Advanced Research on Information Systems Security

ARIS²
an
international journal

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Security in 5G Mobile Communications

Gilson Ferreira

DEISI – Lusófona University, Lisbon, Portugal
Email: gilson_ferreira@hotmail.com

Abstract

In mobile communication services, since its conception as a signal to be transmitted with quality and security. The evolution of this concept applied to the 5G standard, which is a system composed of several architectural innovations, technologies, concepts to meet service requirements, implies validation of the security aspect. Using a methodology to obtain the materials to be analyzed and thus carry out a review of scientific publications with a restricted focus on safety. Its architecture, main services, security, risks and mitigations observed in this review, added with other sources so that we can compose a restricted view of the security of this standard compared to what was proposed and observed with its implementation evolution, seen in the reports issued. Finally, the discussions, proposals and conclusions obtained will be based on whether networks are composed of security at their origin, or whether security mechanisms are created through weaknesses created by the constant evolution of the complexity of these networks.

Keywords: Security; Mobile Networks; 5G; Risks; Vulnerability

Citation: G. Ferreira, "Security in 5G Mobile Communications", ARIS2-Journal, vol. 4, no. 2, pp. 16–31, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.41

* Corresponding author. Email address: gilson_ferreira@hotmail.com

1. Introduction

Mobile networks use aerial propagation in the form of electromagnetic waves, so from the beginning, their information transport capacity was restricted by channel limitations in the frequency spectrum, where their bands are normally established by the regulatory agencies of each country.

Due to it being a frequency and power range, propagation (distance) and its ability to transmit information are limited, and when we analyze it with a focus on security, these networks have always suffered from security requirements [1].

Over time, various coding protocols were developed to ensure control of transmission errors, also ensuring that the transmitted information could only be recognized by the authorized receiver.

Mobile networks are actually a cluster of technology, connections, protocols, networks and services, which we can call interconnected systems, or merely, systems.

These systems need to be secure in themselves, as well as at the junction of each subsystem that composes them, making this network not only a signal transmitter in which coding and decoding of its transmission guarantee the security of the system.

Mobile networks are evolving and as a result their systems are becoming increasingly complex and heterogeneous, with the current standard being 5G R15 [2], it really became a composition of technologies, focused on providing services and based on this premise, its operating requirements were developed with a real paradigm shift [1], [3], [4], [5].

With the development of these 5G and, in the future, 6G mobile network systems, security requirements have become increasingly important so that services can actually be used, which require a high level of security, these being decisive as the Shared services applied to 5G are sensitive borders, requiring increasingly greater protection and security barriers.

In this literary review, the PRISMA methodology was used [6] and so we separated the reports necessary to answer the question that is the subject of this work: “Security in 5G mobile communication?”.

Security in a mobile network, including 5G, is an extensive subject, therefore, this work is limited to the items now collected by the applied methodology and thus we have a restricted view on the subject of security in a 5G network, focusing in a limited way on its architecture, main services, security, risks and Mitigations from a security perspective.

Additionally and complementing the methodology, we will include in the final discussion some points of ethics, security framework that are increasingly valuable to guide future development and proposals arising from this analysis.

2. Methodology and Database

This review of reports was prepared adopting the Preferred Reporting Items for Systematic and Meta - Analysis - PRISMA methodology [6].

Initially, we defined what would be the object of this review in order to parameterize the research criteria to be carried out.

We used the IEEE Xplorer Digital library database as the main source, applying the determined filters and criteria, which will be demonstrated in item 2.2 - Criteria Applied to Research.

Additionally, as secondary sources we will introduce:

- ISO IEC 27001:2022 [7];
- Gartner Research [8];
- The Human Tecnology Fundation [9];
- OSI Layer [10].

2.1 Research Object

This review applied to the PRISMA methodology seeks to strictly answer the following question:

"Security in 5G mobile communication?”

2.2 Criteria applied for Search

Considering the PRISMA 2022 methodology, which is a guiding workflow, being flexible in defining the research method.

In this way, we composed the modeling of the main library: IEEE Xplorer Digital.

