# Desafíos de Seguridad en Redes 5G

*Carlos González*

*Universidad Autónoma de Chiriquí Vicerrectoría de Investigación y Posgrados David, Panamá*

*carlos.gonzalez5@unachi.ac.pa*

**Abstract— Las redes de comunicaciones móviles conectan a gran parte de la población mundial. La seguridad de la transferencia de la información, los mensajes y los datos de los usuarios dependen de las garantías proporcionadas por protocolos de autenticación y técnicas de cifrado. En la quinta generación (5G) de red se deben desarrollar nuevos protocolos para garantizar la integridad, privacidad y la consistencia de los datos. Este documento presenta un estudio exhaustivo sobre las características y desafíos de seguridad de los sistemas de redes inalámbricas 5G. En cada caso de vulnerabilidades descritas se recomiendan posibles soluciones vis-a-vis a los ataques y a las debilidades encontradas. Basado en nuestro trabajo de investigación sobre una nueva arquitectura para el Internet de las Cosas (IoT) [1], en este documento se describen los principales desafíos y amenazas potenciales en las redes 5G..**

***Keywords— Seguridad en Redes 5G, Redes de comunicación móvil, Protocolos 5G.***

## I. INTRODUCCIÓN

La administración de redes tradicionales se ha convertido en un desafío dado el volumen de datos y sistemas propietarios. Ya sea para crear nuevos servicios individualmente, o bien crear la interconexión de centros de datos se requiere de un sin número de operaciones sucesivas duplicando el trabajo a realizar. El problema básico se debe a la restricción de la red que se establece entre la Interfaz de Programación de Aplicaciones (API) de norte a sur; pues es ahí donde se implementan un número infinito de protocolos distribuidos y el uso de interfaces cerradas. El proceso resulta difícil tanto para el operador de la red o incluso para el vendedor al gestionar y personalizar la configuración personalizadas de acuerdo con las normas emergentes, por lo tanto, susceptibles a errores. Las redes tradicionales presentan problemas de seguridad, programabilidad y adaptabilidad que han sido evaluados en diversos trabajos de investigación.

La nueva generación de sistemas de telecomunicaciones móviles está basada en un sistema inalámbrico de Quinta Generación (5G). La tecnología 5G no es solo una próxima versión mejorada, o el avance de los actuales sistemas 4G; es mucho más que los sistemas conocidos hasta hoy. La tecnología 5G liberará nuevas capacidades de servicio sobre demanda y enfrentará desafíos de implementación en todo el mundo. La demanda de todas las redes celulares hasta el año 2020 está estimada en 50 billones de dispositivos conectados;

*1Agradecimiento a la Secretaría Nacional de Ciencia y Tecnología e Innovación (SENACYT) por financiar la investigación a través del programa del Sistema Nacional de Investigación SNI.*

esto genera un enorme aumento del tráfico de datos, en comparación con el escenario actual [2]. La red celular (4G) no será capaz de soportar estos requerimientos, por lo que hay una necesidad de emigrar hacia un nuevo sistema de comunicaciones móviles. El enfoque de estudio por parte de los investigadores se ha centrado más en la capacidad para la transmisión de datos de los dispositivos de red 4G, así como nuevos servicios Comunicación Dispositivo a Dispositivo (D2D), masiva Múltiple-Entrada Múltiple-Salida (mMIMO) y manejo de grandes volúmenes de flujo de datos [3]. Más allá de la capacidad para proporcionar la conectividad, la compatibilidad y la escalabilidad a miles de millones de dispositivos, la 5G debe contar con estrictas restricciones de seguridad, que evolucionen al ritmo de su desarrollo [4].

Algunas características avanzadas de la red 5G contemplan:

a.Conexiones de 1-10Gbps

b.1 millón de dispositivos conectados por Km2

c.Alta disponibilidad

d. Reduce el consumo de energía de los equipos de red

e. Promete una mayor duración de la batería aproximadamente 10 años para los dispositivos con menor consumo [5].

En comparación con el estándar 4G LPWA el cual solo soporta 60,680 dispositivos con el rango de cobertura, muy lejos de la conectividad que la 5G puede ofrecer. Para lograr la conectividad 5G se necesita una combinación de otras tecnologías tales como Redes Heterogéneas (HetNet) [6], mMIMO [7], onda milimétrica (mm- wave), comunicaciones D2D [8] y M2M [9]. Sin embargo, la red 5G no solo proporcionará servicios convencionales de datos y voz. También puede soportar casos de comunicación de vehículo a vehículo, asistencia médica, ciudades inteligentes, automatización de la industria, agricultura inteligente, entre otros [10].

