5G Security Issues Challenges and Solutions Against DDoS Attacks:A Survey

Sharma Ji
Research Scholar
Computer Science and Engineering
IFTM University
Moradabad, India
saurabh12d@gmail.com

Dr. Abhishek Kumar Mishra
Associate Professor
Computer Science and Engineering
IFTM University
Moradabad, India
abhimishra2@gmail.com

2024 2nd International Conference on Disruptive Technologies (ICDT) | 979-8-3503-7105-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICDT61202.2024.10489295

***Abstract*—The Fifth Generation of Communications Networks (5G) is projected to greatly develop wireless cellular networks by delivering quicker speed, higher capacity, and lower latency. It is expected to significantly alter both important industries and national economies. It has acquired wide recognition throughout the world. Despite the data integrity, confidentiality, and availability that 5G service providers provide, security is still a serious problem that requires immediate attention. To help customers, service providers, and researchers better understand the network, this article offers a thorough overview of 5G security problems, typical attacks, security services, and concerns. It also includes a case study.**

***Index Terms*—Fifth Generation (5G), Cellular network, Wireless Communication, Capacity, Security Issues, Latency.**

I. Introduction

5G wireless networks enable new gadgets for the Internet of Things and machine-to-machine communication [1], and Cyber-Physical Systems by providing higher QoS, more coverage, and low latency. In order to meet consumer traffic demands, they integrate innovative technologies to deliver dependable and reasonably priced internet connectivity. However, considering that wireless networks have posed a significant security risk ever since their inception, robust security measures are essential with 5G networks [2]. Due to the wide variety of possibilities of 5G, nearly every asset of human activity will be able to connect to communication networks, emphasizing the importance of having strong security measures in place throughout the entire 5G network. Since their beginnings, wireless networks have been a key source of security issues.

It was discovered that 1G mobile networks were vulnerable to issues such as cloning, impersonating, and illegal interception [3]. Inappropriate marketing, false information, and message spamming all grew on second-generation (2G) mobile networks. Due to problems with IP-based connectivity, Third Generation (3G) experienced substantial disruption. In fourth-generation (4G) networks, IP-based communication increases complexity. Security concerns are anticipated to worsen when 5G applications, such as smart homes, electric grid systems, transportation, and hospitals, become more widely available.

The sector has been greatly impacted by the new services and technology's quick evolution, security techniques from3G and 4G are not applicable for 5G. While sharing in- compatible services, virtualization and multi-tenancy share thesame mobile network architecture. For 5G networks, security architectures from earlier generations are too simplistic, and radio bearer and hop-by-hop techniques shouldn't be used.

This article looks at the current state of 5G network security. First, the security flaws and corresponding remedies for the 1G through 4G network generations are discussed. Next, a detailed analysis of the 5G technologies is conducted with respect to the security risks they pose and the associated remedies. This article contains information regarding next-generation (XG) security in 5G and beyond communication networks. The essay's remaining section is organized as follows: Section II provides an overview of security in previous generations of wireless cellular networks. In contrast, Section III provides a thorough analysis of security in 5G networks. The security issues and suggested solutions for 5G networks are discussed in Section IV. Due to their impact on the core and backhaul networks, these challenges and their solutions are categorised. while security solutions are presented in Section V. In Section VI privacy-related issues are covered along with possible fixes. In order to address current vulnerabilities and upcoming security difficulties in communication networks, Section VII highlights future characteristics of network security. The paper is concluded in Section VIII.

II. Related work

The goal of the 5G network, which aims to provide universal connectivity with less than 1 millisecond of latency and gigabit speeds, and it has made significant progress toward fruition. In comparison to 4G systems, the 5G network isintended to offer very high data throughput, very little latency,

TABLE I THE RECENT GROWTH OF TECHNOLOGY

Generations	1G	2G	3G	4G	5G
Installation	1970-1980	1990-2004	2004-2010	2010-2020	Now
Data Bandwidth	2Kbps	64Kbps	2Mbps	1Gbps	More than 1Gbps
Technology	AMPS, TACS ,NMT	GPRS/GSM,cdmaOne, D-AMPS	HSPA+/WCDMA,EV-DO/TD-SCDMA/CDMA2000	Advanced LTE,LTE	Not yet standardized
Crucial Distinction	Mobility	Mass adoption,Secure	Better internet,Applications, Experience	Lower latency,Faster broadband internet	Faster internet,Wide range of applications,IoT
Services	Voice	Digital Voice,SMS, Higher capacity packetized data	Video and data, Cohesive high-class audio	Wearable devices, Dynamic information access	Wearable devices with AI capabilities ,Dynamic information access
Core network	PSTN	PSTN	Packet Network	Internet	Internet
Weakness	Major security concerns, Poor spectral efficiency	Narrow data rates, challenging to support requests for e-mail	Failure of WAP for internet access, Real performance failed to match the hype, Tied to legacy	Mobile explicit architecture and protocols	Infrastructure,Privacy, Security, etc