Providing the results after applying the following filters:

Location	Quantity
Conference	10
Journals	8
Books	1
Early Access Articles	2

Table 1 - selection criteria

Following the methodology and formatting to search for the object of this work, we adopted the following report exclusion methods:

KEYWORD	OPERATOR
Internet security	AND
Cybersecurity	AND
Privacy Protection	AND

Table 2 - exclusion criteria

In the same way, through the introduction of another study source, ISO-IEC 27001:2022 and thus adopting a reference on the security framework as a view of the object of this Report.

Therefore, we adopted table 3 as an eligibility item:

KEYWORD	OPERATOR
Internet security	AND
Cybersecurity	AND
Privacy Protection	AND

Table 3 - eligibility criteria

We added new alternative sources, being complementary, to improve the discussion on security, which we evaluated with additional material to better compose the limits and values that guide the discussion of security to be applied in order to better address the issue raised by this work.

Thus, regarding ISO IEC 27001:2022, we compared the items relevant to the protocol, which brought the Cyber Security innovation to it, among other sources of support for the determination that we consider important to better qualify this work.

Regarding the Gartner paper: The Gartner 100 Data Analytics Predictions Trough 2028, we consider a more realistic scenario based on this market research.

We consider the ethical contours via The Human Technology Foundation, being: "Operatinalizing Ethics in the Digital: How to go beyond good intentions?".

Through the OSI layer, we used the concepts exposed in the paper in question, to compose a non-extensive and mere reference list of the main threats around its layers, given the current 5G architecture.

