IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14610

Security Threats at the 5G Air Interface and Implications for Telemedicine Reliability: A Literature Survey

G.Sai Keerthi and Vikas Vippalapalli*

Dept. of Electronics and Telematics Engineering, GNITS (for Women), Hyderabad, India

Abstract: The rollout of fifth-generation (5G) networks has opened up new possibilities for telemedicine. It allows for real-time remote diagnostics, ongoing patient monitoring, and high-speed clinical communication. However, the open wireless nature of the 5G air interface brings significant security risks. These vulnerabilities can compromise network reliability and threaten the continuity of medical services. This paper reviews existing literature on security threats related to the 5G air interface, focusing on the reliability of telemedicine Quality of Service (QoS). This paper examine documented types of attacks, including physical-layer jamming, adaptive overshadowing, signaling flooding at the NAS and RRC layers, core network GTP exploitation, paging storms, and replay attacks. Thid paper draw on findings from recent peer-reviewed studies about their effects on important radio parameters like Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), Signal-to-Interference-plus-Noise Ratio (SINR), latency, jitter, and throughput. This paper also look at machine learning methods for detecting anomalies linked to these attacks as mentioned in the literature. By relating documented attack patterns to established telemedicine QoS standards, this survey shows that the security of the 5G air interface is a matter of patient safety that needs careful consideration in healthcare network design. The paper points out ongoing research challenges and future paths that connect wireless network security with digital health.

Keywords: 5G security; telemedicine; air interface; jamming; signaling flooding; anomaly detection; RSRP; RSRQ; network reliability; healthcare IoT.

1. INTRODUCTION

The advent of 5G wireless technology and digital health systems has provided telemedicine with an array of new opportunities. These include real-time diagnostics, continuous patient monitoring, surgical tele-mentorship assisted by robots, and AI-powered clinical decision making. The three types of 5G wireless services defined by 3GPP, Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLLC), and Massive Machine Type Communication (mMTC), are all capable of meeting the demands posed by modern telemedicine applications [1]. eMBB enables streaming of clinical HD videos, URLLC makes possible tele-surgical mentorship with minimal delays, while mMTC is capable of providing massive connectivity to biosensors and wearables in hospitals.

Yet, being wireless, 5G raises its own problems. In contrast to wired clinical networks where there is a certain physical control over the network's security, 5G wireless air interface is inherently open to any radio transmission around. That implies the possibility of attack due to which security threats in 5G cannot be addressed by protocol design alone. It opens up numerous opportunities for an attacker to perform attacks on multiple layers of the protocol stack. Such attacks range from physical layer attacks like jamming and signal overshadowing, NAS/RRC signaling flooding, exploitation of GPRS tunneling protocol (GTP) in the user plane, and authentication procedures attacks.[2]

However, the implications of such attacks transcend mere technical problems. The applications of telemedicine must adhere to certain levels of Quality of Service (QoS). Any deviations from these standards can result in adverse clinical results. Consider a case whereby the QoS standards of a telemedicine session exceed the 150 ms latency threshold resulting in audio-video delay, thus hindering clinical diagnosis. Also, a denial-of-service attack on a telemedicine session can compromise patient data streams, thus failing to trigger an alarm for a detected heart rhythm problem. Additionally, a jamming attack on a telemedicine mentoring session may result in the loss of visual contact between the guide and the operating surgeon [12].

In this survey, the paper presents a systematic analysis of literature pertaining to attacks against the air interface security in 5G wireless networks and their impact on the reliability of telemedicine services. This is done by analyzing peer-reviewed papers that provide detailed discussion of attack scenarios, effect(s) of those attacks on relevant 5G wireless parameters and proposed machine learning techniques for detecting such attacks using abnormalities in measurements

DOI: 10.17148/IJIREEICE.2026.14610

from 5G wireless radio layer. This survey, which combines the findings from literature on wireless security attacks with known telemedicine QoS standards, will be useful for healthcare network engineers, researchers in medical informatics and clinical technology decision makers.

The paper is organized as follows. In Section 2, literature review is presented for the following topics: physical layer attacks; protocol and signaling attacks; core network attacks; and machine learning techniques used in anomaly detection for 5G security. Section 3 presents the threat taxonomy that categorizes attacks based on their effect on telemedicine services. Section 4 presents QoS requirements for telemedicine and mapping of attack signatures onto QoS metrics. Section 5 presents the methods of detection. Section 6 presents the open issues and research directions.

