Seguridad en Redes 5G Militares Desplegables

Autor: Cartujo Olmo, Pablo

Director: Gil Castiñeira, Felipe

Contacto: pcarolm@fn.mde.es

Resumen: En este Trabajo Fin de Master se realiza un análisis exhaustivo sobre la implementación y los desafíos de seguridad de las redes 5G en contextos militares. En una primera parte se describen las capacidades avanzadas de las redes 5G, incluyendo su alta velocidad y flexibilidad, que son cruciales para las operaciones militares modernas. Se enfoca en cómo estas redes mejoran la comunicación en escenarios tanto navales como terrestres, pero también destaca la importancia de abordar sus vulnerabilidades ante ciberataques. A continuación se profundiza en la infraestructura de las redes 5G, detallando su funcionamiento y las soluciones específicas desarrolladas para Armada por Telefónica.

Se analiza en detalle las vulnerabilidades de estas redes, constatando un avance en cuanto a las medidas de seguridad ante ciberataques comparadas con las redes 4G. Esto se debe a su mayor complejidad y al uso de nuevas tecnologías que aún están en proceso de maduración en términos de seguridad o a impresiones en la implementación de los estándares.

Ante estas evidencias se proponen una serie de medidas para mitigar estos riesgos, entre las que se incluyen el desarrollo de protocolos de seguridad más robustos, la implementación de sistemas de detección y respuesta a intrusiones y la constante actualización y revisión de las prácticas de seguridad. Además, sugiere la investigación y adopción de nuevas soluciones técnicas que puedan reforzar la ciberdefensa en el contexto de las redes 5G militares.

Finalmente, el documento concluye con una reflexión sobre la importancia crítica de asegurar las redes 5G en el ámbito militar. Subraya que, aunque las redes 5G ofrecen numerosas ventajas en términos de rendimiento y capacidad, la seguridad debe ser una prioridad para garantizar el desarrollo de la nube de combate.

Palabras clave: 5G, LTE, Ciberataque, Ciberespacio, Ciberdefensa, Sistema

---

1. Introducción

Las redes 5G en sus múltiples configuraciones son una tecnología compleja con múltiples posibilidades de funcionamiento que se deben conocer para entender las soluciones que se pueden utilizar en el mundo militar. Es de vital importancia entender la evolución que ha supuesto el sistema 5G frente a los sistemas tradicionales en cuanto al modelo de creación de redes y los múltiples sistemas radio que es capaz de manejar.

La evolución de las redes de telecomunicaciones móviles ha sido significativa en los últimas décadas, comenzando con la 1G, que introdujo las comunicaciones móviles analógicas, y avanzando a la 2G, que trajo consigo la digitalización y los servicios de mensajes. La 3G mejoró la capacidad y velocidad, enfocándose en la transmisión de datos y soporte para internet, mientras que la 4G se centró en la alta velocidad y la computación en la nube. La 5G, siendo una evolución natural, hereda y mejora tecnologías de generaciones anteriores, ofreciendo mayor velocidad,capacidad, y plantea nuevos desafíos y consideraciones en cuanto a seguridad.