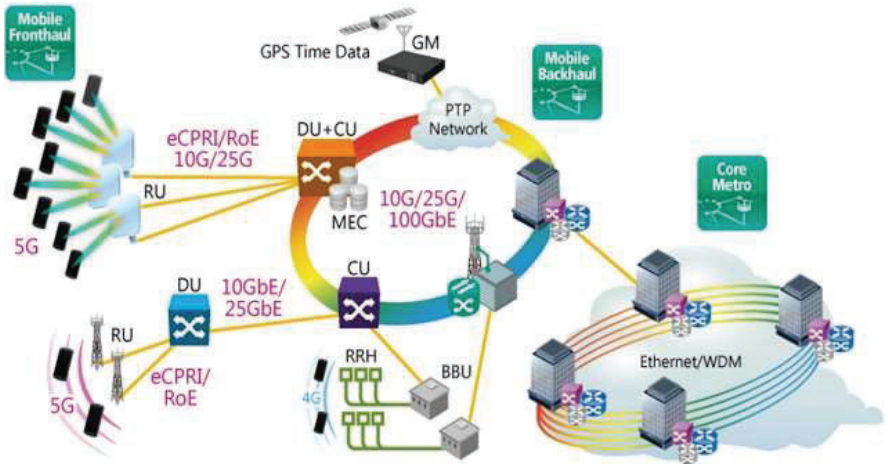

Fig. 1. Network Architecture of 5G [4].

greatly increased capacity, base station density, and significantly improved quality of service [5]. Several survey papers go into great detail about 5G networks, including references. To protect networked systems, users, and the network itself, major efforts are required due to the anticipated impact of 5G security on daily life. The restrictions of 4G and methods to transition to 5G while overwhelming these restrictions are covered in [6]. Latency, the restricted processing power of base stations, and the absence of methods to facilitate data traffic surges are security-related 4G issues that, if not directlyharm, at least indirectly do so. If these restrictions are not eliminated, the network will be vulnerable to security issues. For instance, spikes in data traffic may occur for valid causes, such as crowd movements, or for other reasons, such as DoS attack. Comparably, in ultra-dense 5G networks, the limited base station may cause issues with availability for authorized users or act as a point of entry for attacks that deplete resources. The same goes for latency, which might cause issues when communicating between vehicles using the Vehicle to Everything (V2X) protocol. As a result, the survey [6] offers some intriguing perspectives on the existing shortcomings of the 4G network and how 5G will address them.

There are general specifications and procedures for enhancing security in 5G presented in [7]. The authors provide an in-depth analysis of the 5G security needs, focusing on the most modern techniques for both 4G and 5G network authentication and privacy preservation. In addition to standardization initiatives in 4G and previous generations, security issues and potential mitigation measures are addressed. This article surveys threats to mobile networks' security. The study's key subjects are the security dangers and challenges that mobile access and core networks face. However, the 4G network architecture poses the most challenges.

The author offers solutions needing automation and context awareness to address the security issues presented by new technologies including 5G networks,NFV, SDN, MEC, and

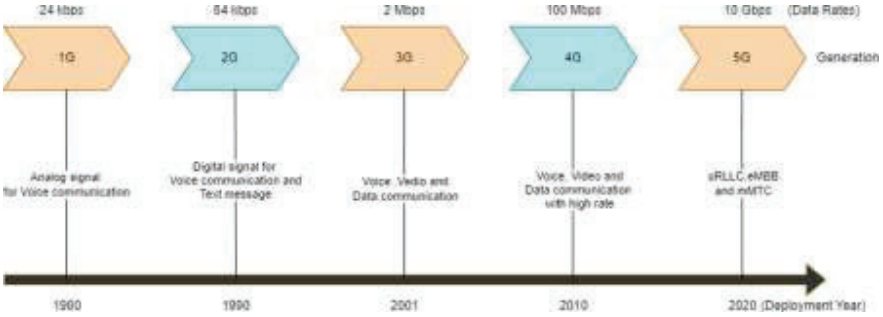

Fig. 2. From 1G to 5G, the evolution of wireless communication.

massive MIMO. It also discusses protecting XG societies employing disruptive technologies like AI, blockchain, and UAVs as well as security in IoT-enabled contexts, including smart cities.