2. LITERATURE SURVEY

2.1 Overview

There has been considerable attention paid to the security of 5G wireless systems after the publication of the 3GPP Release 15 standards in 2018. The existing literature can be classified into four categories with respect to their relevance to this study: (i) attacks at the physical layer, which target the characteristics of the radio frequency medium and reference signals in 5G NR; (ii) attacks at the signaling layer, which make use of the security flaws in the protocols, such as NAS and RRC; (iii) core network attacks, especially on the GTP user plane; and (iv) detection and prevention mechanisms based on machine learning on radio measurements.

2.2 Physical-Layer Attacks

2.2.1 Adaptive Overshadowing Attacks

An adaptive form of overshadowing attack was demonstrated by Erni et al. [3] in the case of cellular network. It has been revealed that using a software-defined radio, an attacker could jam downlink reference signals through transmission of interference signals. In contrast to a classic jamming attack which uses brute force, overshadowing attacks target synchronization and channel estimation symbols used by user equipment (UE) to decode the physical downlink shared channel (PDSCH). Through overpowering of reference symbols while keeping other time-frequency resources unharmed, the attack reduces the channel quality estimate of UE without detecting the interference.

A reduction in RSRQ and SINR values at the UE due to the attack causes throughput loss without disconnectivity. Thus, the attack becomes more dangerous in telemedicine applications because the presence of such attacks is unlikely to cause alarm in monitoring applications. It has been established that the attack could continue with lower transmission powers due to the timing and power control loopback feature of the cellular air interface. Thus, their results indicate the importance of anomaly detection systems based on correlation analysis of the parameters rather than threshold detection.

2.2.2 Jamming and Physical Denial of Service

Lichtman et al. [4] presented a comprehensive classification of jamming techniques for cellular communications. Continuous, reactive, deceptive, and follow-on jamming techniques were considered. For the case of the 5G NR, reactive jamming works well since the attacker may watch for activity on a channel and interfere specifically during certain transmissions. This minimizes the required energy for effective interference. The authors concluded that minimal jamming energy was enough to cause continuous decrease of RSRP, which makes UEs unable to decode PDCCH and consequently disrupt communication.

Ahmad et al. [13] studied the vulnerabilities and security problems in 5G and emphasized physical layer denial of service as one of the most dangerous attacks. It was highlighted that using millimeter-wave frequencies in 5G made devices particularly susceptible to directional jamming. In healthcare environments, the use of 5G small cells indoors makes several possible targets for jamming.

2.3 Protocol and Signaling Layer Attacks

2.3.1 Vulnerability Detection in 5G Protocol Stacks

According to Yang and Wang [5], the approach for vulnerability detection is an effective combination of formal verification and fuzzing to uncover vulnerabilities at the level of logic in the 5G NR protocol specification. The authors

DOI: 10.17148/IJIREEICE.2026.14610

examined state machines for NAS and RRC and discovered that certain combinations of edge cases involving messages could cause non-compliant state transitions on behalf of network functions. These would lead to scenarios such as denial of service attacks, exhaustion of resources, and unauthorized manipulation of states. Notably, it was determined that the impacts of an attack on the protocol layer have implications on the air interface itself by increasing latency, creating abnormal scheduling, and decreasing throughput.

2.3.2 Formal Security Analysis of 5G Authentication

A formal analysis of 5G authentication protocols was performed by Basin et al. [6] using the Tamarin prover. The authors were able to prove the security attributes of 5G-AKA and EAP-AKA' authentication protocols, as well as reveal potential vulnerabilities in some deployments. Basin's work demonstrates that NAS level attacks leverage flaws in the protocol to induce repeated failures of the authentication process, creating overhead traffic that is comparable to NAS flooding attacks. This increases the utilization rate of access slots and delays the authentication process, thereby impacting the reliability of telemedicine sessions initiation in particular, especially when used by healthcare wearables.

2.3.3 UE Security Testing in 5G Standalone Networks

Bitsikas et al. [7] developed a security testing framework that is open-source for 5G standalone user equipment. The proposed framework enables conducting testing on commercial user equipment in a way that does not require any alteration in user equipment to evaluate security threats posed by NAS and RRC attacks systematically. The authors found that some commercial user equipment did not comply with security policies for particular message sequences where security mode command was accepted by the device in a downgrade form. It was argued that medical Internet-of-things devices relying on 5G will not undergo such strict security policy checks.