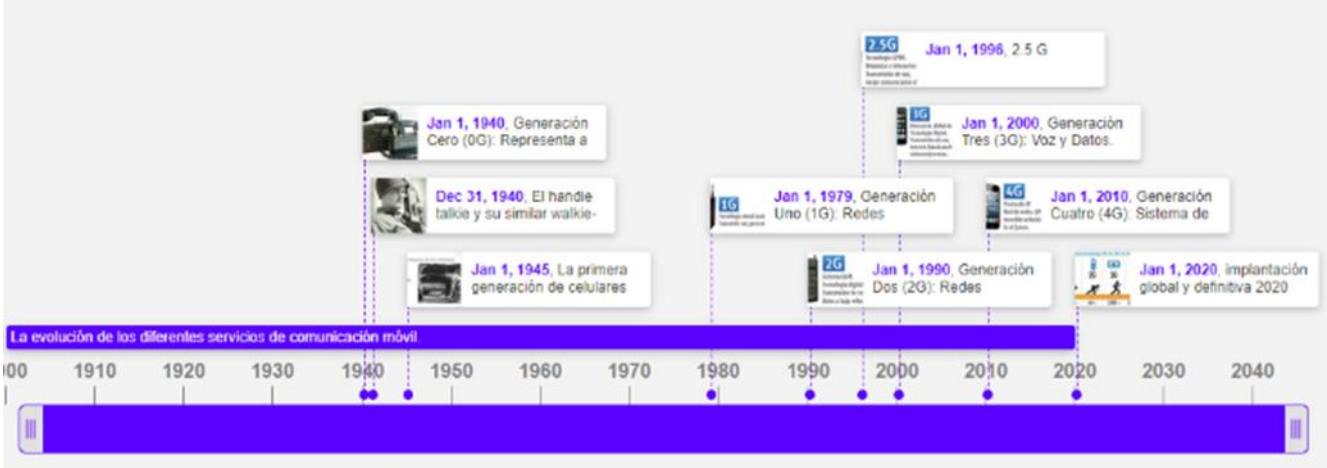

Figura 1Evolución de las redes móviles. [1]

Las redes 5G aprovechan tecnologías ya existentes como la MIMO: la Multiple-Input Multiple-Output (MIMO), basándose el principio de que utilizando múltiples antenas, se pueden enviar y recibir múltiples flujos de datos simultáneamente, lo que aumenta significativamente la capacidad y la calidad de la conexión.[2]. Tambien aplican tecnologías nuevas como el slicing, mediante el cual se introduce la virtualización de redes y la computación lógica para facilitar aplicaciones emergentes que pueden tener diversos requisitos de servicio. Por medio del slicing se divide una red física en múltiples redes lógicas virtualizadas únicas sobre una infraestructura común de múltiples dominios. A través de este concepto, se pueden asegurar tanto QoS como recursos de red. [3]

Con estas mejoras técnicas las 5G presenta como principales beneficios frente a tecnologías anteriores una obstensible mejora en la tasa de transferencia de datos, en la latencia, en la eficiencia energética, en el volumen de tráfico soportado y en la densidad de conexiones [4]

A la hora de desplegar las redes 5G existen dos modelos: el modelo Stand Alone (SA) y el modelo Non Stand Alone (NSA). El 5G SA es el modelo de implementación donde el 5G proporciona una red 5G de extremo a extremo; en esta arquitectura, tenemos una red independiente como 5G New Radio . SA presenta una arquitectura 5G pura, esta implementación se basará en el uso de 5G para el Plano de Control y el Plano de Usuario[5]. La opcion Non Stand Alone por el contrario responde a una red 5G respaldada por la infraestructura 4G y las radios 5G acopladas a la LTE EPC. Es decir las redes NSA ofrecen conectividad vía tanto a través de 4G AN (E-UTRA) como de 5G (NR) Esta doble característica también se denomina EN-DC, o doble conectividad E-UTRAN-NR [6]

Un problema al que deben de hacer frente las 5G es la gestión del espectro, las frecuencias son un bien escaso y muy demandado dentro de las comunicaciones tanto civiles como militares y su uso debe de ser regulado por la administración[7]. Existen numerosas iniciativas para la gestión del espectro, entre las que se encuentra Authorized Shared Access (ASA); creado como una herramienta para evaluar las bandas asignadas al servicio móvil, Mobil Service, (MS) mediante las Regulaciones de Radio, pero identificado y utilizado para diferentes propósitos derivadas de decisiones nacionales de las administraciones (y/u organizaciones regionales). Al final como ha sido el caso con las 5G se ha tenido que compartir el espectro en este sentido, uno de los ejemplos internacionales de mayor importancia, es el conocido como Servicio de Radio de Banda Ancha para Ciudadanos (CBRS) americano. En CBRS, los niveles de acceso se dividen en tres niveles, el primer nivel de acceso a acceso para titulares esta compuesto por los radares navales en aguas litorales y el servicio comercial de satélites fijos, Fixed Satellite Service (FSS). El segundo nivel consiste en Licencias de Acceso Prioritario (PALs), y el tercer nivel comprende a los usuarios oportunistas conocidos como Usuarios Autorizados Generales (GAA) La asignación de canales a diferentes niveles y las configuraciones relacionadas son realizadas por el SAS.[8].