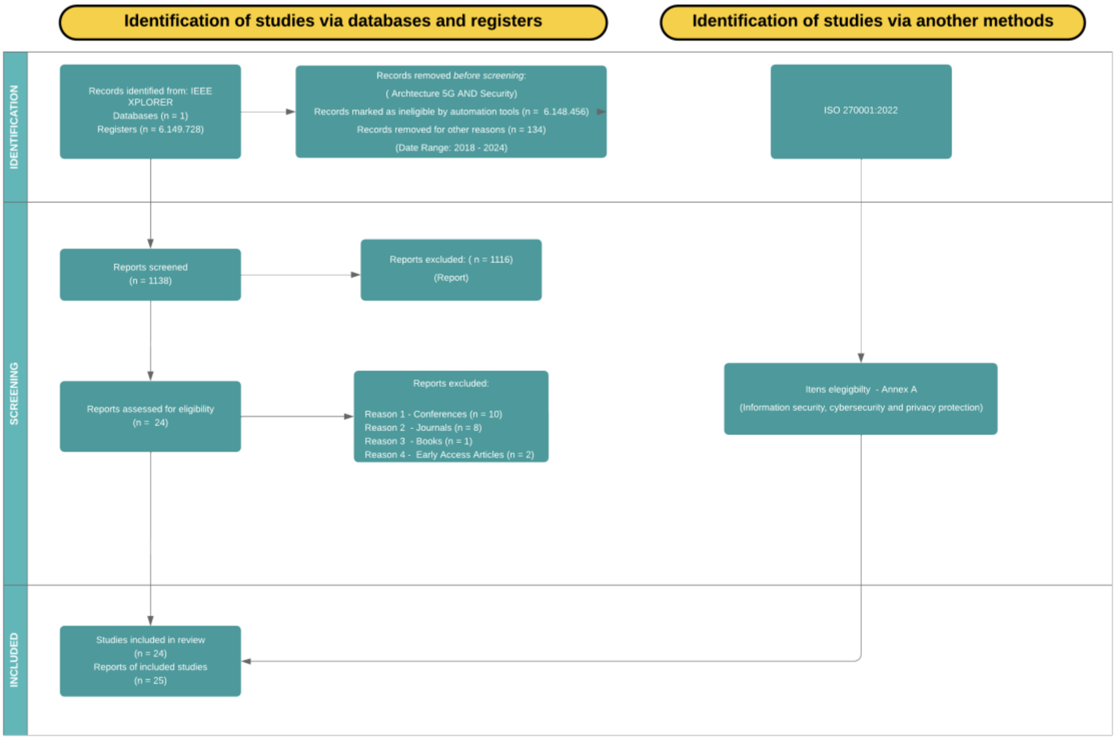

Identification of studies via databases and registers
Identification of studies via another methods
IDENTIFICATION
Records identified from: IEEE XPLORER
Databases (n = 1)
Registers (n = 6.149.728)
Records removed *before screening*:
(Archtecture 5G AND Security)
Records marked as ineligible by automation tools (n = 6.148.456)
Records removed for other reasons (n = 134)
(Date Range: 2018 - 2024)
ISO 270001:2022
SCREENING
Reports screened
(n = 1138)
Reports excluded: (n = 1116)
(Report)
Reports assessed for eligibility
(n = 24)
Reports excluded:
Reason 1 - Conferences (n = 10)
Reason 2 - Journals (n = 8)
Reason 3 - Books (n = 1)
Reason 4 - Early Access Articles (n = 2)
Itens elegigbilty - Annex A
(Information security, cybersecurity and privacy protection)
INCLUDED
Studies included in review
(n = 24)
Reports of included studies
(n = 25)

Figure 1 - complete PRISMA review flowchart

2.3 Report Study by Selection

Through the selections and criteria applied to the main source, we obtained more than 1100 Records, all in the English language, highlighting that existing reports from 2018 were considered, supported by the fact that the 5G R15 standard was adopted as an official standard and from this year onwards, and through this, documentation for the proposed study can be obtained.

The alternative sources and the secondary source were considered as the eligibility criteria that allow us to observe the entire ISO-IEC Standard [7], which in its current edition presented significant changes that we will use as a basis to conceptualize proposals and discussions applied to this work.

3. Results

As detailed in the previous sessions, the methodology applied, with method, selection and exclusion criteria above we collected twenty-three articles and a book section for the main source.

Via an alternative source, an annex was inserted consolidating a total of twenty-five works to compose material to answer the question presented below, restricted in the articles and with the aim of evaluating the main topics applied to the 5G mobile network.

Our review considers it an analysis restricted to the selected papers, being divided into the following themes:

- Architecture and Services;
- Security, Risks and Mitigations.

3.1 Architecture

The architecture proposed by 5G technology was created with audacious technology challenges, breaking existing paradigms [4], [8].

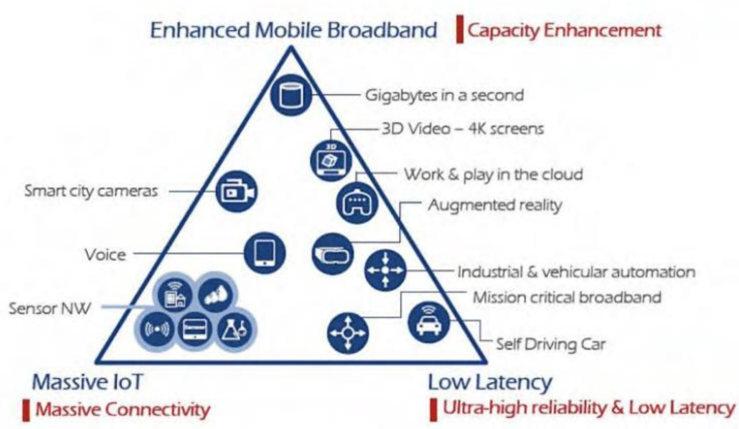


Figure 2 - The triangle of 5G applications (source: ETRI graphic, from ITU-R IMT 2020 requirements)

The most audacious technological standard being discussed and in the search for its viability is the network architecture based on service delivery anywhere and for this, non-terrestrial networks (NTN) are being introduced, composed of integrated satellite networks with UAV networks.

These configurations have become a modality that seeks to reduce hardware, maintenance and power costs with the appeal of “anywhere” access. [11], [12].