III. SECURITY IN 5G: AN OVERVIEW

In addition to offering ubiquity in internet services and enabling enormous IoT device connectivity, 5G will also entertain people and high-mobility devices that are also incredibly dependable and economically priced [8]. The advancements in IP-based communication made possible by 4G are built upon for 5G, a new ecosystem combining all facets of so- ciety. However, it challenges present and future networks by presenting new security flaws and dangers. Infrastructures like the electrical grid are vulnerable to security breaches that could have disastrous effects. Security for 5G must therefore be taken into account throughout design.

A. General Overview of Security in 5G

The Next Generation Mobile Networks (NGMN) have published suggestions for 5G based on existing network designs and security mechanisms [9]. The proposals draw attention to the fact that 5G is still in its infancy, full of unknowns, without clear design ideas, and end-to-end and subsystem architectures. They place a focus on access network security issues, online attacks on users and network infrastructure, and the requirement for effective management of significant fluctuations in traffic volume.

DoS attacks on the Infrastructure: The functioning of critical infrastructure, such as that for the delivery of energy, healthcare, transportation, and communications networks, may be disrupted by Distributed DoS (DDoS) and DoS attacks. DoS attacks are frequently designed to exhaust all of the physical and intellectual resources of the targeted machine. Because of worries about possible attacks from numerous, geographically dispersed, and extensively dispersed IoT devices, this threat will be more significant.

IV. SECURITY IN 5G NETWORKS: CHALLENGES AND SOLUTIONS

In order to provide clarity, the study evaluates network security at three different network levels: access and core networks. It also presents possible solutions.

A. Diverse Access Network Structures

1) Security Challenges: Requirements for 5G networks include higher data speeds, worldwide availability, lower latency, and a range of use cases, such as MTC, IoT, and V2X [10]. Due to the wide range of nodes and access techniques, these networks are more vulnerable to security attacks. The demand for network bandwidth is rising more quickly than ever thanks to the rapid expansion of new devices and applications. Due to its diversity and access methods, HetNets, Because they consist of both high- and low-power radio frequency macro nodes that are managed by the same entity, they pose significant security issues [11].

Network operators favor open access auxiliary networks to boost network capacity, such as wireless local area networks or femtocells. However, unauthorized users and eavesdroppers can easily access these networks. For both large base stations and small cells, the technology offers data offload relief, greater coverage, quicker data rates, and cost-effectiveness[12], low power access points have become more common. Low-complexity, highly effective handover authentication procedures are needed for low-power access points, however, they have not yet been created for 5G.

Security issues arise when switching between several access technologies, such as 3GPP and non-3GPP. The main issues include session replay attacks and the potential for malicious points of access that are not 3GPP secure. In 5G networks, developing secure key management protocols remains a difficult task.

Massive data-sending and -receiving nodes can overload signaling planes by jamming radio interfaces [13]. The current 5G jamming protections include passive eavesdropping and channel prediction.

2) Security Solutions: Users, infrastructure, and services should be shielded from potential threats in the radio portion of the network by access network security. In order to increase system robustness against security concerns, 5G makes use

TABLE II
AN OVERVIEW OF SECURITY'S DEVELOPMENT FROM 1G TO 5G

Network	Security System	Security Issues
1G	Absence of clear security or privacy measures	Call interception, eavesdropping, and a lack of privacy protection.
2G	Protection based on encryption and anonymity during authentication	Spam, one-way authentication, radio link security, and fake base stations
3G	Adopted 2G security, Facilitated secure network access, and implemented two-way authentication and Authentication and Key Agreement (AKA)	Vulnerabilities in the security of encryption keys, IP traffic, and travelling
4G	New integrity protection, Non-3G Partnership Project (3GPP) access security, Encryption key security, and trust methods have been developed	Security challenges caused by an increase in IP traffic include DoS attacks, Data integrity, Base Transceiver Station (BTS) security, and listening in on long-term keys. Unsuitable for securing novel services and devices, such the vast Internet of Things that 5G is anticipated to provide.
5G	Include stronger authentication, network slicing isolation, strong encryption, and IoT-specific security measures to guarantee data availability, confidentiality, and integrity in the dynamic wireless environment	Safeguarding network slicing, Managing IoT security at scale, addressing increased attack surfaces due to denser deployments, Ensuring robust authentication and encryption, and protecting against emerging threats in a rapidly evolving technology landscape

of a variety of access technologies [14], including virtualization, SDN, and cloud. Initiated by Shannon and enhancedby Wyner, Without using encryption or other higher-levelsecurity techniques, physical layer security simplifies designs and ensures information security. By leveraging random noiseand communication channels, This tactic limits information leakage and increases the difficulty of information access and decoding for attackers.

