Threats and AI Trends in Threat Modeling for 5G/6G

1st Wesley R. Bezerra
BCC/ IFC
Rio do Sul-SC, Brazil
wesley.bezerra@ifc.edu.br

2nd Edwardes A. Galhardo
UFG
GO, Brazil
edwardesamarogalhardo@inf.ufg.br

3nd Lais M. Bezerra
SENAI
SC, Brazil
lais.machado1@gmail.com

3rd Carlos B. Westphall
PPGCC/ UFSC
Florianópolis, Brazil
carlosbwesphall@gmail.com

***Abstract*—With the increase in the attack surface provided by the advancement of 5G/6G, concerns about attacks and security breaches also increase. Since this is a recent area of research and development, some challenges are encountered. Furthermore, with the increase in capillarity and the number of connected devices promoted by technologies such as Reconfigurable Intelligent Surface, attacks that can exploit connected devices may become a problem since these devices will have a considerable number. With the perspective of providing a future vision for the solutions that were in threat modeling and a current view of the threats researched in this topic, we bring an analysis of articles that address threat analysis in 5G/6G and Reconfigurable Intelligent Surface, presenting their results and considerations through a qualitative analysis of the challenges encountered.**

***Index Terms*—5g, 6g, ris, generative ai, security, threat modeling**

I. Introduction

5G/6G networks will likely expand in the medium to short term, enabling increased capabilities for using the Internet of Things (IoT) for smart services. Services that require integrating a large number of devices (159 billion according to [1] in 2030) or that require indoor coverage can benefit from these technologies. However, as the possibilities for use increase, so do the challenges associated with these possibilities for use.

Some challenges are not yet well known. Since this is a very recent tool and not yet well established, new challenges and usage capabilities have been constantly evolving together [2]. Some challenges, mainly security-related, will arise after the massive adoption of these technologies and the emergence of curiosity about the subject by the hacker community. Its establishment is not a reality since few countries, such as China, have been prominent in research and publishing articles and studies on the subject, Figure 1.

Therefore, some vulnerabilities are imminent and will appear as soon as this topic becomes part of the day-to-day use of end users and researchers. Some challenges may be encountered, mainly related to the new attack surfaces emerging from establishing these new technologies based on metasurfaces [3], [4]. As a result, new questions arise: *What will these new attack surfaces be? This new approach of transmission, forms of beamforming [5], [6], or transmission with reconfigurable intelligent surfaces? With more elements participating in the transmission, the attack capacity will expand, mainly regarding the attack surface after a major 6G adoption?*

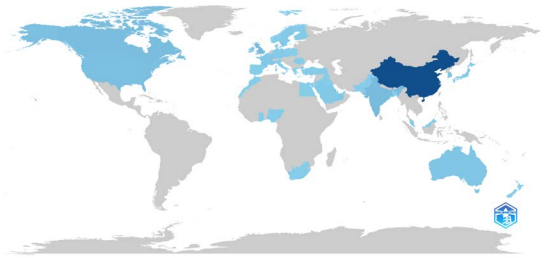

Fig. 1. Scientific Production by Country. The darker the color, the more occurrences there are in the country.

Specifically, in this study, the authors will address the area of 5G/6G and *Reconfigurable Intelligent Surfaces* (RIS). These are two of the main technologies brought by 6G and will significantly increase the number of devices connected to an antenna. Through another related technology, massive MIMO (mMIMO) [7], [8], a massive number of connections to a single antenna can be expanded through the use of RIS and support several ubiquitous devices that will use Ambient Backscattering Communication (AmBC).

Such increase in the coverage is considered a significant advance in data communication. However, with more devices connected, these devices could potentially become part of a botnet [9], [10] if they are not properly configured [11]–[13]. Yet, as has happened in several cases, they can suffer *spoofing* or *impersonation*, or even data leaks, among other issues to be discussed.

Therefore, by attacking a smart surface, an adversary's device can jam [14], [15] the transmission blocking information that travels through it. In this case, the RIS would be the medium where the *man-in-the-middle* (MITM) would act and violate the system's security. This is an example of how these surfaces could be exploited shortly [16], [17].