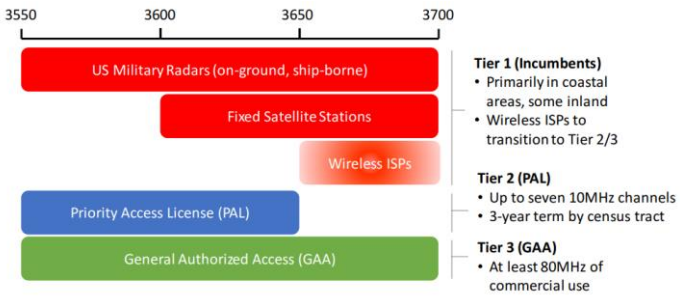

Figura **Error! No text of specified style in document.**-CBRS Tier 1-3 [9]

2. Desarrollo

2.1 Despliegue 5G en la Armada

Si bien en el pasado la Armada experimentó con la tecnología 4G-LTE, implementada en los BAM "Furor" y "Audaz", únicamente para los Trozos de Visita y Registro . Con la implementación de las redes 5G las capacidades logradas anteriormente mejoran de forma exponencial en términos de fiabilidad, velocidad y alcance haciéndose extensivo a todo espectros de las operaciones navales, en la

forma del concepto “nube de combate”. Este concepto, tanto a nivel nacional como internacional, cada vez está ganando más importancia. Esta “nube” será un sistema complejo, sobre el que se desarrollen e integren los servicios necesarios para alcanzar la superioridad en la información que permita reducir los tiempos del ciclo de decisión, disponiendo de la información correcta en el lugar adecuada y en el momento preciso, proporcionando una capa de comunicaciones de calidad lo que ya se conoce como “Burbuja Tactica”.

Para ello se ha planteado tres escenarios:

- Proyecto Base Naval, escenario litoral. Despliegue de Nodo Fijo: La solución propuesta debe permitir el empleo de una combinación de frecuencias de radio que posibiliten la conectividad de los distintos elementos en un ambiente litoral como extensión o apoyo a unidades navales o intra base maximizando la distancia operativa y mitigando posibles problemas de interferencias. Las bandas que se consideran más adecuadas para optimizar este proyecto son las de 700MHz y 4.4GHz, aunque podría evaluarse la posibilidad de emplear la banda de 26 Ghz en principio desestimada por el bajo alcance que ofrece.
- Proyecto buques de la Armada: la instalación de equipos 5G en una plataforma naval y los equipos necesarios para explotar esta capacidad entre al menos dos buques de la Armada. Esta solución debe permitir su despliegue temporal en otras unidades, hasta que la implantación de la Tecnología 5G sea alcanzada en todas las unidades navales.
- Por otro lado, la instalación de un nodo SA en un buque permite establecer comunicaciones buque-cosas y el establecimiento de una burbuja de comunicaciones alrededor del buque que posibilitará el empleo de vehículos no tripulados, el establecimiento de las comunicaciones con otras unidades que se encuentren dentro de la burbuja y sensorizar gran parte de los sistemas del buque. Tambien permitiría la conexión a los nodos en ambiente litoral
- Proyecto Unidades de Infantería de Marina. Como complemento a los dos proyectos anteriores se realizó un diseño de red con las antenas necesarias para establecer una burbuja de comunicaciones y con toda la pre-instalación necesaria para integrar un 5G CN en un vehiculo táctico de Infanteria de Marina,

Simultáneamente se probaron las antenas y alcances en el “palo integrado” de las fragatas F-110 y en los buques de mando con resultados satisfactorios.