Orthogonal frequency division multiple access (OFDMA) systems' resource allocation issue is affected by many factors, such as the need for secrecy data rate requirements, dynamic power utilization, false noise injection, and multiple-antenna eavesdropping [15]. Dual decomposition is used to build the closed-form solution, maximizing the amount of securely transferred bits per joule. The security and secrecy of OFDM systems are improved by a physical layer method utilizing time domain scrambling.

Place low-power base stations in regions with substantial route loss to increase security in multi-tier HetNets. Use SDN-based authentication handover for worldwide resource management and monitoring. Implement a distributed access control system for 5G HetNets based on public key infrastructure. For travelling between trusted and untrusted networks, use ephemeral identities [16] and non-3GPP access networks.

B. Core Network

1) Security Challenges: While end-to-end service delivery, security, and quality of service are given top priority in the more dynamic and IP-based 5G core network, which leverages NFV, SDN, and cloud technologies, it is also very vulnerable to attack [17]. Since there will be more IoT devices using 5G, there will be more signaling traffic, which will make it harder to launch DoS attacks. For LTE interfaces, the 3GPP advises employing IPSec encryption, which raises signaling costs in the central network components.

2) Security Solutions: Compared to EPC, the 5G core network includes novel technological concepts and features such as flexible non-3GPP [18] control-user plane separation, network slicing, access internetworking, and service-based architecture.

The heirarchical SDN-based network-wide control system improves handoff, routing, and mobility while enabling multiple performance gradations and service differentiation, increasing network capacity and security.

V. PRIVACY CHALLENGES AND SOLUTIONS Since

the development of mobile and communication devices, privacy has remained a major concern. Customers now have access to a wider range of services as a result of the recent advancements in smart devices, such as smartphones and other portable electronics. The services are also getting more intelligent, pervasive, and omnipresent as mobile technology improves. The current transition to 5G networks holds a lot of promise, both from the standpoint of the consumers and the other interested parties. Various stakeholders will be assisted in improving their business models in order to generate more and better income. However, privacy issues must be resolved for the full and successful deployment of future 5G networks.

VI. NEW ILLUSTRATIONS IN FUTURE NETWORK SECURITY:THE XG

A paradigm shift in security is necessary to address the development of IoT devices and networked smart societies [19]. Quantum computing and other paradigm shifts in computing call for new, robust security systems. Future-proofing the XG wireless network with lightning-fast security mechanisms, AI-driven security automation, and blockchain-based services.

A. The Concept of XG

XG is a secure, autonomous network of intelligent things interconnected to build a latency-free, bandwidth-unrestricted smart city that is accessible everywhere. Smart surroundings are revolutionized by IoT, while smart networks serve as the IoT's supporting infrastructure Intelligent communication networks that can respond to real-time IoT needs and offer coverage everywhere are necessary for smart cities to reap the full benefits of the Internet of Things. With these qualities, XG is the network of the future.

B. An Overview of XG's Security Challenges

In the next 10 years, there will be an estimated 80 billion IoT devices in use, and 5G networks will integrate low-power and low-data-rate devices. New security issues will result fromthis, necessitating the use of secure communication protocols as IEEE 802.15.4, IPv6, and CoAP [20]. As existing security techniques may be challenged by quantum computing and increased processing power, new tactics including services-based security, resilient isolation, network slicing, portable software, and AI for preventative measures in future 5G networks may be required.

C. Security Softwarization and Virtualization

Future wireless networks will see a significant increase in virtualization [21], which makes it possible to implement network services as software components. This strategy improves end-to-end reliability while reducing costs and improving performance. Depending on the situation, software-based security features can be installed in any network perimeter, opening up fresh possibilities for enhancing network security. While intrusion detection or prevention systems (ID/P-S) can discover vulnerabilities and take countermeasures, traffic monitoring can detect and prevent invasions. Firewalls are commonly used in access control methods to stop assaults and illegal access [22]. By enabling programmability, centralization, and global visibility of network state, technologies like SDN help to reduce risks and monitor network traffic. In virtualized networks, softwarized security features like dynamic, dependable, and scalable firewaling are also accessible [23].Despite its limitations in speed and latency, virtualization and softwarization are crucial for future networks because of their flexibility and agility.