Unfortunately, this problem has previously occurred with other technologies, such as fiber optic technology [18]. In the case mentioned, an optical fiber passed under the ocean to Europe, with a *tapping* on the fiber. This fact caused significant discomfort between the governments of the United States and Brazil during the administration of President Dilma [19], [20],

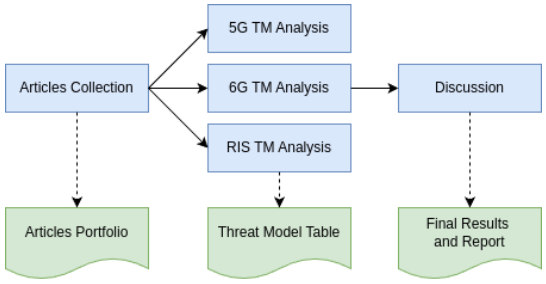

Fig. 2. Work Methodology. The steps and sub-steps are represented in blue, and the results are represented in green. The dashed arrows correlate the results with their generating steps.

leading us to install fibers from here directly to Portugal.

Concerning these challenges, this work aims to address threat modeling for 5G/6G and RIS, providing an overview of how researchers are currently approaching the topic and the existing automated approach trends. It also presents threat models specific to 5G that may directly influence vulnerabilities in 6G. We also presented perspectives on using automated threat model generation for 6G. Finally, a brief consideration was made about security involving RIS devices.

The rest of the work is organized as follows: Section II presents the methodology adopted for developing this work and its steps. Section III presents the collected data and the set of threats already summarized. This is followed by Section IV, which proposes a discussion on the threats found and their impacts. Finally, Section V brings the article to a close and presents future directions for work.

II. Methodology

In this section, the methodology used to develop this work is discussed, Figure 2. This methodology was conducted in three stages: **(1)** a collection of articles, **(2)** an analysis of articles in three sub-stages (threat model 5G, threat model 6G, and threat model RIS), and **(3)** a discussion of the results and planned future work.

The work begins with the **collection of articles** composed by three sets of articles: 5G threat model articles, 6G threat model articles, and relevant articles in RIS. Regarding it, three bibliographic searches were carried out: one on threats to 5G (1), one on threats to 6G (2), and others on RIS and AmBC (3). The latter used the Scopus database, because it was shared with another bibliometric study on the subject. The first two use the Google Scholar portal[1] as an integrator of the other databases. Regarding the time restriction on the consultation, there was none; that is, regardless of the publication date, the article was included in the results.

$$threat\ AND\ model\ AND\ 5G \tag{1}$$

$$threat\ AND\ model\ AND\ 6G \tag{2}$$

[1]https://scholar.google.com/

$$(\text{"}reconfigurable\ intelligent\ surfaces\text{"})\ AND\ (\text{"}ambient\ backscatter\text{"})AND\ (energy\ AND\ throughput\ AND\ efficiency) \tag{3}$$

In a second step, **analyses** of each article were carried out. Each article was analyzed, and a list of threats or how it models threats was extracted. These threats were presented in a table (Table I) that also quantified the relevance of each threat to the set of studies. This step is divided into three sub-steps: analysis of threat models in 5G, analysis of threat models in 6G, and analysis of threat models in RIS - according to the previously mentioned queries.

The 5G TM Analysis sub-step analyzed studies addressing threat modeling for 5G systems in web interfaces, architecture, and other aspects. The 6G TM Analysis sub-step continued to address threat modeling, but included studies involving ML, Digital Twins, and GenAI approaches. Equally important is the RIS TM Analysis, which discusses important studies addressing existing threats to this type of smart surface.

Finally, a **discussion** of how these threats can affect daily life when adopting this new technology is proposed. Possible advances in the types of new technologies and how they impact advances in the search for security by researchers will also be discussed.

In summary, through the adoption of this work methodology, it was possible to carry out a representative survey of the state of the art of threats that affect 5G/6G and RIS, which in turn is described in the next Section and commented on in Section IV.

