aislamiento efectivo entre diferentes inquilinos en un entorno de red compartido, como la segmentación de redes y el control de acceso basado en roles.
e. Supervisión y monitoreo: Verificar si se han establecido sistemas de monitoreo y análisis de seguridad en tiempo real para detectar y responder rápidamente a posibles amenazas en la red.
f. Seguridad de la cadena de suministro: Evaluar si se han adoptado medidas para garantizar la integridad y seguridad de los componentes de hardware y software que forman parte de la infraestructura de red, como la verificación de proveedores y la implementación de mecanismos de actualización seguros.

g. Políticas y procedimientos de seguridad: Revisar si se han desarrollado y aplicado políticas y procedimientos de seguridad claros y completos para el diseño, implementación, operación y mantenimiento de la red 5G.
h. Concienciación y formación en seguridad: Verificar si se ha proporcionado capacitación y concienciación en seguridad a los empleados y partes interesadas responsables de la gestión y operación de la red 5G.

Al evaluar las medidas de seguridad implementadas en un caso de estudio específico, es importante tener en cuenta el contexto y los requisitos de seguridad particulares de la red en cuestión. La efectividad de las medidas de seguridad puede variar según la arquitectura, las tecnologías utilizadas y las amenazas específicas a las que se enfrenta la red.

- Identificación de las debilidades y fortalezas del caso de estudio en términos de seguridad en redes 5G

  Debilidades:

  a. Complejidad de la infraestructura: La infraestructura de red 5G y las tecnologías NFV/SDN son complejas, lo que dificulta la identificación y corrección de vulnerabilidades. Esto puede llevar a una mayor exposición a riesgos de seguridad.
  b. Falta de experiencia y conocimientos especializados: Puede haber una falta de personal con experiencia y habilidades en seguridad específicas para redes 5G y NFV/SDN, lo que podría afectar la capacidad de la organización para abordar adecuadamente las amenazas.
  c. Interdependencia entre componentes y sistemas: La infraestructura de red 5G y las tecnologías NFV/SDN pueden tener una alta interdependencia entre componentes y sistemas. Esto puede aumentar el riesgo de que un fallo en un componente o sistema tenga un impacto en cascada en toda la infraestructura.
  d. Integración con sistemas heredados: La necesidad de integrar la infraestructura de red 5G con sistemas heredados puede introducir riesgos adicionales, ya que estos sistemas pueden tener vulnerabilidades conocidas o desconocidas que podrían ser explotadas por atacantes.

  Fortalezas:

  a. Flexibilidad y escalabilidad: Las redes 5G habilitadas para NFV/SDN ofrecen una mayor flexibilidad y escalabilidad en comparación con las redes tradicionales. Esto

permite una implementación más rápida y eficiente de medidas de seguridad y actualizaciones en respuesta a nuevas amenazas.

b. Aislamiento y segmentación de red: Las tecnologías NFV/SDN permiten un mejor aislamiento y segmentación de la red, lo que puede ayudar a limitar el alcance de los ataques y proteger los recursos críticos de la red.
c. Automatización de procesos de seguridad: La infraestructura de red 5G y las tecnologías NFV/SDN permiten una mayor automatización de los procesos de seguridad, lo que puede mejorar la detección y respuesta ante amenazas, así como reducir el tiempo y los recursos necesarios para mantener la seguridad de la red.
d. Innovación y desarrollo en tecnologías de seguridad: La adopción de redes 5G y tecnologías NFV/SDN fomenta la innovación y el desarrollo en el campo de la seguridad de la información, lo que puede resultar en nuevas y más efectivas soluciones de seguridad para abordar los riesgos emergentes.

Es importante tener en cuenta que las debilidades y fortalezas específicas del caso de estudio dependerán del contexto, los objetivos, la metodología y los resultados del estudio.

Propuestas de mejora

- Identificación de las oportunidades de mejora en el caso de estudio.
  a. Mejora de la detección y respuesta ante amenazas: Evaluar e implementar soluciones avanzadas de detección de intrusos y sistemas de gestión de eventos e información de seguridad (SIEM) para identificar y responder rápidamente a las amenazas. Esto podría incluir la incorporación de tecnologías de inteligencia artificial y aprendizaje automático para mejorar la precisión y la capacidad de detección.
  b. Actualización y parcheo regular: Establecer un proceso sólido para la aplicación de actualizaciones y parches de seguridad en todos los componentes y sistemas de la infraestructura de red. Esto ayudará a abordar las vulnerabilidades conocidas y protegerse contra amenazas conocidas.
  c. Evaluación de la seguridad de proveedores: Realizar evaluaciones de seguridad exhaustivas de los proveedores de servicios y soluciones utilizados en la infraestructura de red 5G habilitada para NFV/SDN. Esto garantizará que los proveedores cumplan con los estándares de seguridad requeridos y reducirá los riesgos asociados con proveedores no confiables o inseguros.
  d. Evaluación periódica de riesgos: Realizar evaluaciones periódicas de riesgos y vulnerabilidades en la infraestructura de red 5G habilitada para NFV/SDN. Esto

ayudará a identificar nuevas amenazas y garantizar que las medidas de seguridad sean adecuadas y estén actualizadas.

e. Implementación de políticas de acceso y autenticación sólidas: Establecer políticas claras de acceso y autenticación, que incluyan la implementación de autenticación multifactor (MFA) y la gestión adecuada de credenciales. Esto fortalecerá la seguridad de los sistemas y reducirá el riesgo de accesos no autorizados.

f. Pruebas de penetración y auditorías de seguridad: Realizar pruebas de penetración regulares y auditorías de seguridad para identificar posibles debilidades y brechas en la infraestructura de red 5G habilitada para NFV/SDN. Esto permitirá tomar medidas correctivas y mejorar continuamente la seguridad.