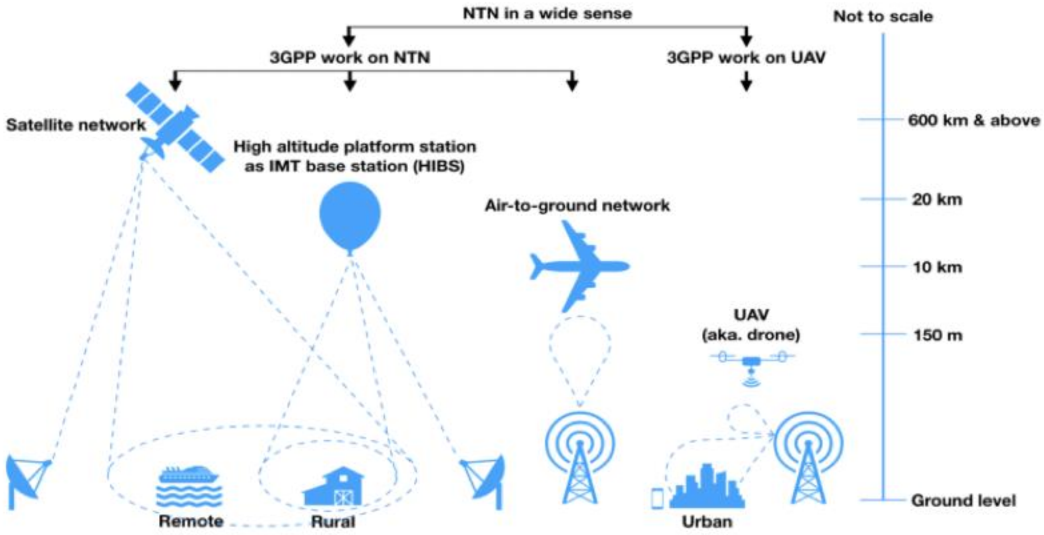
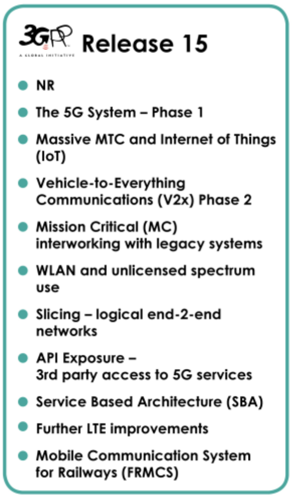


Figure 3 - NTN - Non Terrestrial Network (source: Share Tech Note, from 5G NTN)

This new concept implemented by the 5G standard, with its technological multiplicity, provides several adjustments, new concepts and challenges, which must include security in its structure, being one of the most complex elements [1], [3], [12], [13], [14], [15].

This new network delivery concept, based on a composition of technologies, was the necessary means to deliver the requirements established by the 3GPP R15 standard.



Release 15

- NR
- The 5G System – Phase 1
- Massive MTC and Internet of Things (IoT)
- Vehicle-to-Everything Communications (V2x) Phase 2
- Mission Critical (MC) interworking with legacy systems
- WLAN and unlicensed spectrum use
- Slicing – logical end-2-end networks
- API Exposure – 3rd party access to 5G services
- Service Based Architecture (SBA)
- Further LTE improvements
- Mobile Communication System for Railways (FRMCS)

Figure 4 - 5G Standard (source: 3GPP, from 3GPP R15)

It is observed that 5G architecture came in the form of service delivery as can be seen in figures 2 and 4, and the requirements for latency, bandwidth, simultaneous access, among others were subsidiary to provide the services, thus being an architecture oriented towards services and not network requirements and/or protocols [16], maybe security.

Architecture developed for 5G, which in its predecessors was delivered through networks connected by connection towers and with equipment from each operator, has currently become a complex solution delivery system among other solutions under development that go beyond the scope of this work, [4], [12], [17].

It becomes noticeable that 5G has a heterogeneous architecture, making up other innovations such as RAN (Open Network Radio), which enables countless possibilities for business and application development, which takes up the concept of network disaggregation, seeking to make it more flexible and modularize new/current wireless communication networks, [3], [18].

In the meantime, RAN was introduced with the need to reduce costs and simplify operations, as we are distributing investments with other players and focusing on services respectively, [3].

This fact in itself is not new, as decades ago we had the same path with fixed networks, the famous neutral networks, turning operators into content providers on shared networks.

This “open” architecture begins in this author's understanding as Neutral Mobile Network - NMN (author's definition), starting with Service Slicing, softwarezation, SBA, API in 5G, [3], [4], [5], [19], [20], [21], [22].

As in O RAN, C RAN are for virtualization of services and networks, being located in clouds, composing this architecture or part of it in NMN, which will be fully consolidated with the evolution to the 6G standard (Deep Slicing and another share concepts), [1], [3], [4], [5], [18], [21], [23], [24], [25].