2.2 Seguridad en las redes 5G

Aunque generalmente la red 5G es considerada una evolución tecnológica, en tanto incrementa la capacidad y cobertura, puede ocurrir que en algunos aspectos o sea más segura que la red 4G. Esto es porque en virtud del desempeño de la red se han hecho concesiones de seguridad [9]; Por su carácter inalámbrica puede sufrir ataques de emulación de la BS [10]; o tambien debido al factor de su gran velocidad de transporte de datos y el soporte creciente de las aplicaciones las cuales generan nuevas brechas de seguridad, tanto a nivel de los proveedores de servicios, como de los usuarios finales. [11]

Por otra parte, existen ciertas mejoras en cuanto a la seguridad. Una parte importante de ellas no había sido considerada en la redes anteriores a 5G mientras que en otros campos solo se mejoran las capacidades de seguridad.

Pese a estas mejoras frente a las anteriores versiones, lo cierto es que entre otras causas con una mayor velocidad de datos, la red 5G puede ser objeto de ataques, por ejemplo, de Denegación de Servicio Distribuido (DDoS) más fuertes y precisos.

Así la seguridad debe de abordarse desde diferentes enfoques

La seguridad de las redes 5G no se puede abordar desde un único frente sino que se plantean 6 diferentes enfoques:

- Seguridad en el acceso a la red: características de seguridad que permiten a un terminal de usuario autenticarse y acceder a la red al proporcionar protección en las interfaces de radio.
- Seguridad en el dominio de la red: características de seguridad que permiten a los nodos de la red intercambiar señalización y datos de usuario de manera segura.
- Seguridad en el dominio del usuario: características de seguridad que permiten el acceso seguro de los usuarios a los dispositivos móviles.
- Seguridad en el dominio de la aplicación: características de seguridad que permiten el intercambio seguro de mensajes entre aplicaciones en los dominios de usuario y proveedori.
- Seguridad en el dominio de la Arquitectura Basada en Servicios (SBA): un nuevo conjunto de características de seguridad que permite a las funciones de red de la SBA comunicarse de manera segura dentro de los dominios de servicio y otros dominios de red. Visibilidad y configurabilidad de la seguridad: características de seguridad que permiten al usuario estar informado sobre qué características de seguridad están en funcionamiento

2.3 Seguridad en las redes 5G de la Armada

Los sistemas 5G en la Armada /Defensa presentan como hemos visto ciertas singularidades con respecto a los sistemas comercializados por los operadores o los ISP. Estas singularidades a la vez son tambien unas meddas de seguridad en si mismas. Entre otras podemos destacar que se trata de sistemas que cuentan con su propia RAN, su propio core y con una cantidad limitada y conocida de UEs. Estos terminales usan su propia SIM que como hemos visto llevan su propio sistema de cifrado.

Además, los elementos de la red están protegidos de forma física. Por ejemplo la RAN de un operador cualquiera puede estar colocada en la azotea de un edificio de una comunidad de vecinos cualquiera. Sin embargo la RAN militar se encontrará en una unidad militar o baja lo protección continua de esta.

Tambien debemos de recordar que los UE no hacen *roaming*, no se conectan a otras redes, aunque se traten de redes comerciales seguras. De hecho no se pueden conectar ni siquiera a la red del *partner* tecnológico. Así mismo tampoco esta contemplada la posibilidad de que se una a las redes 4G con las que cuenta la Armada.

Por todo lo anterior las vulnerabilidades a estos sistemas están más restringidas que las de las redes 5G de las operadoras. Sin embargo afrontan otras problemáticas como la confidencialidad de la información que manejan así como la disponibilidad de la misma y la robustez en las comunicaciones.

Cara a analizar las vulnerabilidades para este escenario en cuestión, vamos a admitir que el atacante no pude tener nunca acceso físico, a las SIM card, a la estación base, o al CN para obtener acceso a las claves de sesión a las claves criptográficas. Por el contrario en nuestras premisas sí que establecemos

que el atacante puede o está dispuesto a interceptar la señal radio, realizar ataques MiM, Spoofing y que es capaz de transmitir en la misma frecuencia que nuestra BS y con igual o más potencia.

En este sentido se estudian las vulnerabilidades que se consideran más factibles teniendo en cuenta el modelo de red que se ha adoptado como son:la autenticación mediante MAC, o el aprovechamiento de los mensajes MIB, Master_Info_Block, y los mensajes SIB, System_Info_Block, o la Defensa contra *Jamming* y *Spoofing*. Se desdeñando todas a aquellas otras que no se aplican, bien porque afectan a factores como el roaming que son no aplicables o porque se consideran solventadas con la infraestructura aplicada. En este sentido se propondrán soluciones a estas carencias de seguridad.

