ARI 140/2020
9 de diciembre de 2020

Descubriendo los desafíos técnicos para la seguridad en las redes 5G

Antonio Casquero Jiménez | Departamento de Señales, Sistemas y Radiocomunicaciones, Universidad Politécnica de Madrid

Jorge Pérez Martínez | Catedrático en la UPM y coordinador del Foro de Gobernanza de Internet | @Jorgeperezmarti

Pilar Rodríguez Pita | Departamento de Señales, Sistemas y Radiocomunicaciones, Universidad Politécnica de Madrid

Tema

La seguridad en las redes 5G es un tema muy complejo desde el punto de vista técnico. Incluye necesariamente múltiples conceptos y siglas de difícil comprensión para los analistas de otras disciplinas, aunque es fundamental que éstos entiendan lo mejor posible las claves técnicas que rodean a estas nuevas tecnologías.

Resumen

Un aspecto fundamental en la prestación de servicios de telecomunicaciones es la seguridad, pues la protección de la red frente a amenazas, además de la integridad y la garantía de la privacidad de los datos que transporta, se plantean como aspectos imprescindibles para poder ofrecer servicios fiables. Estos elementos se acentúan aún más en las redes móviles de quinta generación (*5th generation mobile networks*) o redes 5G, orientadas a la prestación de servicios muy variados con requisitos muy dispares; algunos de ellos, como los relacionados con la salud, tratan con datos e información muy confidencial. En este ARI presentamos los principales riesgos y desafíos asociados a la seguridad de las redes 5G, así como las principales medidas que se adoptan para superarlos.

Análisis

El 5G se ha posicionado, junto con la inteligencia artificial, como uno de los habilitadores digitales más importantes que facilitarán la disrupción digital. Las ventajas que ofrece el 5G no se limitan a bajas latencias y a lidiar con grandes cargas de tráfico, sino que, mediante la innovación y la colaboración entre los proveedores de servicios, se podrán conseguir nuevos servicios que generarán ganancias económicas extraordinarias. En primer lugar, el mercado de consumidores ya genera a los proveedores la mayor parte de los ingresos por servicios inalámbricos y se espera que continúe creciendo según aumenta la importancia del 5G. Recientemente, Ericsson ha calculado que estos proveedores podrían obtener para 2030 un acumulado de 3,7 billones de dólares

estadounidenses a partir de los ingresos de los consumidores de 5G[1]. Además, los proveedores podrán generar directamente 131 billones de dólares de los servicios digitales si realizan un desarrollo y *marketing* proactivos de los servicios 5G, como la realidad aumentada, la conectividad de los coches o vídeos mejorados[2]. No obstante, el mayor valor será generado por la industria 4.0 y otros sectores verticales, como la educación, la sanidad, el transporte, etc. Solo en aplicaciones del internet de las cosas (*Internet of Things*, IoT), el GSMA calcula que se generarán 900 billones de dólares en 2025[3]. Estas expectativas dependen de la capacidad técnica de hacer sistemas seguros y fiables en un entorno de creciente apertura de las redes a múltiples agentes.

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

Las redes 5G presentan una serie de características y mejoras técnicas que las hacen muy superiores a otras generaciones previas de redes móviles. Sin embargo, distintos agentes tecnológicos y entidades europeas, como la Comisión Europea, la Agencia Europea de Ciberseguridad (ENISA) o el Grupo de Cooperación NIS, han señalado un incremento significativo de los riesgos de seguridad en las redes 5G respecto a otras generaciones de redes móviles. Estos riesgos guardan especial relación con la disponibilidad, integridad, privacidad, confidencialidad y accesibilidad de las redes. Además, se han identificado como aspectos cruciales los asociados a la multiplicación de suministradores y operadores en las cadenas de suministro o a la inseguridad del suministro debido a la dependencia de un único proveedor.

