General Aspects of Information Security in 5G Networks: Survey

VITOR ORIEL DE CASTRO NUNES BORGES[1]
RENATA LOPES ROSA[2]

Department of Computer Science
Federal University of Lavras
vitor.borges1@estudante.ufla.br

Abstract. As the deployment of 5G networks accelerates, ensuring robust security becomes paramount. This article presents a comprehensive review of security in 5G networks, aiming to analyze security applications and strategies for mitigating vulnerabilities. Through an extensive literature review, several threats and specific security vulnerabilities of 5G networks are identified as issues in corporate networks, user equipment, and applications. Furthermore, possible future security trends, vulnerability mitigations, and emerging technologies in 5G networks are explored. The article concludes by highlighting the importance of addressing security concerns in 5G networks and provides recommendations for future research in this field. Understanding the security landscape of 5G networks is crucial to ensuring the safe and reliable operation of next-generation communication infrastructure.

Keywords: 5G networks, security, network security, attacks

(Received May 12th, 2023 / Accepted June 30th, 2023)

1 Introduction

The fifth generation (5G) of wireless mobile communication networks has emerged as a transformative technology, with the initial standard proposal made by the Third Generation Partnership Project (3GPP), revolutionizing the way we connect, communicate, and interact in the digital era [3, 2, 7, 11]. With its promise of ultra-fast speeds, low latency, massive device connectivity, and enhanced reliability [35], 5G networks are poised to drive the deployment of innovative applications and services across various domains, including healthcare, transportation, smart cities, augmented reality, and industrial automation [20, 22].

The 5G network enables a wide variety of terminals and a significant increase in the number of nodes, extensive deployment of nodes in ultra-high density, the coexistence of multiple wireless network technologies, and security mechanisms [23, 33, 18]. The 5G network allows for the evolution of end-to-end direct communication capabilities and the integration of innovative techniques such as Vehicle-to-everything (V2X), Software Defined Network (SDN), and Network Functions Virtualization (NFV). These new features and techniques pose several new security challenges for 5G networks [6, 23]. Despite the evolution of technical aspects of communication and security, it is essential to educate people about the importance of information security in 5G networks [27, 29, 21, 28].

In this paper, we present the general aspects of security in a 5G network. For this purpose, the paper is organized as follows: Section 2 provides a summary of the existing works on information security in 5G networks. Section 3 presents the criteria and methods of analysis used in this study, and Section 4 analyzes and discusses the security issues found in the literature.

2 Related Work

The security architecture in 5G networks is a crucial topic to ensure the protection of systems and data in an increasingly connected environment. The work [24] provides a review of the 5G-IoT architecture, presenting the attacks and cyber risks at each layer of this ar-

chitecture. Its objective is to propose a security taxonomy for this type of network, focusing on the threats highlighted in its layers, in the context of applications in smart cities. The authors argue that the proposed architecture can address different security challenges and provide forensic techniques to prevent potential risks and cyber attacks in the network.

In the article [13], the security requirements and applicable standards for 4G and 5G wireless networks were synthesized. Specifically, it presented security aspects in the LTE and 5G wireless systems developed by the 3GPP group. It emphasizes the importance of LTE security requirements in 5G wireless systems and highlights the need to protect privacy. The article [4] presents a comprehensive study on security in 5G networks, under the 5G-NextGen Core (5GC) architecture. It introduces cyber risks and security measures along with use cases applied to this architecture, including requirements such as authentication, integrity, availability, non-repudiation, and confidentiality. The article [15] provides insights into the integration of innovative devices, 5G networks, and security through case studies in vehicular-to-everything (V2X) network scenarios.

The article [32] describes the work carried out in the 5G-ENSURE project to address the need for security and reliability in enterprise networks using 5G. With the aim of developing a trust model in 5G networks in the corporate environment, it worked with a scenario involving various reliability mechanisms. On the other hand, the article [14] presents a comprehensive study on the security of 5G wireless network systems compared to 4G cellular network, highlighting the security risks and tradeoffs in each of these architectures. The work [19] analyzes the security features of 5G and measures their implementation in commercial 5G networks. The results show that there is a significant discrepancy between 5G security standards and real-world deployment, with vulnerabilities such as user data leakage, location exposure, and denial-of-service (DoS) attacks still applicable to commercial 5G networks. The article [1] presents a framework for the management and monitoring of security events in 5G networks, including the solution architecture, related works, and use cases.

The work [12] presents a comprehensive study on recent developments in 5G wireless security, focusing on existing security solutions and emerging security aspects associated with technologies such as HetNet, D2D, massive MIMO, SDN, and IoT. It proposes a 5G wireless security architecture that emphasizes flexible identity management and authentication, highlighting its advantages. The article examines the handover procedure and performance to demonstrate the benefits of the proposed security architecture. Additionally, it discusses the challenges and future directions of 5G wireless security, aiming to provide research directions for implementing robust security measures in the near future.