Finalmente se anticipan soluciones consideradas prometedoras entendiendo como tales las necesidades que se pueden plantear como evolución a la propuesta actual. Con las auto limitaciones impuestas tambien se han generado barreras a ciertas capacidades de la tecnología que desde esta opinión deben de al menos ser contempladas caras a futuros desarrollos o a mejoras en el ciclo de vida. Tambien se pueden identificar soluciones a problemas no que pueden ocurrir cuando se establezcan escenarios diferentes como la inclusión de usuarios itinerantes en la red 5G militar, el uso de antenas sobre dron cautivo para ampliar alcances, el uso de slices en frecuencias alternativas o el aumento de la potencia de transmisión.

3. Conclusiones

Las redes 5G son la apuesta de futuro en las comunicaciones tácticas , especialmente en las navales. Si bien ha surgido problemas como la repartición del espectro, problema grave en ambientes como el marítimo en el que no existen a priori otras fuentes de radiación que las propias no parece ser un problema. En otros escenarios, como los terrestres o los litoral, si puede plantear dificultades ya que la banda elegida puede entrar en conflicto con intereses civiles. De todas formas estas dificultades pueden ser fácilmente sosláyales mediante legislación o aumento de potencia.

Lo que sí parece indudable es la gran cantidad de casos de uso que se le pueden atribuir y la capacidad adicional que otorgará a las naciones capaces de explotar sus capacidades. Es de resaltar que otras potencias militares estén interesadas en nuestras soluciones y que seamos como nación y sector industrial pioneros en este campo. Desde mi punto de vista este primacía se ha conseguido por varios factores entre los que puedo destacar el concurso de un ISP importante nacional como es Telefónica, así como de los esfuerzos que se realizaron con el desarrollo del 4G naval.

Los esfuerzos realizados para crear soluciones multi escenario como son el terrestre, naval puro y litoral, han dado como fruto soluciones ya depuradas y experimentadas sobre el terreno, con esa capacidad desplegable que caracteriza a la Armada. El concepto de nube de combate o nube táctico parece estar maduro mientras que se observa una clara evolución en cuanto a capacidades sobre los primeros intentos sobre redes 4G. La continuidad y la segura evolución parece garantizada con las pruebas realizadas con el “palo integrado” de la futura F110. El haber confirmado su viabilidad es de suma importancia ya que la inclusión de nuevas antenas perjudicaría seriamente a un diseño tan notable como lo es la mueva serie de Fragatas de alta capacidad.

Salvado la bondad del diseño y la capacidad de integración en futuras unidades cobra especial relevancia el factor de la seguridad. Si la seguridad en las redes de comunicaciones es un factor sumamente importante y lo es aún más para las redes militares. Las redes 5G no son ajenas a ello y ha evolucionado notablemente en comparación con sus predecesoras y en gran medida las 5G implementan nuevas formas de securización de las redes o mejoran las ya existentes. No obstante

muchas de estas medidas si bien son contempladas por la asociación encargada de estandarizarlas, en gran cantidad de ocasiones deja al libre albedrío del operador la implementación de parte de ellas. Por lo tanto las redes 5G militares deben de hacerse cargo e implementar todas estas medidas o en su defecto sustituirlas por otras que al menos las igualen en capacidades.

A estos efectos durante esta monografía se han explorado los mecanismos y las vulnerabilidades de seguridad. De todas las amenazas conocidas a las redes 5G la solución implementada es la menos vulnerable. Se trata de una solución SA con todo el equipamiento de red propietario y aislado. Esta esquema plantea una red SA con CN, RN y UEs propietarios y aislados de otras redes. A su vez tampoco permite la conexión a otras redes como 4G. Tras analizar la vulnerabilidades que pueden afectarla se puede considerar una red segura más aun teniendo en cuenta que se trata de una red cifrada.