Por otro lado, destacamos que los principales actores que están detrás de estos riesgos serán, en su mayoría, actores accidentales, internos o *hackers* individuales. No obstante, como posibles amenazas destacan también la posible presencia de grupos hacktivistas, terroristas o criminales y los actores respaldados por agentes estatales, estos últimos especialmente peligrosos para la confidencialidad, disponibilidad e integridad de las redes 5G. A continuación, analizamos los principales riesgos, desde un punto de vista tecnológico, que presentan las redes 5G.

Nuevos modelos de negocio con medidas de seguridad insuficientes

Las redes 5G serán el ecosistema de desarrollo de múltiples servicios ofrecidos por distintas industrias y agentes. Con el fin de optimizar la prestación de dichos servicios, surgen las *network slices*, redes lógicas dinámicas de extremo a extremo (*end to end*, E2E) que proporcionan unas características y capacidades de red específicas que permiten la coexistencia de múltiples servicios con requisitos muy dispares bajo una misma infraestructura física de red. En este contexto, destaca el concepto de "red como servicio" –conocido en inglés como NaaS (*network as a service*)–, en el que estas redes virtuales, adaptadas a unos requisitos concretos, se ofrecen bajo demanda a terceros,

[1] Ericsson, "Ericsson estimates USD 31 trillion 5G consumer market by 2030", 17/11/2020, https://www.ericsson.com/en/press-releases/2020/11/ericsson-estimates-usd-31-trillion-5g-consumer-market-by-2030.

[2] Ericsson, "Harnessing the 5G consumer potential", 2020, https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/harnessing-the-5g-consumer-potential.

[3] GSM Association, "4th Global Mobile IoT Summit", https://www.gsma.com/iot/4th-global-mobile-iot-summit-video-1.

lo que permite la creación de nuevos casos de uso y la aparición de modelos de negocio innovadores. Sin embargo, la gestión de la seguridad en estas redes lógicas es una tarea que, en ocasiones, estos terceros no podrán asumir al no tener las capacidades necesarias por falta de recursos económicos o técnicos. En dichas circunstancias, se deben buscar alternativas para poder garantizar la seguridad de los servicios ofrecidos. Además, el uso de tecnologías como el *network slicing* conlleva un incremento de la complejidad del *software* y el alargamiento de las cadenas de suministro, aspectos que provocan un aumento de la exposición de las redes frente a terceros[4].

Network slicing

El *network slicing* ('segmentación de la red') consiste en dividir la red en subredes que pueden ser personalizadas para cubrir las necesidades individuales de cada cliente. Cada una de estas subredes actúa de manera virtualmente independiente aunque comparten una infraestructura física, lo que consigue mejorar la eficiencia tanto energética como económica. Dentro de los servicios personalizados que se pueden ofrecer, cabe distinguir dos categorías: los *servicios de conexión de red*, como pueden ser servicios de cobertura, latencias específicas para aplicaciones o velocidades concretas de carga y descarga, y los *servicios de recursos de red*, como niveles de seguridad en plataformas, *edge computing* o autentificación en tiempo real. Una de las ventajas que presentan en relación con la seguridad es el control de los ciberataques, ya que, al ser cada una de las subredes independiente del resto, un ciberataque puede ser contenido dentro de la subred en cuestión sin comprometer la estructura completa. Otra ventaja sería el control de equipos de riesgo, que en el caso de detectar comportamientos anómalos pueden ponerse en cuarentena en una subred aislada. Podemos identificar algunos riesgos derivados del uso del *network slicing*; por ejemplo, al compartir la infraestructura física, un ataque a una de las subredes puede conllevar que otras se queden sin algunos recursos que comparten.