Evaluating the security of a 5G network is similar to analyzing a conventional network, where it is necessary to capture the traffic and analyze it afterward. Just as in a conventional network, we can use the fuzzing technique [5], and we can also apply the same principles to a 5G network [30]. In the research article [34], a survey provides an overview of system models, including network and threat models, in the context of the 5G-enabled IoT environment.

The analysis of different 5G networks and operators allows the identification of deployment issues, authentication, privacy, confidentiality, capabilities, and data transfer [16]. The research [25] categorizes different types of security protocols and provides an analysis of existing protocols in the 5G-enabled IoT environment. Additionally, it highlights future challenging issues in the security of the 5G-enabled IoT environment, offering valuable insights for researchers in this field.

The existence of entities such as 3GPP facilitates the creation of standards that establish the operating criteria of the 5G network. However, problems can still occur within these standards. The research study [9] analyzed the authentication mechanism and proposed improvements to the implemented algorithm to prevent data leaks and encryption breakage used in USIM [1]. Another research study [17] analyzed the network band slicing mechanism and proposed an algorithm to prevent data leaks.

Security analyses in 5G networks are not limited to the network infrastructure alone but also encompass the applications that utilize the 5G network for communication. The research study [8] analyzed the security of IoT devices that transmit data over the 5G network, considering that these devices have limited processing capabilities and need to conserve energy. The work [10] developed a secure authentication protocol for 5G networks that protects the network against attacks involving quantum computing, providing stronger security than the standard protocol. The article [26] addresses security vulnerabilities in major use cases based on 5G networks, deployed in the context of Multi-access Edge Computing (MEC), as well as strategies to mitigate them.

The article [31] provides an overview of Cellular Vehicle-to-Everything (C-V2X) technologies and stan-

[1] USIM `https://www.ericsson.com/en/blog/2020/1/5g-security-sim-card`

dards, with a specific focus on the current status of LTE-V2X and 5G-V2X. It explores various use cases, service support, and security requirements associated with these technologies. A comparison is made to highlight issues related to existing implementations of 5G-V2X in autonomous and non-autonomous modes. The article presents an architecture based on a conceptualized Security Reflexive Function (SRF), designed to mitigate secure mobility management challenges faced by vehicles in 5G-V2X. Additionally, it discusses open issues and research directions, shedding light on the current aspects of 5G-V2X, its security, and the feasibility of the proposed architecture.

3 Methodology

The objective of this survey is to provide a comprehensive overview of the existing literature on security studies in 5G networks. The aim is to identify and analyze the current state of research, highlight the key challenges and threats, and explore the various security mechanisms and solutions proposed by researchers and industry experts.

This survey paper adopts a systematic approach to conducting a comprehensive review of the literature on security in 5G networks. The following steps were followed:

- Identification of Relevant Keywords: The initial step involved identifying relevant keywords related to the subject. These keywords included "5G networks," "security," "threats," "challenges," "security mechanisms," and "solutions.".
- Literature Search: A thorough literature search was conducted using various academic databases, including IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar. The search was conducted using a combination of the identified keywords to retrieve relevant research articles, conference papers, reports, and other scholarly sources.
- Inclusion and Exclusion Criteria: In order to ensure the relevance and quality of the selected literature, inclusion, and exclusion criteria were defined. Only peer-reviewed articles, conference papers, and reports published between 2018 and 2023 were considered.
- Screening and Selection Process: The retrieved articles were screened based on their titles and abstracts to assess their relevance to the research topic. The selected articles were then read in detail to evaluate their suitability for inclusion in the survey paper. The final selection of articles was made based on their relevance, contribution to the field, and quality of the research.
- Data Extraction and Analysis: The selected articles were systematically reviewed, and relevant information was extracted. The extracted data included the authors, publication year, research focus, key findings, methodologies, and recommendations. The data were analyzed to identify common themes, emerging trends, and gaps in the existing research.
- Limitations: It is important to acknowledge the limitations of this survey paper. The scope of the survey is limited to the literature available up to June 2023. The inclusion and exclusion criteria may introduce some bias in the selection of articles. Additionally, due to the rapid development of 5G networks, new research may have been published after the literature search was conducted.

As a result of applying the methods described above, we obtain Table 1, with some criteria used in the research to facilitate the classification of the works. In Table 1, the keyword refers to the most evident points along with the security theme, the field work is used to identify the referenced work, and the field year is used to identify the year of publication.