In this sense, Edge Computing, provided by the virtualization movement, sought to improve the performance of services via applications, which makes security mechanisms even more complex, so that it can guarantee that this technology mesh, services can be secure, security systems security, firewall, an entire analysis and control system operated by NOC AND SOC [20].

When we enter into systems designed and in great demand for their application, such as the IoT and Vehicular System, which are the major providers of development of this architecture, we have truly entered the era of Machine to Machine, which requires autonomous architectures with security challenges still untried and thus require several studies and analyzes to provide this new market [2], [12], [14], [15], [16], [24], [25], [26], [27].

IoT allows various equipment or devices to communicate anywhere, anytime and without human interference, and in the 5G network, these connections become large-scale, thus making thousands of simultaneous connections, carrying millions of information [15], [16], [26].

As IoT technology allows the use of different communication protocols, the most sensitive security requirements must therefore be endorsed and considered in the 5G architecture, especially in a virtualized and completely heterogeneous network.

Smart/connected cars thus have various network/architecture/application configurations added to the complexity of high data rates, real time and multiple mobile and/or fixed interactions [14], [15], [16], [24].

All of this implies security that was once contained, previously restricted to a closed network and now focused on equipment structured in several networks, becoming a complex set of security segments, which must be fully consolidated together so that we have a network multi technology, multi services operating in complete security [3], [5], [12], [13], [14], [15], [18], [21], [22], [23].

3.2 Security, Risks and Mitigations

Every network since its creation has included the three items, even if they are implicit. Security, Risks and Mitigations are the focus of studies and validations that resulted from the development of the 5G standard [2], [11], [12], [15], [20], [28], [29], [30].

As a guide, we include the description of the OSI layer, to list possible attacks on them.

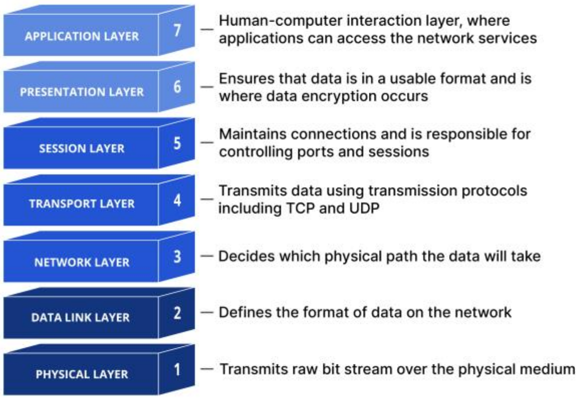

APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATA LINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

Figure 5 - OSI Model (source: CloudFire, from Learning Objectives

As the architecture developed by the 5G standard is a heterogeneous composition that permeates all these layers vertically and horizontally, we evaluate the proposals in the suggested literary reviews in a macro way.

When we talk about these layers, we can list the main types of attacks for each type of layer, which are briefly described in table 4:

Layers	Attacks
Application	Exploit
Presentation	Phishing
Session	Hijacking
Transport	Reconnaissance
Network	Mitm
Data Link	Spoofing
Physical	Snifing

Table 4 - layers x attacks

In every bibliographical review presented, we went into several layers listed above, with the 5G standard being made up of different technologies. In summary, we began to describe each type of attack, as they become the existing risks, in which, each proposal, report brings a mitigation/improvement opportunity for a given layer. Therefore, we describe in table 5 a summary of the types of attacks:

Attacks	Resume
Exploit	Malicious code that exploits a weakness of systems to cause accidental conduct or acquire unapproved access.
Phishing	Method that uses deception to manipulate users into using malicious links or disclosing sensitive personal information.
Hijacking	Security attack on a user session for a web application.
Reconnaissance	Used as a preparation to gather relevant information before launching an actual attack
MITM	Cyberattack where attackers intercept an existing conversation or data transfer by pretending to be a legitimate end user
Spoofing	Intruders act as trusted contacts to access systems and infect them with malware, steal data, cause damage and disruption.
Snifing	Intruders capture network packets to intercept or steal data that may be unencrypted.