III. Development

This section provides an analysis of the documents collected, which represent some of the most relevant articles for analyzing the state of the art regarding to threat modeling for 6G. This analysis is divided into three subsections: threats in **5G (a)**, threats in **6G (b)**, and threats in **RIS (c)**. Through the joint analysis of these three subsections, we can have an overview of the current work in this area.

Since 6G technology will evolve from 5G but will be used in parallel with the latter, it is important to have an overview of the work that involves 5G as well. To this end, we present an evaluation of some works below **(a)**.

For **Farooqui et al.** [21] some attack surfaces (device, Radio Access Network, Edge, Core, Service) and some possible attacks, filtered only those of the Network, Edge, and Devices, are: jamming, MITM attacks, eavesdropping, signaling attack, MEC server vulnerabilities, rogue nodes, authentication issues, side-channel attacks, bots, DDoS attacks, malware.

The work of **Giambartolomeli et al.** [22] tests the security of three different technologies for 5G in their web interface. These are Open5GS, Free5GC, and OpenAirInterface; 10 different tools were used for this test, nine different attacks (some could not be implemented for OpenAirInterface), and none passed 100% of the tests. The tests performed were database permission leakage, SQL injection, NoSQL injection,

dictionary attack, bruteforce attack, DoS and DDoS, directory traversal, clickjacking, and JSON Web Token robustness.

Also **Gupta et al.** [23] analyzes aspects of bandwidth consumption resulting from spoofing using game theory in attacks on Small Cells [24]. The authors also comment on the impacts of DoS and DDoS on these types of networks and the importance of adopting an IDS (Intrusion Detection System) to mitigate this type of situation.

Concerning the author **Kim** [25], its work presents a classification of threats into four categories: UE domain, RAN domain, Edge and Core Domain, and Service Interconnection domain. For the author, the threats can be listed as Malware, firmware hacking, device tampering, IoT botnet, wireless jamming, RAN DoS and DDoS, rogue base station, platform (SDN/NFV/MEC) vulnerabilities, third-party API, access control, network slicing, decentralized network DDoS, API security, roaming vulnerability, and subscriber information leakage.

TABLE I
ATTACK SET BY PUBLICATION

#	Attack	[21]	[22]	[23]	[25]	[26]	[27]	[28]	[2]	[16]	[17]	(%)
01	Jamming	✔	⊘	⊘	✔	⊘	✔	⊘	⊘	⊘	✔	40%
02	MITM Attacks	✔	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	20%
03	Eavesdropping	✔	⊘	⊘	⊘	⊘	⊘	✔	⊘	✔	⊘	30%
04	Signalling attack	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
05	Rogue nodes	✔	⊘	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
06	Auth and AC issues	✔	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	30%
07	Side Channel attacks	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
08	Bots	✔	⊘	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
09	DDoS attacks	✔	✔	✔	✔	✔	⊘	✔	⊘	⊘	⊘	60%
10	Malware	✔	⊘	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
11	DB permission leakage	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
12	SQL injection	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
13	NoSQL injection	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
14	Dictionary attack	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
15	Bruteforce attack	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
16	Directory Traversal	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
17	Clickjacking	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
18	JWT robustness	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	10%
19	Firmware Hacking	⊘	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
20	Tampering	⊘	✔	⊘	✔	⊘	✔	✔	⊘	⊘	⊘	40%
21	Platform vulnerabilities	⊘	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
22	Third-party API	✔	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	30%
23	Network slicing	⊘	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
24	Roaming vulnerability	⊘	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
25	Subscriber Info Leakage	⊘	✔	⊘	✔	⊘	⊘	⊘	⊘	⊘	⊘	20%
26	Cross-domain lateral attack	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	⊘	⊘	10%
27	Sensor exploitation	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	⊘	⊘	10%
28	Adversarial attacks	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	⊘	10%
29	Insider threats	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	⊘	10%
30	Forgery	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
31	Brute force	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
32	Reuse threat	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
33	Partial collision	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
34	Recovery	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
35	Scooping	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
36	Collaborated	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
37	Impersonation	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
38	Disclosure	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
39	Stalking	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
40	Social enginering	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
41	Access aggregation	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
42	Birthday	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
43	Cloning	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
44	Phishing	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
45	Redirection	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
46	Free riding	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
47	Physical	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
48	Environment	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
49	FIFO	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
50	Sync flood	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
51	Message append	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
52	Alteration	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
53	Data diddling	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
54	Session hijack e	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	⊘	10%
55	Nulled interference	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	10%
56	Nulled reflection	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✔	⊘	⊘	10%