Subject	Papers	Year
Architecture and design	[24][13][4]	2018
	[15]	2023
Attacks to 5G networks	[30]	2021
	[16][25]	2023
Physical security	[9][17][8]	2023
Vehicle to everything (V2X)	[31]	2020
	[26]	2021
	[15]	2023

Table 1: Papers separated by subjects

4 Conclusion

This survey provided a comprehensive overview of the current state of research on security in 5G networks. Through a systematic analysis of the literature, the main challenges and threats associated with 5G network security were identified, and existing security mechanisms and solutions proposed by researchers were ex-

plored. The analysis of the selected works shows a trend of studying 5G network security in conjunction with other topics, thus evaluating more practical applications of the established 5G network standards. This approach allows for research that maps other areas of knowledge, expanding the results and possibilities for developing new applications and analyses. Although significant progress has been made in the development of security mechanisms, there are still gaps and research directions that need to be addressed.

Future research should focus on investigating the security implications of emerging technologies in 5G networks, such as network slicing and edge computing. Additionally, efforts should be directed towards standardization and regulatory frameworks to ensure consistent and robust security measures in 5G deployments. However, it is essential to recognize the limitations of this survey. The article selection process may introduce some bias, and there are various research papers that were not included. Furthermore, the rapid development of 5G networks means that new security challenges may arise, requiring ongoing research and updates to address emerging threats. Despite these limitations, this survey article provides a valuable foundation for understanding the current landscape of security in 5G networks and highlights the need for continuous research and collaboration to ensure the secure deployment and operation of 5G networks in the future.

References

[1] Adam, I. and Ping, J. Framework for security event management in 5g. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery.

[2] Al-Falahy, N. and Alani, O. Y. Technologies for 5g networks: Challenges and opportunities. *It Professional*, 19(1):12–20, 2017.

[3] Alain Sultan, M. 5g system overview, 2023.

[4] Amgoune, H. and Mazri, T. 5g: Interconnection of services and security approaches. In *Proceedings of the 3rd International Conference on Smart City Applications*, SCA '18, New York, NY, USA, 2018. Association for Computing Machinery.

[5] Borges, V. and UchÃ´a, J. Fuzzingtool: Ferramenta para testes de intrusao em aplicacoes web. In *Anais do XXI Simposio Brasileiro em Seguranca da Informacao e de Sistemas Computacionais*, pages 391–396, Porto Alegre, RS, Brasil, 2021. SBC.

[6] Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., and Xiong, L. A survey on security aspects for 3gpp 5g networks. *IEEE Communications Surveys Tutorials*, 22(1):170–195, 2020.

[7] Carrillo, D., Kalalas, C., Raussi, P., Michalopoulos, D. S., Rodríguez, D. Z., Kokkoniemi-Tarkkanen, H., Ahola, K., Nardelli, P. H., Fraidenraich, G., and Popovski, P. Boosting 5g on smart grid communication: A smart ran slicing approach. *IEEE Wireless Communications*, 2022.

[8] Cook, J., Rehman, S. U., and Khan, M. A. Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions. *IEEE Access*, 2023.

[9] Cui, Z., Cui, B., Su, L., Du, H., Wang, H., and Fu, J. Attacks against security context in 5g network. *arXiv preprint arXiv:2303.10955*, 2023.

[10] Damir, M. T., Meskanen, T., Ramezanian, S., and Niemi, V. A beyond-5g authentication and key agreement protocol, 2022.

[11] dos Santos, M. R., Batista, A. P., Rosa, R. L., Saadi, M., Melgarejo, D. C., and Rodríguez, D. Z. Asqm: Audio streaming quality metric based on network impairments and user preferences. *IEEE Transactions on Consumer Electronics*, 2023.

[12] Fang, D., Qian, Y., and Hu, R. Q. Security for 5g mobile wireless networks. *IEEE access*, 6:4850–4874, 2017.

[13] Fang, D., Qian, Y., and Hu, R. Q. Security requirement and standards for 4g and 5g wireless systems. *GetMobile: Mobile Comp. and Comm.*, 22(1):15â20, may 2018.

[14] Hanane, O. and Tomader, M. 4g and 5g: Security and privacy analysis. In *Proceedings of the 4th International Conference on Big Data and Internet of Things*, BDIoT'19, New York, NY, USA, 2020. Association for Computing Machinery.

[15] Imbruglia, A., Cancila, D., and Settembre, M. 5g communication and security in connected vehicles. *Ada Lett.*, 42(2):109â113, apr 2023.

[16] Lasierra, O., Garcia-Aviles, G., Municio, E., Skarmeta, A., and Costa-Pérez, X. European 5g security in the wild: Reality versus expectations. *arXiv preprint arXiv:2305.08635*, 2023.

[17] Li, X., He, M., and Ni, J. Secure and privacy-preserving network slicing in 3gpp 5g system architecture. *arXiv preprint arXiv:2305.17524*, 2023.