Table 5 - resume of the attacks

Normally we can cite almost all the references on the topic of this item, since the methodology used revolves around them, so the solutions highlighted denote possible flaws and/or improvements in the report issued.

The 5G standard arises from several innovations, one of which is softwarezation and virtualization, in which the security mechanisms of traditional Data Center, VPN and Firewall systems provoke validations and studies of more robust security mechanisms [4], [5], [11], [28], [29], [30].

New program models for better connectivity and operationalization between edges [26], demonstrate the need to implement mitigations or improvements to risks identified in this standard.

Methodologies and processes being evaluated for authentication, even for 5G architecture, highlight the need for mitigation and security validity [22].

The composition of a heterogeneous architecture composed and developed to support numerous complex interaction services (IoT devices, Vehicle Systems) causes the use of various data security mechanisms [12],[14], [21], [22], [23], [25], [26].

Em uma avaliação mais aprofundada sobre todas as camadas desse padrão, pode-se quantificar e também exemplificar mecanismos de intrusão, avaliação e auditoria, demonstrando implicitamente os quesitos de segurança, probabilidades de riscos existentes no 5G [30].

Based on the models and types of acquisition, distribution and connections necessary in the 5G architecture, as seen in figure 4, to compose the deliveries provided in the triangle of functionalities seen in figure 3, it is necessary to implement security mechanisms [3], [11], [12], [14].

Considering the applications, encryption protocols, authentication modeling, blockchain to create security and/or mitigate risks, all mitigation and control techniques used in cloud computing are used, with virtualization complicating how to use these methodologies together [22], [25], [26], [27], [28], [29], [30].

It should be noted that 5G necessarily requires infinite or constant growth in processing and control algorithms to provide all this interactivity, requiring the implementation of quantum computing for security improvements. [23].

The need for multiple services, with shared modeling, fixed, mobile, various control protocols interacting simultaneously with each other and with other networks, we have with quantum computing a reliable alternative to provide security (encryption) in real time in comparison with traditional methods encryption [23].

When we observe the development of the ISO-IEC standard, it is clear that it is now involving 5G for development and deployment [7].

Since the vision of this standard goes from control groups to thematic areas, 5G architecture is fully applicable, as it is focused on layer 7 of the OSI standard, that is, services.

The new controls implemented in this 2022 version, I mention a few: 5.7, 5.23, 5.30; 7.4; 8.9; 8.12, 8.16, 8.23, which compared to the 5G standard demonstrates a gap to be filled and reviewed to ensure security and mitigations.

5G and Artificial Intelligence (AI) begin to bring new security challenges, but mainly about ethics, which must increasingly be observed, parameterized and mainly audited [9].

The need to use AI to improve the 5G system must have ethical guidelines respected, thus having ethical deliberations for use and implementation in 5G, which is currently still in experimentation and knowledge of this new technology applied to any technology [9].

Regarding predictions as indicated by Gartner, the importance of Ethics together with softwarelization and virtualization is clearly noted, as AI presents credibility problems together with the 75% adoption of cloud computing [8].

4. Discussion

This report, based on the applied and adapted methodology, sought to generate material to understand conditions to respond to its object in a restricted and contained way, observing the themes of the revisited literature, we can see that 5G technology lacks credibility in terms of security.

All literature, even restricted in this analysis, demonstrate improvements or proposed solutions for perceived problems regarding performance, capacity, authentication, integration and/or deployment.

The services themselves imply a better ability to mitigate risks, implement improvements to guarantee integrity and thus security, highlighting the exchange of information between: networks, users, equipment, protocols and security system must be widely studied for minimum necessary, but real protection and not theoretical.

One of the improvements, entering the evolution of the standard, is the adoption of AI, which in itself suffers from credibility, ethical standards and is thus another element of high complexity for its security and its interactions throughout these systems and their services.

But it is still clear that this new approach is still new, having to be developed and perfected, but it demonstrates that the 5G system in its complexity has gaps to be filled with better encryption mechanisms, control and increasingly shorter processing time. .

As we can see the importance of security validation, risks and mitigations were one of the motivators for updating the IEC-IEC 27001-2022 standard [7], and this validation compared with the models proposed in 5G, we have to note that it lacks application the same in order to guarantee better data protection, privacy and cyber security.