Continuing with some **6G works**. In these cases, the threats that affect the technology are not always listed, as some of them are not yet well known. We can see in the works presented that efforts are being made to automate threat identification and threat hunting [29], [30], since due to the large attack surface, the use of AI to assist in the modeling process has become a trend.

In the work of **Islam et al.** [31], the focus is on only one type of threat, the FSI attack. For this, the authors propose an approach that uses machine learning to solve the problem. The authors established their scenario in the energy grids in servers that manage energy on demand based on workloads.

As for the authors **Ferrag, Debbag, and Al-Hawawreh** [32], they bring an approach using generative AI for threat modeling in a 6G environment. In their work, the authors evaluate three AI approaches for generating models. They analyze Generative Adversarial Networks (GAN), GPT-based, and BERT methods. Finally, they propose a model based on GAN and a transformer-based model for threat modeling in this 6G scenario.

Von de Assen et al. [33] contributes to using AI for active vulnerability hunting. The authors propose a methodology based on seven steps for threat modeling capable of using a knowledge base and quantifying the impact of a threat on the business. The proposal, called ThreatFinderAI, uses ENISA[2], OWASP AI[3], and Mitre Atlas[4] as its database.

No less important, **Rodrigues et al.** [34] present the use of AI and Digital Twins models for vulnerability analysis. The authors also present the HORSE architecture, which is part of an EU project and brings key concepts for the future security of 6G networks, such as human-centric, open source, green, sustainable, coordinated provisioning and protection evolutionary platform.

The work by **Wu** [26] comments on a threat analysis based on spatiotemporal metrics and focuses on cross-domain lateral attack, large-scale DDoS, and sensor exploitation. The author presents a model that analyzes the device and slice level of the topology for high-frequency traffic flow and performs a cross-slice and cross-protocol analysis to identify the attacks.

Enright, Hammad, and Dutta [35] show the use of machine learning and federated learning for the security solution for 6G networks. This work does not directly mention which type of algorithm should be used but indicates federated learning as the solution for security through a Zero Trust approach.

In **Karaçai et al.** [27], a Machine Learning approach is also adopted to identify threats in All-sense meetings. The authors analyze the threats using STRIDE and attack trees. The authors present the following threats to this application: unauthorized access to the structure, jamming, tampering with haptic signals, adversarial attacks, and insider threats.

Regarding the work of **Kazmi et al.** [28] is a literature review that provides a broad view of the threats that affect 6G; however, in this work, we will only address the threats. The threats are listed in five groups: authentication, confidentiality, access control, availability, and integrity. For authentication, forgery, brute force, reuse threat, password, partial collision,

[2]https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
[3]https://owaspai.org/
[4]https://atlas.mitre.org/

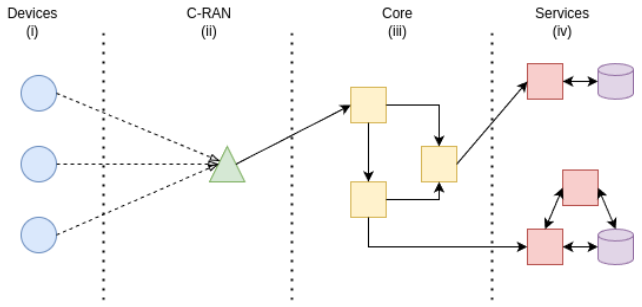

Fig. 3. 6G System Architecture. Where the blue elements designate the devices that access the 6G network via radio, the green element represents the base radio station that is the entry point for other services; the yellow elements represent the central devices of the architecture, the red elements represent services provided through 6G, and the purple elements represent data accessible by these services. As for the arrows, dashed arrows indicate radio communication, while solid arrows indicate communication without formal specification.

and recovery are included. As for confidentiality, there are snooping, collaborated, MITM, chosen plaintext, impersonation, disclosure, stalking, and eavesdropping. Following on from access control, there are social engineering, access aggregation, birthday, cloning, and phishing. Also, availability includes redirection, free riding, physical environment, FIFO, DDoS, and sync flood. Finally, integrity cites message append, alteration, data diddling, session hijack, and tampering.