Virtualización y descentralización de la arquitectura de red móvil

El desarrollo de tecnologías como redes definidas por *software* (*software defined networking*, SDN) y la virtualización de funciones de redes (*network function virtualization*, NFV) permite hacer las redes 5G más agiles, flexibles y dinámicas, una de sus principales ventajas al permitir reducir costes y alcanzar una economía de escala. La virtualización de la red viene acompañada de un proceso de descentralización que acerca ciertas tareas y procesos a los usuarios finales, lo cual reduce la latencia y aumenta la capacidad de cobertura. Sin embargo, estos procesos generan una mayor superficie de exposición a los riesgos de seguridad que la existente en las redes actuales.

El desarrollo de servicios 5G seguros va estrictamente ligado a la existencia de una infraestructura de red robusta. En generaciones previas, como el 4G, la seguridad de la red y de sus elementos está relacionada con la capacidad de aislamiento entre las entidades físicas que la conforman. No obstante, en las redes 5G el concepto clásico de

[4] GSMA, "An Introduction to Network Slicing", 2017, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf; Ericsson, "Serving up secure IoT with network slicing security", 04/09/2020, https://www.ericsson.com/en/blog/2019/9/future-network-slicing-security-iot.

aislamiento no es aplicable al tratarse de una arquitectura basada en funciones de red virtuales desplegadas en la nube. Además, el mayor número de puntos de enrutamiento, fruto de la citada descentralización de procesos, hace que su monitorización sea sustancialmente más compleja que en otras generaciones de redes móviles.

Heterogeneidad de acceso y de dispositivos de usuarios finales

La heterogeneidad es una de las principales características de las redes de acceso de nueva generación a partir de la combinación de micro y macroceldas, así como del uso de diferentes tecnologías de acceso (wifi, LTE, etc.). Esta heterogeneidad implica la existencia de un número muy variado de dispositivos que pueden acceder a la red por medio de distintas tecnologías y arquitecturas de acceso.

La variedad de dispositivos que admiten las redes 5G, además de las diferentes formas de acceso permitidas, pueden provocar importantes brechas de seguridad en las redes, especialmente al tratar con millones de dispositivos. En este contexto, destacan los dispositivos IoT, los cuales presentan en general una falta de mecanismos de seguridad, sobre todo en aquellos dispositivos de bajo y medio coste.

Cadenas de suministros. La tecnología de despliegue O-RAN

Uno de los principales riesgos que se identifican en las redes 5G está relacionado con la cadena de suministro, en concreto con la posibilidad de depender de un único proveedor ante una falta de diversidad. En este contexto, surgen las redes de acceso abiertas, conocidas como O-RAN (*open radio access networks*)[5]. El concepto de O-RAN permite diseñar y desarrollar una red de acceso con componentes de *hardware* de distintos proveedores basados en unos estándares comunes que garantizan la interoperabilidad y el funcionamiento conjunto. Esto favorece un ecosistema abierto de desarrollo y, en consecuencia, poder diseñar e implementar una arquitectura de red más elástica y flexible. Además, permite reducir los costos de los equipos debido a la competencia y la proliferación resultantes de este nuevo paradigma de suministradores. No obstante, una interoperabilidad total de múltiples proveedores en un ecosistema abierto plantea nuevos desafíos en cuanto a las pruebas, la gestión y la integración de los equipos.

[5] Open RAN Policy Coalition, "5G and Open RAN Security: Next Generation Trust", 25/06/2020, https://www.openranpolicy.org/wp-content/uploads/2020/06/5G-and-Open-RAN-Security-Next-Generation-Trust.pdf; O-RAN Alliance, "The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components", 24/10/2020, https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components; Ericsson, "Mobile radio access networks: What policy makers need to know", 17/09/2020, https://www.ericsson.com/en/blog/2020/9/ran-what-policy-makers-need-to-know.