A partir de esta configuración las posibilidades que puede aportar a un entorno táctico son muy elevadas gracias a la velocidad, baja latencia y disponibilidad que otorga. Sobre el terreno la solución puede aportar capacidades tácticas en entornos de comunicaciones degradas como es la "nube de combate". A medida que la efectividad de las redes 5G militares se continúe asi aumentarán los casos de uso.

Si el proyecto dron cautivo se formaliza de correcta el escenario "litoral" pasará a ser aquel cualquiera en el que concurse un destacamento de Infantería de Marina y un buque de la Armada. Es decir, debido al alcance que va a proporcionarnos estos elementos, el elemento de instalación en tierra podrá ser cualquier elemento móvil y además será sumamente discreto.

Como líneas de accion a futuro entendemos que las redes 5G militares deben de disponer de la capacidad de permitir el acceso a las redes militares de usuarios no pertenecientes a las infraestructura original. Es decir permitir que un tercer estado se conecte a nuestra red con sus propios terminales. Aprovechando la capacidad de crear *slices*, se pueden segregar estos terminales dándoles capacidad por ejemplo para disponer de comunicaciones telefónicas mediante el uso de la salida satélite de nuestro nodo. Esta característica tendría un componente "efectista" cara a la opinión pública y representaría una gran publicidad como país generador de tecnología.

Por último considero que la no inclusión de tecnologías menos capaces como las 4G o LTE es un acierto porque crearía puntos únicos de fallo en cuanto a vulnerabilidades.

Agradecimientos

Quisiera agradecer la inestimable colaboración del tutor el Doctor D. Felipe Gil Castiñeira como guía de este Trabajo Fin de Master.

Como mención especial agradecer a mi esposa Maria Jose Osuna su apoyo y comprensión siempre incondicional. Así mismo quisiera tener un recuerdo muy especial para mi tía Maria del Carmen Olmo.

Referencias

[1] J. R. Brito, «Evolucion de las rede móviles hasata hoy en día y el impacto de la red móvil de quinta generación.,» *Revista ReDTiS*, vol. 3, nº 3, 17 Dic 2019.

[2] M. Jordão. y N. B. Carvalho., «Massive MIMO Antenna Transmitting Characterization,» de *2018 IEEE MTT-S International Microwave Workshop Series on 5G Hardware and System Technologies (IMWS-5G)*, Dublin, Ireland., 2018.

[3] C. Zamfirescu, R. Iugulescu, R. Crăciun, A. Vulpe., F. Y. Li y S. Halunga., «Network slice allocation for 5G V2X networks: A case study from framework to implementation and performance assessment,» vol. 45, nº 100691, 2024.

[4] A. R. I. G. A. I. S. a. H. D. I. Parvez, «A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions,» *IEEE Communications Surveys & Tutorials*, vol. 20, nº 4, pp. 3098-3130, 2018.

[5] N. M. Akshatha, P. Jha y A. Karandikar, «A Centralized SDN Architecture for the 5G Cellular Network,» de *2018 IEEE 5G World Forum (5GWF)*, 2018.

[6] A. Sultan, «5G System Overview. 3GPP Rel 19,» 3GPP, 2022.

[7] B. K., J. Engelberg y R. G., «Licensed Shared Access (LSA) — Regulatory background and view of Administrations,» de *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Oulu, Finland, 2014.

[8] K. Mun, «CBRS: New Shared Spectrum Enables Flexible Indoor and Outdoor Mobile Solutions and New Business Models,» Mobile Experts LLC, 2017.

[9] R. Thomas y F. Scholler, «Overview of NIAG Study SG-254,» ORANGE-THALES, 2021.

[10] L.N. Newman, «5G Is More Secure Than 4G and 3G—Except When It's Not,» Wired,, Dec 2019. [En línea]. Available: https://www.wired.com/story/5g-more-secure-4g-except-when-not/, accessed October 2020. [Último acceso: 22 Nov 2023].

[11] C. Gonzalez, «Desafíos de Seguridad en Redes 5G,» *Revista Technology Inside by CPIC*, vol. 3, nº 3, pp. 36-45, 2019.

[i] Es importante destacar que las especificaciones 33.501 no cubren la seguridad en el dominio de la aplicación.