As for the **scope of RIS**, we have some works that can be cited as contributions to threat modeling in this technology. The work of **Di Renzo et al.** [2] is extensive and presents an important set of concepts, technologies, scientific knowledge of physics, and much more. However, we would like to highlight two types of attacks that are very specific to RIS: nulled interference and nulled reflection. Both focus on interrupting data transmission with RIS as an attack surface.

Authors Wei and Guo [16] present the problem of physical layer secret key generation (PL-SKG) leakage. This is a problem that can affect the physical layer of systems involving RIS. Other authors, such as Khalid et al [36] and Gao et al. [37], reinforce the importance of addressing this problem and also highlight the issue of RIS jamming.

Continuing with the jamming theme, authors Sena et al [17] present a scenario where jamming occurs to favor some transmissions, while this is transparent to the receiver.

IV. Discussion

In this section, we will resume discussing the main threat models and trends in approaching threat analysis in 5G/6G. Although 5G/6G TM is a recent topic and not yet widely used, there is an apparent concern about the potential threats this new form of data transmission may face. The advent of 6G will greatly expand coverage, and the number of connected devices will increase significantly. Added to this is the increase in the number of IoT devices, new types of services such as all-sense meetings, telemetry, digital twins, and other services that will benefit from this new type of high-speed and reliable communication.

These factors will result in a massive increase in the available attack surface and will involve much complexity in managing resources and their security. As we have seen through some of the studies cited, the automated approach supported by new AI technologies such as Large Language Models (LLM) and Machine Learning algorithms is a trend for the coming years. In a scenario where it is important to understand security at different levels, such as Device, Edge, RAN, Core, and Services, Figure 3. In this scenario, the challenge of an approach that relies solely on the skills of security managers is significant.

As seen in Table I, in the studies analyzed alone, 56 threats were identified associated with different aspects of the 6G technology ecosystems and at different layers. They are directly linked to the physical layer (i.e. jamming), and others to users (i.e. social engineering). It is also worth noting that DoS attacks, whether distributed or not, constitute a significant problem and appear as a threat listed repeatedly in the articles presented. In other words, with the expansion of Internet use due to 6G, security must be guaranteed from end to end.

From this study, it is possible to note the complexity of addressing threat modeling in 6G. A threat-hunting approach that involves new technologies such as IDS, Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Extended Detection and Response (XDR). This set of technologies enables a proactive approach to combating threats already plaguing 5G and will be inherited by 6G in the future.

Another important vision for the future is the use of threat databases as knowledge base sources in threat-hunting systems, integration with LLMs for threat analysis, the massive adoption of Machine Learning to prevent attacks, and even the use of digital twins for network security assessment. This vision lets us know what advances are necessary for 6G to arrive with greater security.

V. Conclusion and Future Works

This paper presented an overview of threats to 5G, 6G, and RIS and the trends in threat modeling in this field of telecommunications. Through a documentary analysis, it was possible to outline the main threats affecting these three concepts, even some that are not fully used. This overview is of utmost importance for preparing future research involving the theme of 6G and its technologies in the coming years, as it will allow researchers and postgraduate students to have an overview of the threats that will affect their systems.

As this is an initial literature mapping, we propose a more in-depth and formal approach. Furthermore, it is also important to present simulators and security protocols related to the various actors in 6G communication for later validation. The theme of authentication in this scope and the energy issues of each type of equipment involved must be considered. No less important, an analysis of bibliometric (documentary) and scientometric data (researchers, vehicles, affiliations, among

others) is of utmost importance to better outline the future vision of the area.