Open RAN

El O-RAN se refiere a una arquitectura de red de acceso radio abierta, lo que incluye interfaces abiertas interoperables, virtualización de RAN y RAN habilitada por el *big data* y la inteligencia artificial. La arquitectura del O-RAN busca una mayor desagregación del *hardware* y el *software* y crea un ecosistema con una gran flexibilidad e interoperabilidad y completamente abierto a despliegues con múltiples proveedores. La implantación del O-RAN conlleva una serie de riesgos de seguridad, como el aumento de la superficie de riesgo, ya que se añaden nuevas interfaces, riesgos introducidos por el uso de aplicaciones en tiempo real y un mayor riesgo por el desacoplamiento del *hardware*. No obstante, el hecho de tener interfaces abiertas puede ayudar a mejorar la seguridad mediante mecanismos de microsegmentación. Además, el O-RAN está aprovechando el auge de las redes basadas en *software* para virtualizar muchas de las funciones que antes tenía que realizar *hardware* específico. Esta migración permite técnicas de seguridad avanzadas, como el *sandboxing* (aislamiento de procesos para ejecutar programas o funciones de manera separada), y técnicas de contenerización (encapsular funciones de *software* y todas sus dependencias para que puedan ejecutarse en cualquier infraestructura sin que surjan problemas por transferencias).

Mejoras introducidas por el 5G en la seguridad de las redes

Las redes de quinta generación no solo mejoran respecto a generaciones previas aspectos como el ancho de banda, la latencia o la densidad de dispositivos que pueden soportar, sino que además incorporan importantes mejoras relativas a la seguridad en dichas redes a la par que conservan los avances realizados y corrigen y perfeccionan aquellos aspectos que quedaban todavía sin resolver.

El Grupo de Cooperación NIS (*Network and Information Systems*) propuso en 2019 a la Unión Europea un conjunto de medidas denominadas "EU Toolbox" para potenciar la resiliencia de las redes 5G y mitigar los riesgos identificados[6]. Las medidas incluyen aspectos regulatorios, estratégicos y técnicos para la gestión de riesgos. El objetivo de estas medidas es integrar la seguridad en el diseño, despliegue y operación de las redes 5G, aumentar el nivel de exigencia de los estándares de seguridad de los productos y servicios asociados a las redes y reducir los riesgos asociados a suministradores individuales o a su falta de diversidad.

[6] NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 09/10/2019, https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security, y "Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures", enero de 2020, https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission.

EU Toolbox para la seguridad 5G

Publicada por la Comisión en enero de 2020, consiste en una serie de medidas para garantizar la seguridad en las redes reduciendo los riesgos de manera eficaz y que permiten garantizar, por tanto, el despliegue de redes 5G seguras en Europa. También incluye planes de mitigación del riesgo para cada una de las nueve áreas de riesgo determinadas en el informe de la UE sobre la evaluación coordinada de riesgos en redes 5G. Finalmente, recomienda una serie de medidas estratégicas y técnicas que deben adoptar todos los Estados miembros o la Comisión. Las medidas estratégicas consisten en un aumento de poder de las autoridades para tener mayor control sobre las redes 5G que se desplieguen y para mitigar algunos riesgos de ciberseguridad identificados; algunas de las propuestas son la diversificación de proveedores y de la cadena de suministro y la potestad normativa. Las medidas técnicas buscan aumentar la seguridad tanto en redes como en equipamiento; por ejemplo, medidas básicas y específicas para la seguridad en redes y requisitos a proveedores. Por último, dentro de los planes de seguridad en las redes se ofrece una serie de instrumentos para garantizar la seguridad, como el paquete de ciberseguridad o la Directiva NIS, cuyo proceso de consulta pública para su actualización finalizó en octubre y está a la espera de la evaluación de los resultados.

Autentificación y encriptación en las redes 5G

A continuación, nos centramos en estudiar las principales medidas y mejoras técnicas que introducen las redes 5G en el ámbito de la ciberseguridad. La autentificación y la gestión de la identidad son aspectos fundamentales en las redes celulares para proteger a los usuarios, la red y la comunicación entre ellos. En las redes 4G la autentificación es una tarea realizada por los operadores, quienes establecen un proceso de autenticación mutua en el que, por medio del protocolo de autentificación y gestión de claves (*authentication and key agreement*, AKA), tanto los terminales del usuario como el núcleo de la red validan sus identidades. Este protocolo emplea claves simétricas, que se comparten entre el usuario y la red, y tarjetas (U)SIM para la gestión de claves y la identidad.