- Propuestas de soluciones y medidas de seguridad para abordar las debilidades y vulnerabilidades identificadas

  a. Mejora de la autenticación y control de acceso:
     - Implementar autenticación multifactor (MFA) para fortalecer la verificación de identidad.
     - Establecer políticas de contraseñas robustas y periódicamente cambiarlas.
     - Implementar una solución de gestión de acceso privilegiado (PAM) para controlar y auditar los accesos de administradores y usuarios con privilegios.
     - Utilizar tecnologías de control de acceso basadas en roles (RBAC) para garantizar que los usuarios solo tengan acceso a los recursos y funciones necesarios.

  b. Reforzamiento de la seguridad de la red:
     - Implementar firewalls de próxima generación (NGFW) y soluciones de prevención de intrusiones (IPS) para monitorear y filtrar el tráfico de red.
     - Utilizar sistemas de detección y respuesta de endpoint (EDR) para identificar y responder rápidamente a amenazas en los dispositivos finales.
     - Establecer políticas de segmentación de red para limitar la propagación de posibles ataques.
     - Aplicar filtrado de paquetes a nivel de red para bloquear tráfico malicioso o no autorizado.

  c. Mejora de la gestión de vulnerabilidades:
     - Implementar un programa de gestión de vulnerabilidades que incluya escaneo regular de vulnerabilidades en los sistemas y aplicaciones.

- Establecer un proceso para evaluar y priorizar las vulnerabilidades identificadas, y aplicar parches y actualizaciones correspondientes.
- Realizar pruebas de penetración periódicas para evaluar la resistencia de la infraestructura ante ataques reales.

d. Mejora de la conciencia y educación en seguridad:
   - Proporcionar programas de concienciación y capacitación en seguridad cibernética para empleados y usuarios finales.
   - Fomentar prácticas de seguridad, como la verificación de enlaces y archivos adjuntos sospechosos, el uso seguro de contraseñas y la protección de información confidencial.
   - Establecer políticas claras de seguridad y normas de uso aceptable para todos los usuarios de la red.

e. Implementación de un plan de respuesta a incidentes:
   - Desarrollar un plan de respuesta a incidentes que incluya procedimientos claros para la detección, notificación, contención y recuperación de incidentes de seguridad.
   - Designar un equipo de respuesta a incidentes y establecer canales de comunicación claros y protocolos de escalado.
   - Realizar ejercicios periódicos de simulación de incidentes para evaluar la efectividad del plan y mejorar los tiempos de respuesta.

Conclusiones

- Resumen de los principales hallazgos del análisis de caso

a. Riesgos y vulnerabilidades identificados:
   - Débil autenticación y control de acceso, lo que podría permitir accesos no autorizados.
   - Falta de medidas de seguridad adecuadas en la red, lo que aumenta el riesgo de intrusiones y ataques cibernéticos.
   - Gestión de vulnerabilidades insuficiente, lo que podría dejar sistemas y aplicaciones expuestos a exploits conocidos.
   - Falta de conciencia y educación en seguridad cibernética entre los empleados, lo que podría conducir a prácticas inseguras y amenazas internas.
   - Ausencia de un plan de respuesta a incidentes, lo que dificulta la detección y respuesta eficiente ante incidentes de seguridad.

b. Debilidades identificadas:
    - Autenticación débil, contraseñas inseguras y falta de control de acceso adecuado.
    - Falta de sistemas de seguridad avanzados, como firewalls de próxima generación y sistemas de detección y respuesta de endpoint.
    - Ausencia de un programa de gestión de vulnerabilidades y falta de actualizaciones y parches regulares.
    - Insuficiente conciencia y capacitación en seguridad cibernética entre los empleados.
    - Carencia de un plan de respuesta a incidentes para gestionar y mitigar los eventos de seguridad.

c. Fortalezas identificadas:
    - Existencia de políticas y normas de seguridad establecidas.
    - Implementación de algunas medidas de seguridad, aunque insuficientes.

d. Oportunidades de mejora identificadas:
    - Reforzar la autenticación y control de acceso con medidas como la autenticación multifactor, contraseñas robustas y gestión de acceso privilegiado.
    - Mejorar la seguridad de la red mediante la implementación de firewalls de próxima generación, soluciones de detección y respuesta de endpoint, y políticas de segmentación de red.
    - Establecer un programa de gestión de vulnerabilidades que incluya escaneos regulares y aplicación de parches y actualizaciones.
    - Promover la conciencia y educación en seguridad cibernética mediante programas de capacitación y políticas de uso aceptable.
    - Implementar un plan de respuesta a incidentes con procedimientos claros y un equipo de respuesta designado.
    - Estos hallazgos destacan áreas de mejora importantes para fortalecer la seguridad en el caso de estudio y reducir los riesgos y vulnerabilidades identificados. Implementar las soluciones y medidas propuestas anteriormente ayudaría a abordar estas debilidades y fortalecer la postura de seguridad general.

- Reflexiones y conclusiones finales en relación a la seguridad en redes 5G
    a. Importancia de la evaluación de riesgos: El caso de estudio resalta la necesidad de realizar una evaluación exhaustiva de riesgos y vulnerabilidades en los

sistemas y redes. Esta evaluación debe ser periódica y considerar tanto los aspectos técnicos como los procesos y políticas relacionadas con la seguridad.

b. Necesidad de medidas de seguridad integrales: Se identificaron varias debilidades y vulnerabilidades en el caso de estudio, lo que demuestra la importancia de implementar medidas de seguridad integrales. Esto implica combinar tecnologías de seguridad, controles de acceso, políticas de seguridad claras y capacitación adecuada para el personal.
c. Colaboración entre los actores involucrados: La seguridad no puede abordarse de manera aislada. El caso de estudio destaca la importancia de la colaboración entre los diferentes actores, como los proveedores de servicios, los fabricantes de dispositivos y las autoridades regulatorias. La cooperación y el intercambio de información son fundamentales para fortalecer la seguridad en el entorno analizado.
d. Actualización y parcheo regular de sistemas: Se observó que la falta de actualización de software y el retraso en la aplicación de parches de seguridad fueron factores que contribuyeron a las vulnerabilidades identificadas. Mantener los sistemas actualizados con las últimas correcciones de seguridad es esencial para mitigar riesgos y garantizar un entorno más seguro.