As a recommendation, the security requirement should be adopted as the Kernel of the technology and not the act underlying the introduction of “N” technology and its “N” interactions to determine a standard.

As a suggestion, we suggest discussing security in mobile systems, and does it have to be included or overwritten to the triangle of 5G applications (figure 2) offered by ITU-R IMT 2020 requirements?”.

5. Acknowledgements

I thank the one who never leaves me alone, to God and my family who always support me and believe that every day, every act is a path of learning for my evolution.

To my teachers who are always available to guide, explain and make my knowledge more comprehensive and clear, thus allowing me to constantly evolve towards my goal.

Not forgetting my study partners, classmates who were always available to help understand the challenges that arose and thus overcome them.

6. References

[1] "Physical Layer Techniques for 5G Wireless Security", em 5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management, IEEE, 2018, p. 237–274. doi: 10.1002/9781119333142.ch6.

[2] 3GPP. "Specifications & Tecnologie Release 15". Internet: https://www.3gpp.org/specifications-technologies/releases/release-15, Apr. 26, 2019 [Dez. 08, 2023].

[3] M. Hoffmann *et al.*, "Open RAN xApps Design and Evaluation: Lessons Learnt and Identified Challenges", *IEEE Journal on Selected Areas in Communications*, p. 1–1, 2023, doi: 10.1109/JSAC.2023.3336190.

[4] A. Khichane, I. Fajjari, N. Aitsaadi, e M. Gueroui, "5GC-Observer Demonstrator: a Non-intrusive Observability Prototype for Cloud Native 5G System", em *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, may 2023, p. 1–3. doi: 10.1109/NOMS56928.2023.10154369.

[5] A. Khichane, I. Fajjari, N. Aitsaadi, e M. Gueroui, "5GC-Observer: a Non-intrusive Observability Framework for Cloud Native 5G System", em *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, maio 2023, p. 1–10. doi: 10.1109/NOMS56928.2023.10154433.

[6] PRISMA. "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)". Internet: http://www.prisma-statement.org/, 2023 [Nov. 25, 2023].

[7] ISO-IEC. "Information security, cybersecurity and privacy protection — Information security management systems — Requirements", ISO-IEC / 27001, 3rd edition, Oct. 2022, doi: https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC-27001-2022.pdf.

[8] Gartner. "*The Gartner 100 Data Analytics Predictions Trough 2028*". Internet: https://www.gartner.com/en/webinar/498422/1165682, 2023 [Nov. 23, 2023]

[9] E. Goffi, "*Operatinalizing Ethics in the Digital: How to go beyond good intentions?*", em *Lisbon Data & IA Forum, 2023*, October 2023.

[10] Cloudfare. "*What is OSI Model?*", Internet: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, 2023 [Dez. 16, 2023].

[11] S. Kota *et al.*, "Satellite", em *2022 IEEE Future Networks World Forum (FNWF)*, out. 2022, p. 1–182. doi: 10.1109/FNWF55208.2022.00141.

[12] A. S. Abdalla e V. Marojevic, "Security Threats and Cellular Network Procedures for Unmanned Aircraft Systems: Challenges and Opportunities", *IEEE Communications Standards Magazine*, vol. 6, nº 4, p. 104–111, dez. 2022, doi: 10.1109/MCOMSTD.0003.2100108.

[13] A. Sharma, A. Jain, e I. Sharma, "Exposing the Security Weaknesses of Fifth Generation Handover Communication", em *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, jul. 2019, p. 1–6. doi: 10.1109/ICCCNT45670.2019.8944864.

[14] V. Sharma, I. You, e N. Guizani, “Security of 5G-V2X: Technologies, Standardization, and Research Directions”, *IEEE Network*, vol. 34, nº 5, p. 306–314, set. 2020, doi: 10.1109/MNET.001.1900662.

[15] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, e F. Martinelli, “Privacy for 5G-Supported Vehicular Networks”, *IEEE Open Journal of the Communications Society*, vol. 2, p. 1935–1956, 2021, doi: 10.1109/OJCOMS.2021.3103445.