## II. CARACTERÍSTICAS DE LA 5G

Los teléfonos inteligentes son definitivamente un actor importante en la comunicación móvil. Sin embargo, no son el único enfoque de la 5G dada la ubicuidad y la baja latencia, también se pueden incluir dispositivos con recursos limitados de la red. Un componente clave son las conexiones ultra rápidas con mínimos retardos en la comunicación. La transmisión de datos, vídeos, realidad aumentada y juegos en línea entre dispositivos móviles con un flujo de datos completamente trasparente hacia los usuarios finales.

De igual forma que otros métodos de comunicación, inalámbrica, la 5G envía y recibe datos en un espectro radio. Sin embargo, a diferencia de la 4G, la 5G utiliza frecuencias más altas, esto a través de ondas milimétricas, en el espectro de radio con ello facilita velocidades ultra rápidas. El espectro de radio de la tecnología 5G debe estar por encima de los 6 GHz, para alcanzar un ancho de banda móvil a gran velocidad de transmisión de datos.

| Tipo de Tecnología | Velocidad de Descarga |
|---|---|
| 3G | 1 hora, 8 minutos |
| 4G | 40 minutos |
| 4G LTE | 27 minutos |
| 5G | 35 segundos |

Tabla 1: Velocidad de tranferencia de datos por teconología

La tabla I muestra el tiempo de descarga de aproximado de una película de 3 GB de tamaño, utilizando diferentes tipos de redes celulares, sin contemplar ningún tipo de latencia en el proceso.

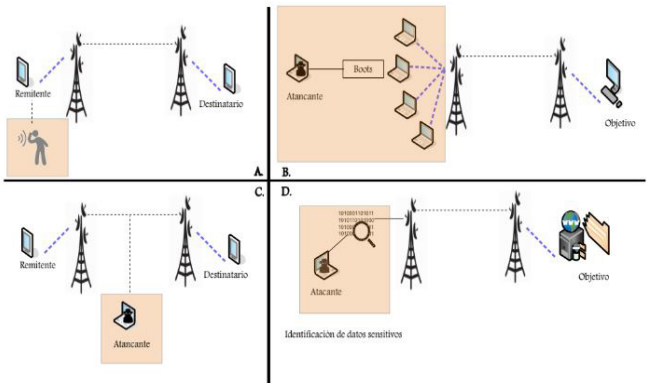
## III. ASPECTOS DE SEGURIDAD

El implementar nuevas tecnologías conlleva a desarrollar modelos de arquitectura de red en entornos de prueba; los cuales atraen amenazas de seguridad y la necesidad de resolverlos. Aunque generalmente la red 5G es considerada una evolución tecnológica, en tanto incrementa la capacidad y cobertura, aun no es más segura que la red 4G. Dada la velocidad, y el soporte creciente de las aplicaciones podrían generarse nuevas brechas de seguridad, tanto a nivel de los proveedores de servicios, como de los usuarios finales.

Con una mayor velocidad de datos, la red 5G puede ser objeto de ataques de Denegación de Servicio Distribuido (DDoS) más fuertes y precisos [11]. Con el desarrollo de nuevos tipos de servicios para dar soporte a una gran cantidad de usuarios y dispositivos conectados, aumenta el rango de posibles ataques. Una nueva generación de tecnologías emergentes se convierte en un blanco atractivo para los atacantes en cuanto a inventar nuevas formas de ingresar y manipular las redes. En el contexto de las redes 5G se producen nuevos retos de privacidad y protección de datos. La transmisión de datos a través de las comunicaciones inalámbricas utiliza ancho de banda limitado, eso impide proporcionar algunas características de seguridad como autenticación de dispositivos, la integridad de datos y confidencialidad de la información. En la actualidad, las redes celulares presentan algunos problemas de seguridad a nivel de la capa de control de acceso a los medios (MAC) y de la capa física (PHY) vulnerabilidades y problemas de privacidad [12]. Con la evolución de la tecnología, cada año se producen ataques cada vez más sofisticados, los cuales demandan mejores controles de seguridad. A continuación, se describen una serie de posibles ataques en las redes 5G.Interceptación del tráfico de datos: Es un tipo de ataque pasivo donde el tráfico de datos y la comunicación entre dispositivos no se interrumpen. En este ataque, el atacante intercepta la comunicación de dos usuarios sin el conocimiento o consentimiento de las víctimas. Al ser un ataque pasivo pasa desapercibido en el entorno de red. La interceptación puede llevarse a cabo con programas de software especiales llamados sniffers para obtener y registrar los datos que circulan por la red. Para grabar las llamadas de voz sobre IP (VoIP) de programas de como Skype, Discord u otros; también pueden interceptar con analizadores de protocolo y luego convertirlas en audio. Si la información esta encriptada, se analiza el flujo de datos con herramientas especializadas que intentan descifrar el código.