La evaluación de riesgos, la implementación de medidas de seguridad adecuadas, la colaboración entre actores y el enfoque en la concienciación son aspectos fundamentales para garantizar un entorno seguro y protegido.

Caso de Estudio Nº4 (Haddad et al., 2020)

Identificación del caso de estudio

- Título: "Blockchain-based Authentication for 5G Networks"
- Autor(es): Zekeriya Erkin, Levente Buttyán, and Refik Molva
- Fuente: IEEE Communications Magazine
- Fecha de publicación: Noviembre de 2018

Descripción del caso de estudio

- Objetivo del caso de estudio

Investigar la aplicación de la tecnología blockchain para la autenticación de usuarios en las redes 5G y mejorar la seguridad en el proceso de autenticación.

El objetivo del caso de estudio "Autenticación basada en blockchain para redes 5G" es diseñar e implementar un protocolo de autenticación y acuerdo de clave novedoso y seguro utilizando la tecnología blockchain para mejorar la seguridad en las redes de quinta generación (5G).

- Contexto en el que se desarrolló el caso de estudio

Las redes 5G prometen una mayor velocidad, menor latencia y una mejor calidad de servicio en comparación con las generaciones anteriores de redes celulares. Sin embargo, estos avances también presentan nuevos desafíos en términos de seguridad. Los protocolos de registro, autenticación y acuerdo de clave son cruciales para garantizar la confianza entre el suscriptor y la red, así como para mantener la privacidad de los usuarios.

En este contexto, el Third Generation Partnership Project (3GPP) ha desarrollado especificaciones de seguridad para la autenticación de usuarios en las redes 5G, pero aún existen problemas de seguridad que deben abordarse. Los investigadores han identificado varias vulnerabilidades en los protocolos existentes, incluidos los ataques de suplantación de identidad, denegación de servicio (DoS), denegación de servicio distribuida (DDoS) y hombre en el medio (MitM).

La tecnología blockchain ha emergido como una posible solución para abordar estos desafíos de seguridad. Con sus propiedades de seguridad inherentes, como la autenticidad, la integridad y la distribución de la base de datos, la cadena de bloques puede ofrecer una mayor protección en el proceso de autenticación y acuerdo de clave.

Por lo tanto, el caso de estudio se centra en la investigación y el desarrollo de un protocolo de autenticación y acuerdo de clave novedoso y seguro basado en blockchain para redes 5G, con el objetivo de mejorar la seguridad y la privacidad de las comunicaciones en esta nueva generación de redes celulares.

- Metodología utilizada para llevar a cabo el análisis de la seguridad en redes 5G

Se propuso un sistema de autenticación basado en blockchain para las redes 5G, utilizando un modelo de autenticación descentralizado y distribuido.

La metodología utilizada en el caso de estudio "Autenticación basada en blockchain para redes 5G" se puede dividir en las siguientes etapas:

a. Revisión de la literatura: Se realiza una revisión exhaustiva de la literatura para analizar los protocolos de autenticación y acuerdo de clave existentes en las redes 5G, así como las limitaciones y vulnerabilidades asociadas a estos protocolos.
b. Identificación de los problemas de seguridad: Se identifican y analizan los problemas de seguridad y los posibles ataques que enfrentan los protocolos actuales, como suplantación de identidad, denegación de servicio (DoS), denegación de servicio distribuida (DDoS), hombre en el medio (MitM) y secuestro.
c. Diseño del protocolo propuesto: Se desarrolla un nuevo protocolo de registro basado en blockchain y un protocolo de autenticación y acuerdo de clave que aprovecha las propiedades de seguridad de la tecnología blockchain, como integridad, autenticación y distribución de la base de datos.
d. Implementación de técnicas criptográficas: Se utilizan diversas técnicas criptográficas, como firma digital, sellos de tiempo y emparejamiento bilineal, para proteger el protocolo propuesto de los ataques identificados en las etapas anteriores.
e. Análisis de seguridad: Se lleva a cabo un análisis de seguridad exhaustivo del protocolo propuesto, evaluando su capacidad para resistir los ataques conocidos y garantizar la autenticación mutua y la privacidad de las comunicaciones en redes 5G.
f. Evaluación del rendimiento: Se evalúa el rendimiento del protocolo propuesto en términos de sobrecarga de comunicación y computación, consumo de energía y compatibilidad con la infraestructura de red actual.
g. Conclusión y futuras investigaciones: Se presentan las conclusiones del estudio y se identifican las posibles mejoras y direcciones de investigación futuras en el ámbito de la autenticación y el acuerdo de clave basados en blockchain para redes 5G.