[16] A. Feraudo, A. Calvio, A. Bujari, e P. Bellavista, “A Novel Design for Advanced 5G Deployment Environments with Virtualized Resources at Vehicular and MEC Nodes”, em *2023 IEEE Vehicular Networking Conference (VNC)*, abr. 2023, p. 97–103. doi: 10.1109/VNC57357.2023.10136327.

[17] R. Palisetty *et al.*, “Area-Power Analysis of FFT Based Digital Beamforming for GEO, MEO, and LEO Scenarios”, em *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, jun. 2022, p. 1–5. doi: 10.1109/VTC2022-Spring54318.2022.9861037.

[18] P. Kryszkiewicz e M. Hoffmann, “Open RAN for detection of a jamming attack in a 5G network”, em *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, jun. 2023, p. 1–2. doi: 10.1109/VTC2023-Spring57618.2023.10201067.

[19] J. Wen, J. Weng, Y. Fang, H. Gacanin, e W. Luo, “Novel Properties of Successive Minima and Their Applications to 5G Tactile Internet”, *IEEE Transactions on Industrial Informatics*, vol. 15, nº 5, p. 3068–3076, maio 2019, doi: 10.1109/TII.2019.2895089.

[20] A. Manan, Z. Min, C. Mahmoudi, e V. Formicola, “Extending 5G services with Zero Trust security pillars: a modular approach”, em *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, dez. 2022, p. 1–6. doi: 10.1109/AICCSA56895.2022.10017774.

[21] R. Solozabal, J. Ceberio, A. Sanchoyerto, L. Zabala, B. Blanco, e F. Liberal, “Virtual Network Function Placement Optimization With Deep Reinforcement Learning”, *IEEE Journal on Selected Areas in Communications*, vol. 38, nº 2, p. 292–303, fev. 2020, doi: 10.1109/JSAC.2019.2959183.

[22] N. Wehbe, H. A. Alameddine, M. Pourzandi, E. Bou-Harb, e C. Assi, “A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture”, *IEEE Communications Magazine*, vol. 61, nº 1, p. 48–54, jan. 2023, doi: 10.1109/MCOM.001.2200183.

[23] M. Mehic *et al.*, “Quantum Cryptography in 5G Networks: A Comprehensive Overview”, *IEEE Communications Surveys & Tutorials*, p. 1–1, 2023, doi: 10.1109/COMST.2023.3309051.

[24] A. M. Romanov, F. Gringoli, K. Alkhouri, P. E. Tripolskiy, e A. Sikora, “Enabling Time-Synchronized Hybrid Networks With Low-Cost IoT Modules”, *IEEE Internet of Things Journal*, vol. 10, nº 11, p. 9966–9978, jun. 2023, doi: 10.1109/JIOT.2023.3235052.

[25] L. Xie, Y. Ding, H. Yang, e X. Wang, “Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs”, *IEEE Access*, vol. 7, p. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.

[26] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, e P. Castoldi, “P4 Edge node enabling stateful traffic engineering and cyber security”, *Journal of Optical Communications and Networking*, vol. 11, nº 1, p. A84–A95, jan. 2019.

[27] P.-H. Tseng, M.-H. Lee, Y.-H. Lin, H.-L. Lung, K.-C. Wang, e C.-Y. Lu, “ReRAM-Based Pseudo-True Random Number Generator With High Throughput and Unpredictability Characteristics”, *IEEE Transactions on Electron Devices*, vol. 68, nº 4, p. 1593–1597, abr. 2021, doi: 10.1109/TED.2021.3057028.

[28] Y.-C. Cheng e C.-A. Shen, “A New Tracking-Attack Scenario Based on the Vulnerability and Privacy Violation of 5G AKA Protocol”, *IEEE Access*, vol. 10, p. 77679–77687, 2022, doi: 10.1109/ACCESS.2022.3193372.

[29] S. Gupta, B. L. Parne, e N. S. Chaudhari, “Security Vulnerabilities in Handover Authentication Mechanism of 5G Network”, em *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, dez. 2018, p. 369–374. dot: 10.1109/ICSCCC.2018.8703355.

[30] A. Nieto, “An Overview of Proactive Forensic Solutions and its Applicability to 5G”, em *2018 IEEE 5G World Forum (5GWF)*, jul. 2018, p. 191–196. doi: 10.1109/5GWF.2018.8516940.