VI. Acknowledgments

The authors sincerely thank the Federal University of Santa Catarina (UFSC). This study was partially funded by the Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina (FAPESC), Edital 20/2024.

References

[1] S. Das and E. Mao, "The global energy footprint of information and communication technology electronics in connected internet-of-things devices," *Sustainable Energy, Grids and Networks*, vol. 24, p. 100408, 2020.

[2] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE journal on selected areas in communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[3] M. Y. Shalaginov, S. D. Campbell, S. An, Y. Zhang, C. Ríos, E. B. Whiting, Y. Wu, L. Kang, B. Zheng, C. Fowler *et al.*, "Design for quality: reconfigurable flat optics based on active metasurfaces," *Nanophotonics*, vol. 9, no. 11, pp. 3505–3534, 2020.

[4] H. Liu, C. Guo, G. Vampa, J. L. Zhang, T. Sarmiento, M. Xiao, P. H. Bucksbaum, J. Vučković, S. Fan, and D. A. Reis, "Enhanced high-harmonic generation from an all-dielectric metasurface," *Nature Physics*, vol. 14, no. 10, pp. 1006–1010, 2018.

[5] A. M. Alwakeel, "6g virtualized beamforming: a novel framework for optimizing massive mimo in 6g networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2025, no. 1, p. 23, 2025.

[6] Z. Q. Al-Abbasi, "Optimized beamforming for multiuser massive mimo 6g wireless networks," *Telecommunication Systems*, vol. 88, no. 1, p. 6, 2025.

[7] H. Ma, J. Du, H. Wu, L. Xing, and R. Zheng, "A review of channel estimation research methods for massive mimo systems," *Physical Communication*, p. 102632, 2025.

[8] V. Inzillo and A. Ariza Quintana, "Implementation of 802.11 ax and cell-free massive mimo scenario for 6g wireless network analysis extending omnet++ simulator," *SIMULATION*, p. 00375497241266256, 2025.

[9] A. Woodiss-Field, M. N. Johnstone, and P. Haskell-Dowland, "Examination of traditional botnet detection on iot-based bots," *Sensors*, vol. 24, no. 3, p. 1027, 2024.

[10] B. Bojarajulu and S. Tanwar, "Customized convolutional neural network model for iot botnet attack detection," *Signal, Image and Video Processing*, vol. 18, no. 6, pp. 5477–5489, 2024.

[11] S. A. G. Asgar and N. Reddy, "Analysis of misconfigured iot mqtt deployments and a lightweight exposure detection system." USENIX, 2025.

[12] A. S. A. Elgazazz, H. J. Dagenborg, and N. El Ioini, "Misconfiguration of cluster and iot systems recovery: Extended experiments," 2024.

[13] R. Yaben, N. Lundsgaard, J. August, and E. Vasilomanolakis, "Towards identifying neglected, obsolete, and abandoned iot and ot devices," in *2024 8th Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 2024, pp. 1–10.

[14] Y. Sun, K. An, Y. Zhu, G. Zheng, K.-K. Wong, S. Chatzinotas, H. Yin, and P. Liu, "Ris-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9212–9231, 2022.

[15] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Communications*, vol. 29, no. 3, pp. 131–138, 2022.

[16] Z. Wei, B. Li, and W. Guo, "Adversarial reconfigurable intelligent surface against physical layer key generation," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2368–2381, 2023.

[17] A. S. de Sena, J. Kibiłda, N. H. Mahmood, A. Gomes, and M. Latva-Aho, "Malicious ris versus massive mimo: Securing multiple access against ris-based jamming attacks," *IEEE Wireless Communications Letters*, vol. 13, no. 4, pp. 989–993, 2024.

[18] Y. Sánchez, "The contingency of cultural negotiations in cross-border networks," *Chaos in the Contact Zone: Unpredictability, Improvisation and the Struggle for Control in Cultural Encounters*, vol. 94, p. 159, 2017.

[19] J. Ishaya Hanna, "The snowden files," Ph.D. dissertation, Lebanese American University, 2020.