No obstante, estos procesos presentan ciertas carencias, entre las que destacamos la falta de encriptación en la red de acceso al enviar la identidad del usuario. Para ello, las redes 5G encriptan la identidad internacional del abonado móvil (*international mobile subscriber identity*, IMSI), lo que aumenta la seguridad del proceso y extiende la longitud de las claves de sesión de 128 a 256 bits, con lo cual mejora la protección de la comunicación entre el dispositivo y el núcleo de la red. Además, las redes 5G introducen una serie de funciones de red específicas diseñadas para mejorar la seguridad de los procesos de autentificación y definen un marco unificado con nuevos métodos: 5G-AKA, EAP-AKA y EAP-TLS. Este marco permite la autentificación del equipo de un usuario tanto si accede al núcleo de la red a través de las redes estandarizadas como no estandarizadas.

Por otro lado, con el fin de gestionar la gran variedad de dispositivos que se pueden conectar a las redes 5G, especialmente en el ámbito del IoT, el mencionado marco incluye métodos alternativos de autentificación, como el método EAP-TLS, compuesto por un protocolo de autentificación extensible (*extensible authentication protocol*, EAP) con seguridad en la capa de transporte (*transport level security*, TLS). Este método no requiere el uso de tarjetas (U)SIM para la gestión de la identidad y procesos de

autentificación en la red, lo que facilita el uso de dispositivos con distintos tamaños, formas y consumo energético[7].

EAP-TLS y las tarjetas (U)SIM

Las tarjetas SIM son tarjetas inteligentes utilizadas en las redes móviles que almacenan las claves de servicio del usuario para identificarse al entrar en la red. La SIM tradicional tiene integrado tanto el *hardware* como el *software* en la misma tarjeta física. Una evolución adoptada a partir del estándar 3G es la separación del *hardware* y el *software* para una mayor seguridad; el módulo de identificación del abonado universal (*universal subscriber identity module*, USIM) es una de las aplicaciones de *software* dentro de la tarjeta de circuito integrado universal (*universal integrated circuit card*, UICC), la parte *hardware*. Desde el punto de vista de la gestión de la identificación y el acceso, las USIM utilizadas en el 4G son perfectamente compatibles con el 5G al ser capaces de autentificarse para acceder al sistema. Hay dos razones principales para su compatibilidad: no es necesaria una clave de seguridad fija entre la red y la tarjeta y todos los nuevos requerimientos de seguridad pueden descargarse y añadirse al *software* existente. No obstante, con la adopción del marco EAP para los procesos de autentificación, es posible implementar el método EAP-TLS en despliegues aislados, con lo que las USIM ya no serían necesarias.

El EAP es un protocolo de autentificación que proporciona múltiples métodos de autenticación, como tarjetas inteligentes, claves públicas o contraseñas de un solo uso. El EAP-AKA utiliza el módulo USIM para acceder a los datos de autentificación almacenados en la tarjeta inteligente del usuario. El EAP-TLS es una extensión del protocolo EAP al que se añaden los requisitos de seguridad descritos en el protocolo TLS, el cual proporciona comunicaciones seguras en Internet mediante técnicas de negociación cifrada, autentificación mutua y capacidades de manejo de claves. De esta forma, el EAP-TLS utiliza las confirmaciones de seguridad en la capa de transporte, encapsuladas en un túnel seguro, para autentificar tanto al cliente como al servidor mediante certificados.