2.3.4 Paging and Privacy Attacks

Hussain et al. [14] considered privacy-violating attacks targeting 4G and 5G cellular paging protocols. It was proven that the unencrypted nature of the paging channel could be leveraged to conduct tracking, deduce activity patterns, and mount targeted denial of service attacks causing UEs to continuously engage in paging operations. In healthcare applications, such attacks would render medical wearable devices ineffective as paging storms would deplete their energy and block any alarm communications. Furthermore, tracking via paging may pose risks to location privacy of patients in hospitals.

2.3.5 New Protocol Vulnerabilities in 5G Access Networks

A number of new vulnerabilities were reported by Shaik et al. [15] in 4G and 5G cellular access network protocols based on the examination of the device capability exposure issue in the connection setup process. These vulnerabilities encompass attacks allowing the adversary to degrade security settings, commit a denial of service attack against a target UE, and fingerprint its identity. RRC-layer flooding attacks that are enabled by the connection setup process constitute one of the attack scenarios analyzed. The resulting effects on scheduling effectiveness and air interface resource allocation cause quality deterioration in all connected UEs in a given cell.

2.4 Core Network Attacks

Positive Technologies [8] discovered GTP (GPRS Tunneling Protocol) vulnerabilities existing in current 4G and 5G core networks. It was found out that insufficient checking of GTP packets in the user plane can lead to the injection of malicious traffic into the session, tunnel hijacking, and resource exhaustion of the User Plane Function (UPF). Attacks through GTP protocol are especially problematic for telemedicine due to their core network operation and the possibility of interfering in medical data traffic without leaving any traces on air interface radio parameters. Thus, it becomes more difficult to notice such threats while tracking UE radio measurements.

2.5 Machine Learning Approaches for 5G Security

2.5.1 Supervised Classification for Network Intrusion Detection

Apruzzese et al. [9] studied machine learning and deep learning techniques applied to cybersecurity, among which wireless network intrusion detection was included. The authors showed through their analysis of several data sets and attack scenarios that ensembles, namely, Random Forest and Gradient Boosting, demonstrate higher accuracy in classification than single estimators. Moreover, feature importance ranking provided by ensembles allows gaining insights into the results. The authors stressed the role of temporal feature aggregation and cross-feature interactions for

DOI: 10.17148/IJIREEICE.2026.14610

detection of attacks hiding in variations of regular behavior. This is relevant for 5G security monitoring based on radio measurements.

2.5.2 Unsupervised Anomaly Detection

Mirsky et al. [10] introduced an unsupervised anomaly detector Kitsune based on the ensemble autoencoder architecture. This system is trained only on examples of regular behavior and learns the representation of common traffic. When Kitsune finds deviations from the learned representation, it triggers an alert. For wireless networks, autoencoders can detect new attack patterns that cannot be identified by a simple signature check. This is very important in 5G healthcare systems, where the environment constantly evolves, and new threats emerge faster than they can be described.

2.5.3 Feature Engineering for Radio-Based Detection

The work of Xiao et al. [11] focused on the investigation of feature engineering techniques for IoT security employing machine learning methods. The authors proved that composite features, which reflect relations between several parameters, yield better results in classification than simple features based on one parameter. When applying these conclusions to the study of 5G radio measurement data, this paper presents the usefulness of applying derived values such as RSRQ-to-RSRP ratio (as an indicator that discriminates between interference and path loss), rate of change in the value of SINR (as an indicator of the speed of attacks), and normalized jitter related to baseline latency (distinguishing between delay changes resulting from congestion and attacks).

2.6 5G Quality of Service for Telemedicine Applications

The International Telecommunication Union [12] has issued QoS guidelines for use in wireless telemedicine. Latency should not exceed 150 milliseconds, packet loss 1%, jitter 50 ms, and sustained downlink data rates must be no less than 10 Mbps for high-definition video. In remote patient monitoring applications using wearable biosensors, while latency is less demanding, availability becomes critical at over 99.9%. Similarly, emergency telemedicine cases, such as video calls from ambulances to hospitals and telestroke, demand the maintenance of QoS even when radio propagation conditions are poor. Disrupted QoS in the midst of an emergency situation could have adverse effects on patients' health status.

Security and privacy issues for 5G are surveyed by Khan et al. [2], who observe that conflicting QoS needs of 5G systems result in security being in direct competition with QoS. Security features of mobility management in 5G, including frequent re-keying, encryption overhead, and signaling messages, use up precious resources. This results in competition between security and applications for available bandwidth, making network-level light security very attractive to telemedicine.