**Solución:** El primer paso para proteger los datos transmitidos a través de la red 5G es utilizar técnicas de cifrados. Las posibilidades de acceso no autorizado a los datos pueden minimizarse si los datos están cifrados, pues el atacante no puede interceptarlo fácilmente. Por ejemplo, con una clave

criptográfica especial para acceder a la información, así como con las herramientas adecuadas para cifrar los datos,. Gracias a la alta velocidad de la red 5G se pueden implementar técnicas de cifrado de tipo seguridad de capa física (PLS) para evitar la interceptación del tráfico de datos [13].




DoS y DDoS: Los ataques de Denegación de Servicios y Denegación Distribuida de Servicios son muy utilizados actualmente para vulnerar y rechazar el acceso a algunos recursos de la red utilizando peticiones masivas al servidor. Este tipo de ataque es activo, pues afecta a la disponibilidad de la red. El DDoS se realiza por un grupo de nodos infectados con un virus, para hacer uso de los recursos del hardware y lanzar el ataque desde diversos sitios del mundo. La Red Inalámbrica 5G al tener una mayor densidad de dispositivos conectados, haría que estos tipos de ataques pueden afectar varias capas de comunicación hasta convertirse en una seria amenaza para los sistemas de comunicaciones y operadores de red.

**Solución:** La autenticación será uno de los servicios de seguridad más importantes a implementar en redes inalámbricas de nueva generación 5G. Dada la naturaleza de la 5G, para lograr una autenticación rápida, las propias Redes Definidas por Software (SDN) son las mejores herramientas con una alta flexibilidad y programabilidad son [4].

MITM: El ataque de intermediario toma control del canal de comunicación entre usuarios finales, así es tomada por el atacante. El atacante puede reemplazar, modificar, o cambiar totalmente el mensaje entre dispositivos. Este tipo de ataque activo compromete la confidencialidad e la integridad de los datos. En una red celular 5G, se pueden crear falsas estaciones bases fundado en un ataque MITM en donde el atacante fuerza a un usuario a autenticarse en su sistema ficticio, y así obtener toda la información.

**Solución:** Con una autenticación mutua entre el dispositivo móvil y la estación base, normalmente se puede evitar un ataque de tipo MITM. Los protocolos 5G AKA y EAP-AKA son una solución emergente para registrar las solicitudes de conexión y luego iniciar el proceso de autenticación en redes 5G [14].

Vulnerabilidades en las API: La Interfaz de Programación de Aplicaciones es responsable de transferir la información entre sistemas y el medio de comunicación entre aplicaciones. En algunos casos la información sensible y datos confidenciales se transfieren a través de las API. Las APIs de código abierto a menudo se documenta la información sobre su implementación y estructura interna. Esta información puede ser utilizada para realizar un ataque cibernético. Algunas

vulnerabilidades adicionales, como la autenticación débil, la falta de cifrado, y dispositivos finales inseguros hacen que el nivel de riesgo de ataque sobre las APIs aumente. **Solución:** En redes a gran escala como la 5G, los métodos tradicionales de seguridad no son suficientes para soportar una enorme carga de red, con ellos proporcionan elasticidad de aprovisionamiento y desaprovisionamiento de recursos de elementos conectados de manera autónoma. La virtualización distribuida de AAA (V- AAA) en combinación con dos sistemas de normas internacionales independientes (3GPP y ETSI), permite una gestión flexible y elástica en múltiples puntos de acceso [15].

La red celular 5G facilita las comunicaciones de dispositivos IoT, y una diversidad de equipos industriales. Actualmente, se están desarrollando nuevas arquitecturas para administrar la generación masiva de información y la automatización del flujo de datos. La tecnología más prometedora es la virtualización de redes, a través de SDN y NFV. Sin embargo, como toda tecnología en desarrollo los riesgos de seguridad al implementarse el SDN/ NFV también puede crecer dada la posición centralizada del controlador, y las funciones de administración.

