International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

A Comprehensive Review of Security Challenges and Physical Layer Security in 6G Wireless Networks

Madhuri Verma
BM College of technology, indore
madhurigupta1107@gmail.com
Mohit Jain
bmctmohitcs@gmail.com

Abstract -This survey reviews the evolution of mobile network security from 1G to 6G, with a particular focus on the security challenges, requirements, and enabling technologies of sixth-generation wireless networks. It highlights the limitations of existing 5G security mechanisms in supporting emerging 6G applications, including the Internet of Everything (IoE), artificial intelligence (AI), edge computing, network slicing, and non-terrestrial networks. The study examines security threats associated with new technologies and discusses key requirements such as zero-trust architecture, privacy preservation, virtualization security, post-quantum cryptography, and AI-driven protection mechanisms. It also summarizes recent research on Physical Layer Security (PLS), reinforcement learning, reconfigurable intelligent surfaces (RIS), and machine learning-based security frameworks for secure 6G communication. Finally, the survey identifies major research gaps and outlines future directions for developing intelligent, adaptive, and resilient security solutions for next-generation wireless networks.

Keywords: 6G Networks, Physical Layer Security (PLS), Artificial Intelligence (AI), Machine Learning (ML),

1. INTRODUCTION

Features such as guarantyd low latency, mass connectivity, and extreme reliability were specified by the fifth-generation (5G) radio networks that were used worldwide by 2020. Conversely, 5G won't be able to suit all of our demands after 2030. Expected benefits of 6G wireless network technology include enhanced security, less power usage, wider coverage, and lower overall costs. 6G networks will implement innovative features including multiple accesses, waveform design, channel coding techniques, network slicing, numerous antenna technologies, and cloud edge computing to fulfilll these demands. "6G" has an impact on four major shifts in the future [2]. As a first step, it provides a terrestrial and non-terrestrial network integration for air, ground, space, and sea communication [3]. And secondly, millimeter-wave (mm-wave), sub-6 GHz, terahertz (THz), and optical communications are some of the emerging radio bands that will increase the capacity and speed of network traffic. Third, in reaction to the enormous datasets produced by heterogeneous networks with diverse communication scenarios, new 6G applications' needs, wide bandwidths, and an increased number of antennas, 6G will make possible a new wave of intelligent applications and services that leverage artificial intelligence (AI) and big data technologies [4–7]. On the fourth point, 6G technology and applications necessitate improved network security and privacy [8]. 6G security trends and difficulties of other emerging technologies and applications are presented in this study. In 6G networks, the most important concerns are data encryption, traffic analysis,

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

threat detection, and data processing. Utilising decentralised security systems, where traffic may be managed locally and dynamically, can resolve the security challenges caused by enormous traffic processing. There are more stringent security requirements for 6G use cases compared to 5G use cases [9,10]. It will be more difficult to run and implement distributed artificial intelligence (AI), privacy, and security solutions due to the IoE's extensive capabilities and services. More security and privacy issues arise as a result of the new connected devices' increased mobility, which causes them to alter their interconnected networks and rely on services from other networks. Reduce the end-to-end latency in 6G to a few microseconds for the Enhanced Ultra-Reliable and Low Latency Communication (ERLLC) services. Plus, network energy efficiency needs to be increased by a factor of 100 over 4G and ten over 5G for 6G to be feasible [11]. To put it another way, it's expected to make low-power broadcasts possible for devices with limited resources. Speeds of up to 1,000 km/h will be possible with the help of active and revolutionary mobility management systems. Reviewing the impact of security measures on latency is essential for ensuring ERLLC service quality. Likewise, efficient security solutions are required for high requirements in order to guarantee the availability of services and resources. The latest distributed intelligent AI and ML security solutions experience difficulties in deployment and operation due to the IoE. Finding ways to integrate new security enablers into devices with limited resources is a decisive factor [12]. The data speeds, reliability, latency, and localisation accuracy comparison between 5G and 6G is summarised in Figure 1.

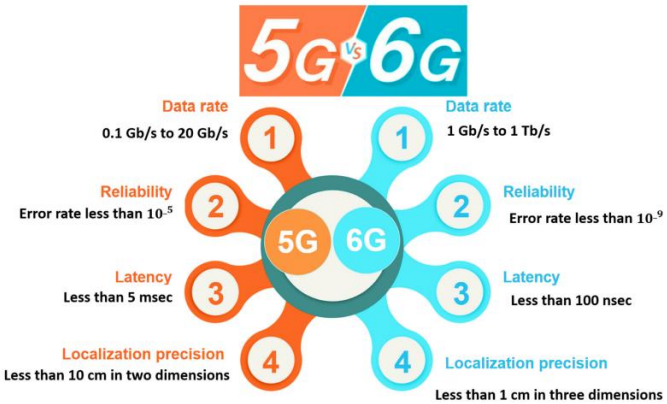

Figure 1. The 5G and 6G features comparison

This study covers all the bases when it comes to security and privacy issues with 6G networks. By highlighting the security flaws in current solutions, we brie⇘y present the evolution of security in mobile radio from 1G to 5G. We look into the 6G security issues in various important domains. The research also details the security needs and concerns of 6G technologies and applications. Afterward, we suggest ways to address the new 6G uses. This paper takes into account one of the first studies to incorporate a comprehensive study for the possible solutions to the security issues with 6G new technology [13,14].

Security Evolution of Mobile Cellular Networks

The section delves into the various security vulnerabilities and privacy problems associated with different generations of cellular networks. Cryptography, physical threats, eavesdropping, and authentication were all major security concerns for the first generation of mobile devices.