2.7 Research Gap and Motivation

Reviewing the existing studies, it becomes clear that there have been many investigations into 5G security vulnerabilities as well as telemedicine QoS needs, yet very little research has explicitly addressed the relation between attack signatures and violations of clinical QoS thresholds. In particular, the security-related work frequently examines the consequences of attacks in terms of generic performance metrics such as throughput, latency, and packet loss, yet not in regard to any clinical requirements. Likewise, studies on telemedicine network QoS usually assume ideal network conditions. This survey attempts to bridge this gap by combining the characterization of attack signatures described in the security literature with the requirements for telemedicine network defined according to the ITU-T and clinical guidelines.

3. ATTACK TAXONOMY AND TELEMEDICINE IMPACT

3.1 Taxonomy Overview

As can be seen from the reviewed literature, 5G air interface attacks can be divided into seven classes based on their target protocol layer, method of influencing radio parameters, and potential risk associated with telemedicine application. Table 1 provides details of this classification. The severity rankings are determined based on expert opinion from the surveyed literature. Telemedicine risks are derived from the mapping of impacts on radio parameters onto the clinical QoS thresholds presented in Section 4.

DOI: 10.17148/IJIREEICE.2026.14610

Table 1: 5G Air Interface Attack Taxonomy and Telemedicine Impact (synthesized from literature)

Attack Type	Layer	Radio Parameter Impact (from Literature)	Severity	Refs.	Telemedicine Risk
Jamming	Physical	RSRP < -100 dBm, SINR < 5 dB, DL ~0 Mbps	High	[4,13]	Total session loss
Adaptive Overshadow	Physical	RSRQ degrades, SINR drops, throughput reduced	High	[3]	Video quality failure
NAS Flooding	Signaling	Latency spike, ASU saturation, auth delays	High	[5,6,14]	Authentication failure
RRC Flooding	Signaling	Jitter increase, scheduler overload, PCI churn	Medium	[5,15]	Session drops
GTP Attack	Core	Throughput degradation, latency spikes	High	[8]	Data stream loss
Paging Storm	Signaling	Power increase, ASU overload, device battery drain	Medium	[14]	IoT device failure
Replay Attack	Protocol	Auth bypass risk, variable latency	Medium	[7,15]	Unauthorized access

3.2 Physical-Layer Attacks

Attacks against the physical layer, which include the attacks such as jamming and adaptive overshadowing by Erni et al. [3] and Lichtman et al. [4] respectively, affect the quality of the radio signal through the degradation of the signal at the UE. The attacks' impacts manifest themselves in a reduction of the RSRP and SINR values below the threshold levels necessary for the proper decoding process. Physical-layer attacks are very dangerous in telemedicine because they totally disconnect the medical device from the clinical server with no application-layer defenses able to handle a total disruption of the physical-layer signal.

3.3 Signaling and Protocol Attacks

The signaling attacks described by Yang and Wang [5], Basin et al. [6], Bitsikas et al. [7], Hussain et al. [14], and Shaik et al. [15] target the control plane processes carried out in the NAS and RRC layer. These kinds of attacks result in increasing the network's latency and jitter levels as well as the access delay. Importantly, signaling attacks may appear to keep a link connection established, while in reality, they lead to a reduction of QoS below the minimum clinically required value.

3.4 Core Network Attacks

The GTP-based attacks, according to Positive Technologies [8], happen at the core network level and affect user plane tunnels between radio access network and 5G core. They do not have a significant effect on air interface radio parameter values, which makes them less harmful compared to physical and signaling attacks, as well as harder to be detected using UE-side radio measurement data collection. To successfully detect the GTP-based attacks, one needs to use network-level telemetry from the 5G core together with air interface measurements.

4. TELEMEDICINE QOS REQUIREMENTS AND ATTACK IMPACT MAPPING

4.1 Clinical QoS Thresholds

The ITU-T [12] and healthcare informatics-related standards provide for an hierarchical approach to defining QoS requirements for various telemedicine use cases. Real-time synchronous video calls require latency below 150 ms, jitter

DOI: 10.17148/IJIREEICE.2026.14610

below 50 ms, and downlink throughput exceeding 10 Mbps for full HD quality. Constant monitoring of patient vital signs requires 99.9% availability and sub-second delivery time for critical alarms. High-throughput medical images transfer for such types of data transfer as radiology images and ultrasound videos is needed. Moreover, emergency telemedicine services should provide quality service even under degraded radio link conditions.