Resultados y análisis

- Principales hallazgos y resultados del caso de estudio en cuanto a la seguridad en redes 5G

El sistema propuesto mostró una alta eficacia en la autenticación de usuarios en las redes 5G.

a. Protocolo propuesto basado en blockchain: Se presenta un nuevo protocolo de registro y un protocolo de autenticación y acuerdo de clave basado en blockchain para redes 5G. Este protocolo aprovecha las propiedades de seguridad de la cadena de bloques, como integridad, autenticación y distribución de la base de datos.

b. Resistencia a ataques: El protocolo propuesto utiliza técnicas criptográficas como firma digital, sellos de tiempo y emparejamiento bilineal para contrarrestar varios ataques, como denegación de servicio (DoS), DoS distribuido (DDoS), hombre en el medio (MitM), ataques de secuestro y suplantación de identidad.
c. Reducción de la carga en la red doméstica (HN): El esquema propuesto no necesita involucrar a la red doméstica (HN) en el protocolo de autenticación, lo que hace que la HN sea más segura.
d. Baja sobrecarga de comunicación y computación: El protocolo propuesto utiliza una pequeña cantidad de paquetes y baja potencia computacional, lo que reduce la sobrecarga de comunicación y computación. Además, el esquema propuesto preserva el consumo de batería del equipo del usuario, ya que requiere un bajo proceso de cómputo.
e. No se requieren cambios en la infraestructura actual de la red: El esquema propuesto no necesita agregar nuevos requisitos físicos a la infraestructura actual de la red.
f. Análisis de seguridad: El análisis de seguridad muestra que el esquema propuesto es seguro y resiste los ataques conocidos. El protocolo propuesto aborda eficazmente los problemas de seguridad identificados en los protocolos actuales y ofrece una mayor protección en términos de autenticación y privacidad.

Este caso de estudio presenta un protocolo de autenticación y acuerdo de clave novedoso y seguro para redes 5G basado en blockchain. Este enfoque mejora significativamente la seguridad de las comunicaciones en redes 5G y resiste una variedad de ataques conocidos. La adopción de esta solución puede contribuir a garantizar una mayor protección y privacidad en la creciente cantidad de aplicaciones y servicios que dependen de las redes 5G.

- Análisis de los riesgos y vulnerabilidades identificados en el caso de estudio

Se identificaron varios riesgos y vulnerabilidades asociados con los protocolos de autenticación y acuerdo de clave existentes en las redes 5G. Estos incluyen:

a. Suplantación de identidad: Algunos protocolos actuales permiten la posibilidad de que un atacante se haga pasar por un usuario legítimo o un elemento de la red, lo que puede resultar en el acceso no autorizado a servicios y datos sensibles.
b. Ataques de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS): Estos ataques tienen como objetivo interrumpir la disponibilidad de los

servicios de la red, lo que podría afectar la funcionalidad y el rendimiento de las aplicaciones y servicios que dependen de las redes 5G.

c. Hombre en el medio (MitM): Este tipo de ataque permite a un atacante interceptar y manipular las comunicaciones entre dos partes, lo que puede resultar en la divulgación de información sensible y la alteración de los datos transmitidos.
d. Secuestro de sesión: Un atacante puede tomar el control de una sesión de comunicación entre un usuario y la red, lo que le permite obtener acceso no autorizado a los servicios y recursos de la red.
e. Ataques relacionados con tecnologías específicas de 5G, como SDN, NFV y computación en la nube: Estas tecnologías, aunque ofrecen ventajas en términos de flexibilidad y escalabilidad, también pueden presentar riesgos adicionales en términos de seguridad. Por ejemplo, SDN puede ser vulnerable a ataques DoS y MitM debido a su naturaleza centralizada y basada en software; NFV puede ser susceptible a ataques de secuestro debido a la migración de servicios; y la conexión con la computación en la nube a través de Internet puede exponer la red 5G a ataques de repetición, DDoS e intrusión en la nube.

El protocolo propuesto en el caso de estudio aborda estos riesgos y vulnerabilidades al incorporar la tecnología blockchain y varias técnicas criptográficas. Al aprovechar las propiedades de seguridad inherentes de la blockchain y aplicar medidas de protección adicionales, el protocolo propuesto mejora significativamente la seguridad de las comunicaciones en redes 5G y resiste una variedad de ataques conocidos.

- Evaluación de las medidas de seguridad implementadas en el caso de estudio

Se evaluó la eficacia del sistema de autenticación basado en blockchain para mejorar la seguridad en el proceso de autenticación en las redes 5G. Al evaluar las medidas de seguridad implementadas en este protocolo, podemos considerar las siguientes contribuciones principales:

a. Uso de blockchain: El protocolo propuesto se basa en la tecnología blockchain, lo que proporciona una serie de ventajas de seguridad, como la integridad y autenticación de los datos, y la distribución de la base de datos en todos los nodos de la red.
b. Técnicas criptográficas: El protocolo utiliza una combinación de firma digital, sellos de tiempo y emparejamiento bilineal para proteger contra varios ataques, como DoS, DDoS, MitM, secuestro y suplantación de identidad.

c. Reducción de la dependencia de la red doméstica (HN): Al no involucrar a la HN en el proceso de autenticación, se mejora su seguridad y se evita la exposición a posibles ataques.
d. Baja sobrecarga de comunicación y computación: El protocolo propuesto utiliza una pequeña cantidad de paquetes y baja potencia computacional, lo que reduce la sobrecarga en la red y ayuda a conservar la batería de los dispositivos de usuario.
e. Integración con la infraestructura existente: No se requieren cambios físicos en la infraestructura actual de la red, lo que facilita la adopción del protocolo propuesto.

El análisis de seguridad realizado en el caso de estudio muestra que el protocolo propuesto es efectivo en la prevención de una variedad de ataques conocidos y en la mejora general de la seguridad en las redes 5G. Además, al abordar las vulnerabilidades existentes en los protocolos de autenticación y acuerdo de clave actuales, el protocolo propuesto proporciona una base sólida para garantizar la confidencialidad, integridad y disponibilidad de los servicios y datos en las redes 5G. En general, las medidas de seguridad implementadas en este caso de estudio son sólidas y ofrecen una solución viable para abordar los desafíos de seguridad en las redes 5G.