D. UAV Base Station for Security

In wireless networks, UAVs with base stations (UAVBS) are used because of their mobility and durability. Strict security measures must be put in place because the usage of UAV- BS-assisted communications is vulnerable to security concernssuch data manipulation and eavesdropping. Since they are susceptible to physical interference, research is creating strategies to deal with these problems.

In order to improve secure information flow in disaster-affected areas and public safety networks, UAV-BS is a potential method for smart cities and dense networks.

E. Privacy

Massive applications in areas like smart health care, industry automation, transportation, and IoT will be made possibleby the use of XG technology. Depending on the needs ofthe application, the privacy landscape will change because enormous volumes of data will be produced. The idea of gadget-free smart surroundings (the "Naked World") enables consumers to access digital services whenever and wherever they want [24]. Users are at risk for identity theft, data leakage, and other privacy problems in this open and shared environment. A number of stakeholders, including infrastructure suppliers, network operators, and service providers, must take precautions to prevent the leakage of personal information. Such intelligent settings require strict laws and rules. In order to deploy smart cities, smart spaces will be crucial, and XG will be crucial in enabling speedier communication. Users' top concern in the future is privacy because smart cities need to be highly interconnected and have many stakeholders offering a variety of services. Location, physical and mental status, social interactions, behavior and action, and media are all subject to privacy rules for smart cities [25].

VII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

As networking technologies have advanced, so too has network security. New technology ideas like SDN, which promoted new security paradigms like Software Defined Security, have also caused new disruptions. To provide solid security in 5G and beyond, additional research is required, with essential topics detailed in depth based on existing literature.

A. 5G Networks: Access, Backhaul, Core Networks

Hospitals, schools, cars, and home appliances will all see a revolution in communication thanks to 5G technology. Ultra-densification, offloading, mmWave, and unlicensed spectrum, and MIMO are important technologies. But because of the particular difficulties they encounter, it is also important to look into the security of these systems. For example, more research is required to safeguard networks or data at the physical layer using AI or big data, as well as to guaran-tee secrecy in the MIMO resource allocation process. The backhaul network, which links access and core networks, is divided into control and data planes by SDN, which has deployed control planes in the clouds and forwarding plane features. Because of the high degree of interactivity between the control and data planes, malicious or compromised nodes still find it challenging to execute saturation attacks. Massive IoT deployment presents difficulties for the core network,making authentication, mobility, and policy control entities easily exploitable by bad actors. The functional separation of firewalls and authentication measures, for example, to identifymalicious activity at the entrance points, is one potential remedy. To fully take use of 5G's potential for boosting connectivity and security, more research is required [26].

B. Key 5G Technologies: SDN, NFV, MEC

Future networks will inevitably employ SDN, NFV, and cutting-edge cloud computing ideas like MEC and fog computing. However, security issues in these technologies are frequently handled singly, without taking the use case or applicability into account. Due to user behavior and network dynamism, Resource expansion in some network areas might not be financially feasible. Future wireless networks must conduct research on control mechanisms for service dynamics and traffic volatility. Security risks can be reduced through case studies on NFV prospects and SDN security.

The difficulties of dispersing security operations across networks and their effects on network security functionality require further study. To prevent unauthorized usage of network resources, security policies and service-level agreements must be created.Despite weaker kinds depending on networking and resource capabilities, virtualization and VNFs are the main causes of security problems in cloud computing. Strong security will be made possible by contemporary cloud computing concepts like MEC and fog computing, which will also bring services closer to users and speed up authentication in latency-sensitive applications. [27].

VIII. CONCLUSION

Utilizing cutting-edge technologies like MEC, SDN, NFV, and MIMO, 5G wireless communication networks link many aspects of life, changing the security landscape from simple phone tapping to myriad assaults on infrastructure, services, and devices. The landscape of network security may grow more complex as a result of the inherent security problems these technologies provide. This study examines security is- sues affecting technology including the access, core, and 5G network components. The growth of devices, services, and networking technologies has led to a rise in the need for new security solutions. As a result, we have covered the security concerns that are raised by the various 5G network components and technologies in depth and have offered a number of potential security guidelines, techniques, and fixes.The increasing control infrastructure owners and system operators have over user privacy and data, as shown in cloud storage systems, has made privacy a hot topic for research. We also examine the privacy issues associated with wireless networks and look into potential remedies to safeguard user and data privacy.