4.2 Attack-to-QoS Impact Mapping

Physica llayer jamming, as defined in the literature [4, 13], decreases both RSRP and SINR to a point where the decoding of the physical layer downlink is not possible by the UEs, leading to a reduction in throughput to zero. This breaks all the quality of service constraints of telemedicine simultaneously and results in an immediate disconnection from the current clinical consultation process. Meanwhile, adaptive overshadowing attacks [3] degrade the RSRQ and channel conditions in such a way that the downgrading of the adaptive coding and modulation techniques occurs, and this could result in a decrease of throughput under 10 Mbps of high-definition video.

Latency and jitter increase due to NAS flooding attacks [6, 14] and RRC flooding attacks [5, 15] exceed levels allowed under real-time consultation guidelines, whereas saturation of access slots prevents authentication and session establishment. A monitor that is subjected to continuous authentication processes because of a NAS flooding attack can be incapable of transferring its critical alarms in time, owing to a latency requirement of less than one second for this procedure. GTP attacks [8] result in throughput degradation and latency increase within the user plane comparable to QoS problems induced by congestion.

5. DETECTION METHODOLOGIES

5.1 Radio Parameter-Based Monitoring

From the reviewed literature, it is clear that the radio measurements taken on the UE side – RSRP, RSRQ, SINR, throughput, latency, and jitter represent the key measurable signs of an air interface attack. Erni et al. [3] show that the degradation in the ratio between RSRQ and RSRP constitutes the signature of the attack that distinguishes itself from the RSRP degradation resulting from path loss. Lichtman et al. [4] describe the specific RSRP/SINR threshold ranges observed under jamming attacks that differ from the values expected due to natural coverage limitations. This consideration justifies the utilization of radio measurement monitoring as the basis for detecting both types of attacks, except where indicated by Positive Technologies [8].

5.2 Machine Learning-Based Anomaly Detection

Apruzzese et al. [9] propose using ensembles of classifiers like Random Forest and Gradient Boosting for intrusion detection using feature sets of varying heterogeneity due to the high resistance to collinearity between features and the capability to learn non-linear decision boundaries. These characteristics can be beneficial in 5G wireless measurements because the values of radio parameters correlate in complex ways; specifically, RSRP and RSRQ correlate during path loss and become independent of each other under conditions of interference, which linear models might miss.

When unlabeled attack data is not available for the training process, Mirsky et al. [10] prove that an autoencoder is able to detect anomalies using only normal traffic instances. In terms of applying intrusion detection in health-care applications, this technique is attractive because it does not need attack data beforehand to recognize new attack vectors. As pointed out by the authors, the disadvantage associated with it is a relatively higher false positive rate compared to supervised learning methods.

5.3 Feature Engineering Recommendations

Based on the conclusions presented by Xiao et al. [11] along with the characteristic features identified by Erni et al. [3] and Apruzzese et al. [9], some of the critical features that should be included in ML-based 5G attack detection models are: (i) raw radio parameters (RSRP, RSRQ, SINR, throughput, latency, jitter); (ii) ratios between such parameters highlighting interference rather than path loss (e.g., RSRQ/RSRP deviations); (iii) rate-of-change values for detecting attack initiation patterns; and (iv) short-window statistical aggregates (average value, deviation, etc.). Such an approach was shown to substantially enhance the discriminability of attack classes over purely monitoring raw radio parameters.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026
DOI: 10.17148/IJIREEICE.2026.14610

6. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

6.1 Multi-Layer Attack Detection

The vast majority of existing solutions for detecting physical layer attacks, signaling attacks, and core network attacks consider each category of threats in isolation from one another. While this is generally a reasonable decision for practical deployment, hybrid attacks, which combine several types of attacks in parallel, can present significant challenges for current telemedicine security systems due to their ability to bypass detection mechanisms built to counter only one vector at a time.

6.2 5G Network Slicing and Healthcare Isolation

Network slicing in 5G provides the opportunity to allocate health traffic into isolated slices with guaranteed QoS, which could minimize the blast radius of the attacks on shared network infrastructure. Nevertheless, the issue of security isolation provided by the current generation of 5G slices requires further research attention. Further studies should focus on characterizing inter-slice attack propagation and designing monitoring tools tailored to clinical applications.

6.3 Privacy-Preserving Federated Detection

Attack detection frameworks using ML require training models based on clinical network data. Since such measurements contain sensitive location and behavior data, there are privacy concerns related to the application of ML. One way to address such concerns is applying the technique of federated learning where machine learning models will be jointly developed among hospitals without aggregating sensitive data from different sources. The problem of federated attack detection in 5G clinical environments remains unexplored.