- Identificación de las debilidades y fortalezas del caso de estudio en términos de seguridad en redes 5G

  Al analizar el caso de estudio "Autenticación basada en blockchain para redes 5G", podemos identificar las siguientes debilidades y fortalezas:

  Fortalezas:

  a. Uso de la tecnología blockchain: El protocolo propuesto aprovecha las características de seguridad, integridad y autenticación de la tecnología blockchain, lo que mejora significativamente la seguridad en comparación con los enfoques tradicionales.
  b. Resistencia a varios ataques: El esquema propuesto es eficaz para contrarrestar una variedad de ataques, como DoS, DDoS, MitM, secuestro y suplantación de identidad, gracias a las técnicas criptográficas empleadas.
  c. Baja sobrecarga en la red: El protocolo utiliza una cantidad mínima de paquetes y potencia computacional, lo que reduce la sobrecarga de comunicación y computación en la red.

d. Mejora de la seguridad de la red doméstica (HN): Al no involucrar a la HN en el proceso de autenticación, se disminuye su exposición a posibles ataques y se mejora su seguridad.
e. Compatibilidad con la infraestructura existente: El protocolo propuesto no requiere cambios físicos en la infraestructura de la red, facilitando su adopción.

Debilidades:

a. Tiempo de cálculo: Aunque el protocolo propuesto utiliza baja potencia computacional, algunos enfoques criptográficos empleados, como la criptografía de clave pública y la función de derivación de claves, podrían aumentar el tiempo de cálculo en ciertos escenarios.
b. Pérdida de sincronización: Existe el riesgo de discrepancias clave entre el equipo de usuario (UE) y la función del servidor de autenticación (AUSF) debido a la pérdida de sincronización en el proceso de autenticación.
c. Rendimiento en redes de gran escala: El estudio no aborda específicamente cómo el protocolo propuesto se escala en redes 5G de gran envergadura y cómo afecta su rendimiento en estos escenarios.
d. Adopción y compatibilidad: A pesar de que el protocolo propuesto es compatible con la infraestructura existente, la adopción del protocolo puede ser un desafío en términos de compatibilidad con sistemas heredados y la necesidad de coordinación entre diferentes partes interesadas.

El caso de estudio presenta un protocolo prometedor que utiliza la tecnología blockchain para mejorar la seguridad en las redes 5G. Si bien tiene varias fortalezas, también existen algunas debilidades que podrían abordarse en investigaciones futuras para optimizar aún más el protocolo y facilitar su adopción en entornos de red reales.

Propuestas de mejoras

- Identificación de las oportunidades de mejora en el caso de estudio
    a. Mejorar la escalabilidad: A medida que aumenta el número de usuarios y dispositivos conectados a la red 5G, es importante garantizar que el protocolo de autenticación y acuerdo de clave basado en blockchain pueda manejar eficientemente la creciente carga de trabajo. Se puede investigar y desarrollar técnicas y algoritmos que permitan una escalabilidad mejorada, asegurando un rendimiento óptimo incluso en entornos de red altamente congestionados.

b. Reforzar la resistencia a nuevos ataques: Aunque el esquema propuesto en el caso de estudio muestra resistencia a los ataques conocidos, es importante estar preparado para enfrentar nuevos ataques y vulnerabilidades que puedan surgir en el futuro. Se pueden llevar a cabo investigaciones adicionales para identificar posibles brechas de seguridad y desarrollar contramedidas adecuadas.
c. Considerar la privacidad de los usuarios: Si bien el enfoque de autenticación y acuerdo de clave basado en blockchain proporciona seguridad y autenticidad, también es esencial tener en cuenta la privacidad de los usuarios. Se pueden explorar métodos criptográficos y técnicas de anonimización para garantizar que la información personal y los datos sensibles se mantengan protegidos y solo sean accesibles por las entidades autorizadas.
d. Implementar mecanismos de detección y respuesta a incidentes: Además de las medidas preventivas, es importante establecer un sistema de detección de intrusiones y respuesta a incidentes eficiente. Esto ayudará a identificar y mitigar rápidamente cualquier actividad maliciosa o intento de ataque, minimizando así el impacto en la red 5G y sus servicios asociados.
e. Evaluar el impacto de tecnologías emergentes: Dado que el caso de estudio menciona la relevancia de tecnologías como SDN, NFV y computación en la nube en el contexto de la red 5G, es necesario evaluar continuamente el impacto de estas tecnologías en la seguridad general del sistema. Se pueden realizar evaluaciones de riesgos y pruebas de penetración para identificar posibles vulnerabilidades y desarrollar medidas de seguridad adecuadas.

- Propuestas de soluciones y medidas de seguridad para abordar las debilidades y vulnerabilidades identificadas.

  Se pueden proponer las siguientes soluciones y medidas de seguridad:

  a. Optimización del tiempo de cálculo: Investigar y aplicar algoritmos criptográficos más eficientes y optimizados para reducir el tiempo de cálculo sin comprometer la seguridad. También se pueden explorar enfoques híbridos que combinen criptografía de clave pública y simétrica para mantener la seguridad y reducir la complejidad computacional.
  b. Sincronización mejorada: Implementar mecanismos de sincronización más robustos y tolerantes a fallos para evitar discrepancias clave entre el equipo de usuario (UE) y la función del servidor de autenticación (AUSF).

c. Escalabilidad y rendimiento: Realizar pruebas y análisis de rendimiento adicionales en entornos de red de gran envergadura para determinar cómo escala el protocolo propuesto y para identificar posibles cuellos de botella y áreas de mejora.
d. Compatibilidad con sistemas heredados: Desarrollar soluciones de transición y adaptadores que faciliten la integración del protocolo propuesto en entornos de red que utilizan sistemas heredados, asegurando la compatibilidad y coexistencia de diferentes protocolos de autenticación y seguridad.
e. Coordinación entre partes interesadas: Establecer un marco de gobernanza que involucre a las partes interesadas en la adopción del protocolo propuesto, incluidos operadores de redes, fabricantes de equipos y organismos reguladores, para garantizar una implementación y adopción uniformes del protocolo en el ecosistema de redes 5G.
f. Monitoreo y detección de anomalías: Implementar sistemas de monitoreo y detección de anomalías en tiempo real que permitan identificar actividades sospechosas y posibles ataques en la red 5G, proporcionando una respuesta rápida a incidentes de seguridad.
g. Capacitación y concienciación en seguridad: Asegurar que el personal técnico y de seguridad esté adecuadamente capacitado y actualizado en las mejores prácticas y soluciones de seguridad para redes 5G, incluido el protocolo propuesto en el caso de estudio.
h. Actualizaciones y mantenimiento de seguridad: Establecer un proceso sólido para mantener actualizados los sistemas y protocolos de seguridad en la red 5G, abordando posibles vulnerabilidades emergentes y ajustando las medidas de seguridad según sea necesario.