[20] R. H. White, C. D. Johnson, L. K. Johnson, Q. E. Hodgson, J. Jaffer, C. D. Johnson, V. Woodbine, T. L. Meyer, A. Golodner, B. Hensley *et al.*, "No. 9-cybersecurity and national defense: Building a public-private partnership," 2015.

[21] M. N. I. Farooqui, J. Arshad, and M. M. Khan, "A layered approach to threat modeling for 5g-based systems," *Electronics*, vol. 11, no. 12, p. 1819, 2022.

[22] F. Giambartolomei, M. Barceló, A. Brighente, A. Urbieta, and M. Conti, "Penetration testing of 5g core network web technologies," in *ICC 2024-IEEE International Conference on Communications*. IEEE, 2024, pp. 702–707.

[23] A. Gupta, R. K. Jha, and S. Jain, "Attack modeling and intrusion detection system for 5g wireless communication network," *International Journal of Communication Systems*, vol. 30, no. 10, p. e3237, 2017.

[24] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, S. B. Taher, M. Kabir, S. Muyeen, and A. H. Gandomi, "Toward a secure 5g-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities," *IEEE Access*, vol. 12, pp. 13 125–13 145, 2024.

[25] H. Kim, "5g core network security issues and attack classification from network protocol perspective." *J. Internet Serv. Inf. Secur.*, vol. 10, no. 2, pp. 1–15, 2020.

[26] G. Wu, "A spatiotemporal transformer framework for robust threat detection in 6g networks," *Internet Technology Letters*, vol. 8, no. 3, p. e70017, 2025.

[27] L. Karaçay, Z. Laaroussi, S. Ujjwal, and E. U. Soykan, "Guarding 6g use cases: a deep dive into ai/ml threats in all-senses meeting," *Annals of Telecommunications*, vol. 79, no. 9, pp. 663–677, 2024.

[28] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, "Security concepts in emerging 6g communication: Threats, countermeasures, authentication techniques and research directions," *Symmetry*, vol. 15, no. 6, p. 1147, 2023.

[29] P. Kumar, A. Jolfaei, and A. N. Islam, "An enhanced deep-learning empowered threat-hunting framework for software-defined internet of things," *Computers & Security*, vol. 148, p. 104109, 2025.

[30] P. Kumar, D. Javeed, A. N. Islam, and X. R. Luo, "Deepsecure: A computational design science approach for interpretable threat hunting in cybersecurity decision making," *Decision Support Systems*, vol. 188, p. 114351, 2025.

[31] S. Islam, I. Zografopoulos, M. T. Hossain, S. Badsha, and C. Konstantinou, "A resource allocation scheme for energy demand management in 6g-enabled smart grid," in *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2023, pp. 1–5.

[32] M. A. Ferrag, M. Debbah, and M. Al-Hawawreh, "Generative ai for cyber threat-hunting in 6g-enabled iot networks," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. IEEE, 2023, pp. 16–25.

[33] J. Von der Assen, A. Huertas, J. Sharif, C. Feng, G. Bovet, and B. Stiller, "Threatfinderai: Automated threat modeling applied to llm system integration," in *2024 20th International Conference on Network and Service Management (CNSM)*. IEEE, 2024, pp. 1–3.

[34] E. Rodriguez, X. Masip-Bruin, J. Martrat, R. Diaz, A. Jukan, F. Granelli, P. Trakadas, and G. Xilouris, "A security services management architecture toward resilient 6g wireless and computing ecosystems," *IEEE access*, 2024.

[35] M. A. Enright, E. Hammad, and A. Dutta, "A learning-based zero-trust architecture for 6g and future networks," in *2022 IEEE Future Networks World Forum (FNWF)*. IEEE, 2022, pp. 64–71.

[36] W. Khalid, M. A. U. Rehman, T. Van Chien, Z. Kaleem, H. Lee, and H. Yu, "Reconfigurable intelligent surface for physical layer security in 6g-iot: Designs, issues, and advances," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3599–3613, 2023.

[37] N. Gao, Y. Han, N. Li, S. Jin, and M. Matthaiou, "When physical layer key generation meets ris: Opportunities, challenges, and road ahead," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 355–361, 2024.