Separación entre la red de acceso y el núcleo

A pesar de la mencionada descentralización de la arquitectura de la red 5G, existe una clara separación entre la red de acceso, centrada en la gestión de la radiocomunicación, y el núcleo de la red, que controla la gestión de recursos y la seguridad. Esta separación permite identificar y aislar fácilmente los elementos de la red en caso de que estén siendo atacados. Como consecuencia de esta separación, el núcleo queda como encargado de garantizar la autentificación del usuario y de encriptar el tráfico, tanto de datos como de señalización, con el estándar de encriptación avanzada (*advanced encryption standard*, AES), mientras que la red de acceso se encarga de enviar el tráfico encriptado entre el equipo del usuario y el núcleo de la red, con lo que protege el tráfico en la interfaz radio.

Además, el uso en el núcleo de la red de una arquitectura basada en servicios permite aplicar mecanismos de protección en capas más altas; por ejemplo, de transporte y aplicación. Por ello, además de la protección a nivel de red de la comunicación entre las entidades del núcleo por medio del protocolo IPsec, el 5G soporta protocolos de

[7] Ericsson, "Does the switch to 5G security require a new SIM card?", 15/01/2020, https://www.ericsson.com/en/blog/2020/1/5g-security-sim-card.

seguridad como el TLS, que protege la comunicación en la capa de transporte, o el OAuth 2.0, en la de aplicación.

Seguridad como servicio

Anteriormente, en relación con el concepto de NaaS, comentamos la posible incapacidad de los proveedores de los servicios para poder gestionar la seguridad en sus redes privadas. Ante esta situación, una posible solución consiste en que los operadores de telecomunicaciones, si poseen los recursos y mecanismos adecuados, les ofrezcan estas capacidades, es decir, ofrecer la seguridad como un servicio. Un ejemplo lo encontramos en la implementación de los mecanismos híbridos de autentificación, contemplados en las redes 5G, donde este proceso lo puede realizar el propio proveedor o el operador de red, el cual devolvería el resultado del proceso al proveedor del servicio.

Estas funciones de seguridad se pueden desplegar en una plataforma en la nube o como parte de la *network slice* privada asociada al vertical. Esta última opción presenta importantes ventajas en términos de seguridad, pues los posibles fallos o ataques en una *slice* no afectarán a todos los servicios que se estén proporcionando. Para ello y con el fin de garantizar la privacidad de los usuarios, se deben desarrollar mecanismos y herramientas que permitan el aislamiento entre *slices* para impedir que usuarios no autorizados accedan tanto a los recursos de red asignados como a la información que transportan. Como podemos ver, las medidas técnicas integran la seguridad desde el diseño, centrándose especialmente en el control de acceso. Igualmente, como queda recogido en la EU Toolbox, es necesario el desarrollo de mecanismos que verifiquen el cumplimiento de las medidas de seguridad física, virtualización, parcheo y actualización del *software* o certificación de los componentes, productos y servicios asociados a las redes 5G.

Conclusiones

Las redes 5G incorporan mejoras en las prestaciones de la red y en los mecanismos de seguridad que permiten ofrecer una plétora de servicios. Las principales mejoras en el ámbito de la seguridad están especialmente relacionadas con los procesos de autentificación, los cuales se han mejorado para evitar que los usuarios puedan ser rastreados en la red y que sus dispositivos sean manipulados. Asimismo, estos nuevos métodos de autentificación permiten el acceso heterogéneo de un número muy diverso de dispositivos a la red.

Sin embargo, todavía se deben seguir mejorando ciertos aspectos, pues aún es posible que usuarios malignos ataquen a otros usuarios en la red, especialmente cuando estos actúan como estaciones base falsas. Se debe seguir mejorando la seguridad en los terminales de usuarios, sobre todo en los dispositivos IoT de bajo coste. Finalmente, debemos destacar que todos los avances en seguridad no serán válidos si los operadores no despliegan las redes 5G respetando y tomando en consideración las reglas y recomendaciones establecidas por los organismos de estandarización a tales efectos.