[18] Melgarejo, D. C., Da Costa Filho, L. Q. R., De Medeiros, Á. A. M., Neto, C. L., Figueiredo, F. L., and Rodríguez, D. Z. Dynamic algorithm for interference mitigation between cells in networks operating in the 250 mhz band. *IEEE Access*, 10:33803–33815, 2022.

[19] Nie, S., Zhang, Y., Wan, T., Duan, H., and Li, S. Measuring the deployment of 5g security enhancement. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '22, page 169â174, New York, NY, USA, 2022. Association for Computing Machinery.

[20] Ogobuchi, O. D., Vieira, S. T., Saadi, M., Rosa, R. L., and Rodríguez, D. Z. Intelligent network planning tool for location optimization of unmanned aerial vehicle base stations using geographical images. *Journal of Electronic Imaging*, 31(6):061822–061822, 2022.

[21] Okey, O. D., Maidin, S. S., Adasme, P., Lopes Rosa, R., Saadi, M., Carrillo Melgarejo, D., and Zegarra Rodríguez, D. Boostedenml: Efficient technique for detecting cyberattacks in iot systems using boosted ensemble machine learning. *Sensors*, 22(19):7409, 2022.

[22] Parnianifard, A., Rodriguez, D. Z., Mumtaz, S., Wuttisittikulkij, L., et al. Speech emotion recognition using anfis and pso-optimization with word2vec. 2022.

[23] PINTO, G. E., Rosa, R. L., and Rodriguez, D. Z. Applications for 5g networks. *INFOCOMP Journal of Computer Science*, 20(1), 2021.

[24] Rahimi, H., Zibaeenejad, A., Rajabzadeh, P., and Safavi, A. A. On the security of the 5g-iot architecture. In *Proceedings of the International Conference on Smart Cities and Internet of Things*, SCIOT '18, New York, NY, USA, 2018. Association for Computing Machinery.

[25] Ramezanpour, K., Jagannath, J., and Jagannath, A. Security and privacy vulnerabilities of 5g/6g and wifi 6: Survey and research directions from a coexistence perspective. *Computer Networks*, 221:109515, 2023.

[26] Ranaweera, P., Jurcut, A., and Liyanage, M. Mec-enabled 5g use cases: A survey on security vulnerabilities and countermeasures. *ACM Comput. Surv.*, 54(9), oct 2021.

[27] Ravishankar, V. and Marshall, A. M. Teaching an undergraduate 5g technology and security course, and its outcomes. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*, SIGCSE 2023, page 1405, New York, NY, USA, 2023. Association for Computing Machinery.

[28] Ribeiro, D. A., Melgarejo, D. C., Saadi, M., Rosa, R. L., and Rodríguez, D. Z. A novel deep deterministic policy gradient model applied to intelligent transportation system security problems in 5g and 6g network scenarios. *Physical Communication*, 56:101938, 2023.

[29] Saadi, M., Bajpai, A., Rodriguez, D. Z., and Wuttisittikulkij, L. Investigating the role of channel state information for mimo based visible light communication system. In *2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, pages 1–4. IEEE, 2022.

[30] Salazar, Z., Nguyen, H. N., Mallouli, W., Cavalli, A. R., and Montes de Oca, E. 5greplay: A 5g network traffic fuzzer - application to attack injection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES 21, New York, NY, USA, 2021. Association for Computing Machinery.

[31] Sharma, V., You, I., and Guizani, N. Security of 5g-v2x: Technologies, standardization, and research directions. *IEEE Network*, 34(5):306–314, 2020.

[32] Surridge, M., Correndo, G., Meacham, K., Papay, J., Phillips, S. C., Wiegand, S., and Wilkinson, T. Trust modelling in 5g mobile networks. In *Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges*, SecSoN '18, page 14â19, New York, NY, USA, 2018. Association for Computing Machinery.

[33] Teodoro, A. A., Gomes, O. S., Saadi, M., Silva, B. A., Rosa, R. L., and Rodríguez, D. Z. An fpga-based performance evaluation of artificial neural network architecture algorithm for iot. *Wireless Personal Communications*, pages 1–32, 2021.

[34] Wazid, M., Das, A. K., Shetty, S., Gope, P., and Rodrigues, J. J. Security in 5g-enabled internet of things communication: issues, challenges, and future research roadmap. *IEEE Access*, 9:4466–4489, 2020.

[35] Ziegler, V., Wild, T., Uusitalo, M., Flinck, H., Räisänen, V., and Hätönen, K. Stratification of 5g evolution and beyond 5g. In *2019 IEEE 2nd 5G World Forum (5GWF)*, pages 329–334. IEEE, 2019.