6.4 Lightweight Detection for Medical IoT

A considerable portion of clinical IoT devices have stringent computational restrictions preventing the use of sophisticated machine learning techniques. This limitation calls for exploring lightweight detection algorithms for constrained medical devices including but not limited to the use of compression neural networks, rule-based statistical monitoring using decision boundaries defined by ML models, or cooperation-based attack detection.

7. CONCLUSION

The above survey conducted to identify possible 5G air interface security threats in terms of telemedicine reliability has resulted in seven attack categories being identified, namely, physical layer jamming, adaptive overshadowing, NAS flooding, RRC flooding, GTP attacks, paging storms, and replay attacks, all of which have been documented in the literature. The attacks have been analyzed in terms of their signatures in terms of radio parameters in relation to the telemedicine QoS thresholds.

The literature on the use of machine learning techniques to detect security threats in 5G networks surveyed in the areas of supervised learning, unsupervised learning, and feature engineering indicates that there is a solid methodological approach to protect healthcare communication networks enabled by 5G technology. Ensemble classifiers can successfully be used to detect most of the attacks mentioned above except GTP attacks performed on core network equipment.

The contributions made by this study can be summarized as follows: (i) a comprehensive analysis of the relationship between the literature on 5G security and telemedicine QoS in the wireless networks domain, both of which have evolved largely independently; (ii) a threat categorization scheme with specific telemedicine risk labels obtained from medical QoS standards; (iii) a discussion on the methods of ML for attack detection in the context of radio measurement data feature extraction; and (iv) highlighting potential research topics such as multi-level attack detection, network slicing security, federated learning, and lightweight IoT-side attack detection systems.

REFERENCES

[1] 3GPP TS 22.261 V17.8.0, "Service requirements for the 5G system," 3rd Generation Partnership Project, Release 17, Mar. 2022.
[2] Khan, R., Kumar, P., Jayakody, D. N. K., and Liyanage, M., "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196-248, First Quarter 2020.

DOI: 10.17148/IJIREEICE.2026.14610

[3] Erni, S., Kotuliak, M., Leu, P., Roeschlin, M., and Capkun, S., "AdaptOver: Adaptive overshadowing attacks in cellular networks," in Proc. 28th Annual International Conference on Mobile Computing and Networking (ACM MobiCom), Sydney, NSW, Australia, Oct. 2022, pp. 98-111.

[4] Lichtman, M., Poston, J. D., Amuru, S., Shahriar, C., Clancy, T. C., Buehrer, R. M., and Reed, J. H., "A communications jamming taxonomy," IEEE Security & Privacy, vol. 14, no. 1, pp. 47-54, Jan.-Feb. 2016.

[5] Yang, J. and Wang, Y., "Formal and fuzzing amplification: Targeting vulnerability detection in 5G and beyond," arXiv preprint arXiv:2307.05758, Jul. 2023. [Online]. Available: https://arxiv.org/abs/2307.05758

[6] Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., and Stettler, V., "A formal analysis of 5G authentication," in Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS), Toronto, Canada, Oct. 2018, pp. 1383-1396.

[7] Bitsikas, E., Khandker, S., Salous, A., Ranganathan, A., Piqueras Jover, R., and Popper, C., "UE security reloaded: Developing a 5G standalone user-side security testing framework," in Proc. 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Guildford, U.K., May-Jun. 2023, pp. 31-42.

[8] Positive Technologies, "Vulnerabilities in LTE and 5G networks 2020," Positive Technologies Research, Technical Report, 2020. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/lte-5g-vulnerabilities-2020/

[9] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., and Marchetti, M., "On the effectiveness of machine and deep learning for cyber security," in Proc. 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, May 2018, pp. 371-390.

[10] Mirsky, Y., Doitshman, T., Elovici, Y., and Shabtai, A., "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2018.

[11] Xiao, L., Wan, X., Lu, X., Zhang, Y., and Wu, D., "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41-49, Sep. 2018.

[12] ITU-T Focus Group on Artificial Intelligence for Health, "Assessment of Machine Learning Solutions for Telemedicine QoS over 5G Networks," Technical Report FG-AI4H-DEL-12.1, International Telecommunication Union, Geneva, Switzerland, 2021.

[13] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., and Gurtov, A., "5G security: Analysis of threats and solutions," in Proc. IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, Sep. 2018, pp. 1-6.

[14] Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., and Bertino, E., "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2019.

[15] Shaik, A., Borgaonkar, R., Park, S., and Seifert, J.-P., "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in Proc. 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Miami, FL, USA, May 2019, pp. 221-231.