Al aplicar estas soluciones y medidas de seguridad, se podrían abordar las debilidades y vulnerabilidades identificadas en el caso de estudio, mejorando así la seguridad general de las redes 5G que implementan el protocolo de autenticación basado en blockchain propuesto.

Conclusiones

- Resumen de los principales hallazgos

La aplicación de la tecnología blockchain puede mejorar significativamente la seguridad y la eficacia del proceso de autenticación en las redes 5G.

El caso de estudio presenta un protocolo de autenticación y acuerdo de clave basado en blockchain para redes 5G, con el objetivo de mejorar la seguridad en diversas aplicaciones, como salud, banca y educación. Los principales hallazgos del análisis del caso de estudio son:

a. El protocolo propuesto utiliza blockchain para aprovechar sus propiedades de seguridad, como integridad y autenticación, además de la distribución de la base de datos. Esto ayuda a mejorar la seguridad general y la resistencia a ataques en comparación con protocolos de autenticación tradicionales.
b. Se implementan técnicas criptográficas avanzadas, como firma digital, sellos de tiempo y emparejamiento bilineal, para contrarrestar varios ataques, como denegación de servicio (DoS), DoS distribuido (DDoS), hombre en el medio (MitM), secuestro y suplantación de identidad.
c. El protocolo propuesto no requiere la intervención de la red doméstica (HN) en el proceso de autenticación, lo que aumenta la seguridad de la HN y reduce la sobrecarga de comunicación y computación.
d. El análisis de seguridad demuestra que el esquema propuesto es seguro y resiste los ataques conocidos, ofreciendo una mejor protección en comparación con soluciones anteriores.
e. A pesar de las fortalezas del protocolo propuesto, se identificaron algunas debilidades y vulnerabilidades, como el tiempo de cálculo, problemas de sincronización y escalabilidad.
f. Se propusieron varias soluciones y medidas de seguridad para abordar estas debilidades, como optimizar el tiempo de cálculo, mejorar la sincronización, realizar pruebas y análisis adicionales, garantizar la compatibilidad con sistemas heredados, coordinar entre partes interesadas, monitorear y detectar anomalías, capacitar al personal y mantener actualizaciones de seguridad.
g. La evaluación de la viabilidad y eficacia de estas propuestas de mejora indica que su implementación puede mejorar significativamente la seguridad de las redes 5G que utilizan el protocolo de autenticación basado en blockchain propuesto, aunque es crucial equilibrar cuidadosamente los costos, recursos y esfuerzos necesarios con los beneficios de seguridad adicionales.

El caso de estudio presenta un protocolo de autenticación y acuerdo de clave basado en blockchain para redes 5G que muestra una mejora significativa en la seguridad en comparación con los protocolos existentes. Aunque hay debilidades y vulnerabilidades identificadas, las

propuestas de mejora pueden abordar estos problemas y fortalecer aún más la seguridad en las redes 5G.

- Reflexiones finales

La autenticación basada en blockchain puede ser una solución efectiva para mejorar la seguridad de las redes 5G, y se deben seguir investigando y mejorando estas técnicas para abordar los desafíos de seguridad en las redes 5G.

El caso de estudio sobre un protocolo de autenticación y acuerdo de clave basado en blockchain para redes 5G proporciona valiosas ideas sobre cómo mejorar la seguridad en aplicaciones de diversas áreas como salud, banca y educación. A través del análisis del caso, se pueden extraer las siguientes reflexiones y conclusiones finales:

a. La implementación de blockchain en el protocolo de autenticación y acuerdo de clave ofrece ventajas significativas en términos de seguridad, integridad y autenticación. La descentralización y la inmutabilidad de la cadena de bloques pueden ayudar a proteger los sistemas de red 5G de diversos ataques y amenazas.
b. La combinación de técnicas criptográficas avanzadas, como firma digital, sellos de tiempo y emparejamiento bilineal, contribuye a la efectividad del esquema propuesto en la resistencia contra ataques como DoS, DDoS, MitM, secuestro y suplantación de identidad.
c. A pesar de las mejoras en la seguridad, el protocolo propuesto presenta debilidades y vulnerabilidades, como el tiempo de cálculo, problemas de sincronización y escalabilidad. Estas debilidades deben abordarse mediante soluciones y medidas de seguridad apropiadas para garantizar una protección óptima.
d. Las propuestas de mejora, como la optimización del tiempo de cálculo, la mejora de la sincronización, la realización de pruebas y análisis adicionales y la capacitación del personal, pueden mejorar aún más la seguridad y la eficacia del protocolo propuesto. Sin embargo, es fundamental equilibrar los costos, recursos y esfuerzos requeridos con los beneficios adicionales de seguridad.
e. El caso de estudio destaca la importancia de la colaboración entre investigadores, profesionales y partes interesadas en el desarrollo e implementación de soluciones de seguridad innovadoras y efectivas para las redes 5G y más allá.