In order to manage the various threat landscapes in networked systems, the XG vision envisions a linked world with a variety of devices and services. This environment necessitates novel security solutions. This essay has focused on how to use blockchain technology to boost user security because it securely distributes information to its intended users. New communication services and technology may bring with them new security concerns and challenges. Potential security and privacy breaches can be minimized by addressing these issues from design through deployment.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5g be?," *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[3] J.-K. Wey, H.-T. Chang, L.-F. Sun, and W.-P. Yang, "Clone terminator: An authentication service for advanced mobile phone system," in *1995 IEEE 45th Vehicular Technology Conference. Countdown to the Wireless Twenty-First Century*, vol. 1, pp. 175–179, IEEE, 1995.

[4] C. Hausl, J. Emmert, M. Mielke, B. Mehlhorn, and C. Rowell, "Mobile network testing of 5g nr fr1 and fr2 networks: Challenges and solutions," in *2022 16th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, IEEE, 2022.

[5] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[6] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5g: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[7] P. Schneider and G. Horn, "Towards 5g security," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 1165–1170, IEEE, 2015.

[8] D. Kutscher, "It's the network: Towards better security and transport performance in 5g," in *2016 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pp. 656–661, IEEE, 2016.

[9] N. Alliance, "'ngmn 5g white paper, version 1.0," *Next Gener. Mobile Netw.(NGMN), Frankfurt, Germany, Tech. Rep*, 2015.

[10] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. Le Moullec, "A survey on the roles of communication technologies in iot-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36611–36631, 2018.

[11] R. Q. Hu, Y. Qian, S. Kota, and G. Giambene, "Hetnets-a new paradigm for increasing cellular capacity and coverage [guest editorial]," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 8–9, 2011.

[12] D. Wake, D. Johansson, and D. Moodie, "Passive picocell: a new concept in wireless network infrastructure," *Electronics Letters*, vol. 33, no. 5, pp. 404–406, 1997.

[13] W. Trappe, "The challenges facing physical layer security," *IEEE communications magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[14] D. Soldani, P. Chatzimisios, A. Jamalipour, B. Barani, S. Redana, and S. Rangan, "5g radio access architecture and technologies [guest editor introduction]," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 14–15, 2016.

[15] E. Suikkanen, J. Janhunen, S. Shahabuddin, and M. Juntti, "Study of adaptive detection for mimo-ofdm systems," in *2013 international symposium on system on chip (SoC)*, pp. 1–4, IEEE, 2013.

[16] A. Neal, "Study on new services and markets technology enablers," *3GPP–TR 22.891 rel. 14.2*, 2016.

[17] J. Kim, D. Kim, and S. Choi, "3gpp sa2 architecture and functions for 5g mobile communication system," *ICT express*, vol. 3, no. 1, pp. 1–8, 2017.

[18] A. Patil and H. Sawant, "Technical specification group services and system aspects ip multimedia subsystem (ims)," *Int. J. Electron. Commun. Comput. Eng.*, vol. 3, no. 2, pp. 234–238, 2012.

[19] I. Ahmad, T. Kumar, M. Liyanage, M. Ylianttila, T. Koskela, T. Braysy, A. Anttonen, V. Pentikinen, J.-P. Soininen, and J. Huusko, "Towards gadget-free internet services: A roadmap of the naked world," *Telematics and Informatics*, vol. 35, no. 1, pp. 82–92, 2018.

[20] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," tech. rep., 2014.

[21] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[22] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[23] M. Liyanage, I. Ahmed, J. Okwuibe, M. Ylianttila, H. Kabir, J. L.Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, and E. M. De Oca, "Enhancing security of software defined mobile networks," *IEEE Access*,vol. 5, pp. 9422–9438, 2017.

[24] K. Halunen, J. Häikiö, and V. Vallivaara, "Evaluation of user authentication methods in the gadget-free world," *Pervasive and Mobile Computing*, vol. 40, pp. 220–241, 2017.

[25] D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489–516, 2017.

[26] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, 2014.

[27] F. Sabahi, "Virtualization-level security in cloud computing," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp. 250–254, IEEE, 2011.