Uno de los ataques más recientes utilizado en redes celulares que podría afectar a la red 5G es Rastreo Mediante Mensaje de Paginación y Distribución (ToRPEDO). Mediante este ataque se puede desde rastrear dispositivos móviles, interceptar las comunicaciones o incluso falsificar los mensajes. La vulnerabilidad reside en los protocolos de paginación celular al realizar la difusión masiva paquetes de datos.

## IV. CONCLUSIÓN

La nueva generación de la red 5G permite el desarrollo de nuevas aplicaciones y proporciona mejoras notables con respecto a las anteriores tecnologías de redes celulares. Según estudios recientes de redes 5G, se presentan los beneficios y vulnerabilidades para esta tecnología, aun en desarrollo. Algunos de los grandes retos de la 5G son la disponibilidad, la autenticación, la confidencialidad e integridad de datos, dada la naturaleza de la tecnología. Algunos riesgos de seguridad se deben a la heterogeneidad de aplicaciones IoT, D2D y protocolos de transferencia de la información. El avance de la tecnología conduce a nuevos requisitos de seguridad y estudios a realizar para hacer frente tanto a ataques ya conocidos, como a los aún por conocer.

Los mecanismos para mitigar los ataques de seguridad en redes 5G deben ser diseñados e implementados en un entorno de desarrollo constante. Con el objetivo de proteger un ambiente 5G, la virtualización de red y controladores de tipo SDN pueden ser utilizados con una combinación de protocolos para facilitar la gestión de grandes flujos de datos. Aún existen varias dudas sobre la implementación real de esta tecnología. Sin embargo, este estudio permite la comprensión de las terminologías y proporciona detalles de los riesgos de seguridad de la red 5G.

## V. REFERENCIAS

[1] F. Olivier, G. Carlos, and N. Florent, "New security architecture for iot network," Procedia Computer Science, vol. 52, pp. 1028 – 1033, 2015. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015).

[2] T. Barnett, S. Jain, U. Andra, and T. Khurana, "Cisco visual networking index (vni) complete forecast update, 2017–2022," 2018.

[3] P. Iovanna and F. Ubaldi, "Sdn solutions for 5g transport networks," in 2015 International Conference on Photonics in Switching (PS), pp. 297–299, Sep. 2015.

[4] M. A. Hasnat, S. T. A. Rumee, M. A. Razzaque, and M. Mamun-Or-Rashid, "Security study of 5g heterogeneous network: Current solutions, limitations future direction," in 2019 International Conference on Elec- trical, Computer and Communication Engineering (ECCE), pp. 1–4, Feb 2019.

[5] I.-G. P. GROUP, "5g network technology architecture white paper," May 2015.

[6] H. Ramazanali, A. Mesodiakaki, A. Vinel, and C. Verikoukis, "Survey of user association in 5g hetnets," in 2016 8th IEEE Latin-American Conference on Communications (LATINCOM), pp. 1–6, Nov 2016.

[7] M. Zahid, S. Shoaib, and M. Rizwan, "Design of mimo antenna system for 5g indoor wireless terminals," in 2019 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1–4, Feb 2019.

[8] R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. J. P. C. Rodrigues, "5g d2d networks: Techniques, challenges, and future prospects," IEEE Systems Journal, vol. 12, pp. 3970–3984, Dec 2018.

[9] M. Naeem, W. Ejaz, L. Karim, S. H. Ahmed, A. Anpalagan, M. Jo, and H. Song, "Distributed gateway selection for m2m communication in cognitive 5g networks," IEEE Network, vol. 31, pp. 94–100, November 2017.

[10] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A survey on iot and 5g network," in 2018 International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–3, Jan 2018.

[11] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate ddos attacks on 5g core network slices," CoRR, vol. abs/1901.01443, 2019.

[12] Y. M. Amin and A. T. Abdel-Hamid, "A comprehensive taxonomy and analysis of ieee 802.15.4 attacks," Journal of Electrical and Computer Engineering, vol. 2016, pp. 1–12, 2016.

[13] L. Sun and Q. Du, "Physical layer security with its applications in 5g networks: A review," China Communications, vol. 14, pp. 1–14, December 2017.

[14] D. A. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sas- se, and V. Stettler, "Formal analysis of 5g authentication," CoRR, vol. abs/1806.10360, 2018.

[15] S. Wong, N. Sastry, O. Holland, V. Friderikos, M. Dohler, and H. Agh- vami, "Virtualized authentication, authorization and accounting (v-aaa) in 5g networks," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 175–180, Sep. 2017.