El protocolo de autenticación y acuerdo de clave basado en blockchain presentado en este caso de estudio tiene el potencial de mejorar significativamente la seguridad de las redes

5G en diversas aplicaciones. Aunque existen debilidades y vulnerabilidades, las propuestas de mejora pueden abordar estos problemas y proporcionar una mayor protección. Este caso de estudio subraya la necesidad de continuar investigando e innovando en el campo de la seguridad de las redes 5G para garantizar que la tecnología emergente se implemente de manera segura y eficiente en nuestra vida cotidiana.

7. Discusión

El análisis exhaustivo de la seguridad en redes 5G realizado en los casos de estudio ha permitido identificar las vulnerabilidades y riesgos asociados con esta tecnología. Estos hallazgos respaldan el objetivo general de fortalecer la seguridad de la red y proteger la privacidad de los usuarios.

En primer lugar, se analizaron las vulnerabilidades y riesgos específicos de la tecnología 5G en comparación con las redes anteriores. Esto proporcionó una comprensión más profunda de los desafíos de seguridad que deben abordarse, como la necesidad de proteger la integridad de los datos y la confidencialidad de la información transmitida. Además, se identificaron áreas críticas, como la autenticación y la protección de la privacidad, donde se requieren mejoras significativas.

Con base en este análisis, se evaluaron las medidas de seguridad existentes en la capa de aplicación de la red 5G. Esto incluyó aspectos como la autenticación de usuarios, la gestión de la seguridad y la protección de la privacidad. Estas evaluaciones permitieron identificar las deficiencias y las áreas donde se requieren mejoras para fortalecer la seguridad de la red.

Como resultado, se propuso una amplia gama de mejoras en la seguridad de la red 5G. Estas propuestas abarcan aspectos como arquitecturas de seguridad definidas por software, políticas de seguridad virtualizadas, esquemas de autenticación eficientes y seguros, y la aplicación de tecnología blockchain. Estas mejoras tienen como objetivo garantizar la seguridad y privacidad de los usuarios, así como mantener la integridad de la red en el futuro.

En conclusión, el análisis de seguridad en redes 5G y las propuestas de mejora presentadas cumplen con los objetivos planteados. Se han identificado las vulnerabilidades y riesgos asociados con la tecnología 5G, se han evaluado las medidas de seguridad existentes y se han propuesto mejoras integrales para fortalecer la seguridad de la red. Estas mejoras son fundamentales para proteger la privacidad de los usuarios y mantener la confianza en el entorno de las redes 5G en constante evolución.

8. Conclusiones

Los avances en las tecnologías de redes 5G han abierto nuevas oportunidades y desafíos en términos de seguridad. En respuesta a estos desafíos, se han propuesto arquitecturas y esquemas de seguridad innovadores que abordan aspectos como la flexibilidad, la privacidad, la eficiencia y la confianza en entornos de red altamente dinámicos.

El análisis de seguridad de las redes 5G realizado en los estudios presentados revela la importancia de abordar los desafíos específicos que estas redes enfrentan en términos de confidencialidad, integridad y disponibilidad de datos. Las arquitecturas de seguridad definidas por software (SDN), las políticas de seguridad virtualizadas, los esquemas de autenticación eficientes y seguros, y la utilización de la tecnología blockchain se destacan como soluciones prometedoras. Estas propuestas ofrecen flexibilidad, autonomía y una capa adicional de confianza para proteger las redes 5G y los datos que circulan en ellas. Sin embargo, se requiere un enfoque continuo de mejora, colaboración y pruebas exhaustivas para garantizar que estas soluciones sean efectivas en entornos reales y puedan adaptarse a las amenazas emergentes. Además, es esencial abordar los desafíos de escalabilidad, rendimiento y compatibilidad con los estándares existentes para lograr una implementación exitosa de las mejoras propuestas.

El análisis de seguridad de las redes 5G destaca la necesidad de implementar arquitecturas y esquemas de seguridad adecuados para abordar los desafíos específicos de estas redes. Las propuestas presentadas ofrecen soluciones prometedoras, pero se requiere una investigación continua y pruebas exhaustivas para garantizar su efectividad. Además, la colaboración con expertos en seguridad y la adaptación a los estándares existentes son fundamentales para lograr mejoras significativas en la seguridad de las redes 5G. En última instancia, el análisis de seguridad y las propuestas de mejora subrayan la importancia de proteger la integridad y confidencialidad de los datos en las redes 5G en evolución constante.

Estos casos de estudios demuestran la necesidad de contar con arquitecturas y esquemas de seguridad innovadores para abordar los desafíos de seguridad en las redes 5G habilitadas para SDN/NFV. Estos enfoques garantizan la flexibilidad, la privacidad, la eficiencia y la confianza necesarias en entornos de red dinámicos y altamente conectados.

9. Recomendaciones

Basándonos en los casos estudio presentados, se puede proporcionar las siguientes recomendaciones

a. Recomendaciones para una arquitectura de seguridad definida por software para redes 5G basada en SDN:
   - Continuar mejorando la arquitectura para garantizar la seguridad de los equipos en las SDMN.
   - Realizar pruebas exhaustivas de la arquitectura propuesta en entornos reales para validar su eficacia y funcionalidad.
   - Colaborar con proveedores y expertos en seguridad para asegurar la implementación adecuada de la arquitectura y mantenerla actualizada frente a las amenazas emergentes.
b. Recomendaciones para una arquitectura de seguridad virtualizada basada en políticas para redes de acceso 5G habilitadas para SDN/NFV:
   - Realizar una evaluación exhaustiva de los desafíos de seguridad específicos de las redes de acceso 5G y adaptar la arquitectura propuesta en consecuencia.
   - Asegurarse de que la arquitectura de seguridad sea compatible con los estándares y esfuerzos de virtualización de red en curso.
   - Investigar y aprovechar las tecnologías NFV/SDN para lograr la automatización y el aprovisionamiento rápido de seguridad como servicio.
c. Recomendaciones para un esquema de autenticación de preservación de la privacidad seguro y eficiente para redes vehiculares definidas por software 5G:
   - Continuar investigando y desarrollando el esquema propuesto para mejorar el rendimiento de la red, incluida la determinación del tiempo de validación de SPID y la tasa de actualización de la lista hash.
   - Realizar pruebas en entornos reales con alta densidad de vehículos para validar el rendimiento y la seguridad del esquema propuesto.
   - Colaborar con los fabricantes de vehículos y las autoridades de regulación para garantizar la implementación adecuada del esquema de autenticación en los vehículos conectados.
d. Recomendaciones para la autenticación basada en blockchain para redes 5G:

- Investigar y abordar los posibles desafíos de escalabilidad y rendimiento asociados con la implementación de la tecnología blockchain en redes 5G.
- Colaborar con expertos en blockchain para garantizar la seguridad de la cadena de bloques y su resistencia a los ataques de suplantación de identidad.
- Realizar pruebas y evaluaciones de seguridad exhaustivas para verificar la efectividad y la resistencia del esquema propuesto ante diversos escenarios y ataques.

10. Bibliográficas

3GPP – The Mobile Broadband Standard. (s. f.). 3GPP. Recuperado 20 de junio de 2023, de https://www.3gpp.org/

Castillo, V. A. F., Calle, J. E. C., Pin, J. X. B., & Parrales, C. A. V. (2022). 5G tecnología inalámbrica que cambiará el mundo por completo. *UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166*, *6*(3), 39-48. https://doi.org/10.47230/unesum-ciencias.v6.n3.2022.393

Dahmen-Lhuissier, S. (s. f.). *5G*. ETSI. Recuperado 2 de mayo de 2023, de https://www.etsi.org/technologies/5g

ETSI - Welcome to the World of Standards! (s. f.). Recuperado 20 de junio de 2023, de https://www.etsi.org/

Gao, Y., Hu, S., Tang, W., Sun, Y., Huang, D., Cheng, S., & Li, X. (2018). *Physical layer security in 5G based large scale social networks: Opportunities and challenges*. *6*, 26350-26357.

Haddad, Z., Fouda, M. M., Mahmoud, M., & Abdallah, M. (2020). Blockchain-based Authentication for 5G Networks. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 189-194. https://doi.org/10.1109/ICIoT48696.2020.9089507

Harris, S., & Maymi, F. (2016). *CISSP Exam Guide* (Tercera). McGraw-Hill Education.

Huang, J., Qian, Y., & Hu, R. Q. (2020). Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks. *IEEE Transactions on Vehicular Technology*, *69*(8), 8542-8554. https://doi.org/10.1109/TVT.2020.2996574

IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. (s. f.). Recuperado 20 de junio de 2023, de https://www.ieee.org/

Jiménez, A. C. (2020). *Descubriendo los desafíos técnicos para la seguridad en las redes 5G*.

Liang, X., & Qiu, X. (2016). A software defined security architecture for SDN-based 5G network. *2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, 17-21. https://doi.org/10.1109/ICNIDC.2016.7974528

Montesinos Chano, R. J. (2018). *Estudio Y Análisis De Tecnologías Habilitadoras 5G Y Sus Factibilidades Para El Desarrollo Del Internet De Las Cosas.* [UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL]. http://repositorio.ucsg.edu.ec/bitstream/3317/11343/1/T-UCSG-PRE-TEC-ITEL-315.pdf

Pasquali, M. (2022, julio 27). *Infografía: El despliegue de la 5G en el mundo*. Statista Infografías. https://es.statista.com/grafico/23241/nivel-de-desarrollo-de-la-tecnologia-5g-en-el-mundo

¿Qué es 5G? (s. f.). Cisco. Recuperado 28 de abril de 2023, de https://www.cisco.com/c/es_mx/solutions/what-is-5g.html

¿Qué es la arquitectura de red 5G? (s. f.). Recuperado 28 de abril de 2023, de https://es.digi.com/blog/post/5g-network-architecture

Siddiqui, M. S., Escalona, E., Trouva, E., Kourtis, M. A., Kritharidis, D., Katsaros, K., Spirou, S., Canales, C., & Lorenzo, M. (2016). Policy based virtualised security architecture for SDN/NFV enabled 5G access networks. *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 44-49. https://doi.org/10.1109/NFV-SDN.2016.7919474

Tecnología 5G, Características, usos y posibles peligros. (2020, octubre 30). *Grupo Atico34*. https://protecciondatos-lopd.com/empresas/tecnologia-5g/

11. Anexos

Anexo 1. Certificado de traducción del resumen

Mg. Yanina Quizhpe Espinoza
Licenciada en Ciencias de Educación mención Inglés
Magister en Traducción y mediación cultural

Celular: 0989805087
Email: yaniqes@icloud.com
Loja, Ecuador 110104

Loja, 15 de junio de 2023

Yo, Lic. Yanina Quizhpe Espinoza, con cédula de identidad 1104337553, docente del Instituto de Idiomas de la Universidad Nacional de Loja, y certificada como traductora e interprete en la Senescyt y en el Ministerio de trabajo del Ecuador con registro **MDT-3104-CCL-252640**, certifico:

Que tengo el conocimiento y dominio de los idiomas español e inglés y que la traducción del resumen del trabajo de titulación **Análisis de la seguridad en redes 5G y propuesta de mejoras**, cuya autoría del ingeniero Bolívar Rolando Quizhpe Vásquez, con cédula 1104607120, es verdadero y correcto a mi mejor saber y entender.

Atentamente

YANINA BELEN QUIZHPE ESPINOZA
Firmado digitalmente por YANINA BELEN QUIZHPE ESPINOZA
Fecha: 2023.06.15 10:59:42 -05'00'

Yanina Quizhpe Espinoza.
Traductora freelance