This has led to an increase in both the sophistication and frequency of attacks, broadening the scope of the threat landscape.

Security Issues in 1G, 2G, and 3G

Designed from the ground up to provide voice communications services, the 1G network came into being in the 1980s. To transmit information, it employs analogue modulation methods. There are a number of drawbacks with this generation, including transmission challenges, no security guarantees, and difficulty with handovers. Furthermore, data transmission cannot be assured to be secure or private because telephone services are not secured. Consequently, there are major security risks to the network and its users, such as eavesdropping and unauthorised access [15].

In order to support voice and short message services, the second generation of mobile devices rely on digital modulation protocols like Time Division Multiple Access (TDMA). Authentication, privacy, transmission, and personal information protection are all part of the security services provided by the GSM (Global System for Mobile Communications) standard [16]. If a user wants to access a provider's network, they must first authenticate with that provider [17]. A challenges and replies strategy forms the basis of the 2G authentication method. Their true identities cannot be traced because they use anonymous identifiers. User data and signalling are protected by encryption, with the keys for this encryption being generated by the SIM. Users can protect their privacy by utilising radio path encryption and Temporary Mobile Subscriber Identity (TMSI) [18]. The security of 2G networks is still somewhat weak, despite significant improvements over 1G networks. When a network verifies a user's identity, but the user is unable to verify their identity to the network, this is known as a three-way authentication issue [19]. Consequently, malicious base stations pose as legitimate members in order to collect sensitive user data.

Additionally, when only a portion of the communication route is encrypted, the end-to-end encryption problem arises. Meanwhile, the channel is vulnerable to attacks because the other sections of the network are not encrypted. Consequently, 2G networks are vulnerable to a variety of assaults, including eavesdropping, and the aforementioned TMSI privacy solutions and radio channel encryption are inadequate [20]. In order to enable internet access and boost data transmission speeds up to 2 Mbps, the 3G network was launched in 2000. On the other hand, at this speed, advanced services like streaming TV, browsing the web, and video are available, which was not possible with earlier mobile communication [21]. The security of 3G networks is based on 2G technologies. In addition, 3G fixes many security issues with 2G, such as the Authentication and Key Agreement (AKA) and two-way authentication [22]. A comprehensive system for controlling access, including safeguards for air interfaces and user identification, is set up by the Third Generation Partnership Project (3GPP). Safeguarding user and network communications via wireless connections is the job of the air interface security. Also, for added security, it has a two-way authentication mechanism that verifies the sender and the receiver's identities as well as the network.

When it comes to 3G networks, the 3GPP backs a number of privacy concerns, such as the safe way to identify, track, and locate users. 3G networks are at risk from attacks and weaknesses related to the Internet Protocol (IP) [24]. 3G networks are vulnerable to assaults on the

communication channels that link end devices to their home networks. Integrity risks, unauthorised data access, denial of service (DoS) assaults, and unauthorised service access are the four main types of wireless interface threats. AKA protocol privacy concerns involving the eavesdropping on users' personal data and identities are

Security Issues in 4G and 5G

In 2009, 4G networks were able to provide up to 500 MBit/s for uplink communication and 1 Gbit/s for downstream transmission [25]. With their reduced latency and great spectrum efficiency, 4G networks can manage demanding applications like digital video broadcasting and high-definition television (HD TV). A variety of intelligent mobile terminals, IP core networks, backbone networks, and access networks make up 4G systems. Threats to 4G's main security include tampering, eavesdropping, data manipulation, network authentication, and wireless radio transmission. The 4G network is more susceptible to security concerns than earlier mobile radio networks because of the increased indirect connection between users and mobile terminals. The advancements in storage and computational capabilities of mobile terminal devices have a devastating effect on many security concerns. Examples of security issues include viruses, attacks on operating systems, and tampering with hardware platforms. Eavesdropping and replay attacks are two of the many Medium Access Control (MAC) layer vulnerabilities that affect 4G standards and essential management protocols. Data integrity assaults, unauthorised user difficulties, and location tracking utilising MAC layer protocols are additional potential threats to 4G networks.

With the 5G network getting closer to its commercial launch, we might see faster data transfers thanks to more intricate systems and more secure designs. The innovative feature of 5G networks is their ability to link an increasing number of devices while simultaneously providing all network nodes with better quality services. Looking at the network design is the simplest way to classify 5G security and privacy concerns. Three types of networks—access, backhaul, and core—make up the 5G architecture. There are a lot of devices and ways to access networks that pose extra security risks. The likelihood of an attack is further increased during handoffs between various access technologies and device kinds [25]. Microwave links, wireless channels, satellite connections, and conventional telephone lines make up the backhaul networks that connect the access and core networks. There are fewer privacy concerns with backhaul networks compared to access networks due to the fact that they slack devices' connections. Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) are two methods that bring security concerns to the core network by transferring the backhaul network to the data plane [26]. The increased risk of denial-of-service (DoS) and resource attacks is a security concern with the high data rates of Further Enhanced Mobile Broadband (FeMBB). At this time, there are two approaches that can handle signalling overloads. The first uses lightweight authentication and key management approaches to provide communication between several devices, and the second uses protocols to enable device grouping using numerous group-based AKA protocols. The 5G network's speed can be increased by new technologies, however these approaches also introduce security concerns. To conceal both active and passive eavesdropping, for instance, huge MIMOs are employed. Furthermore, malicious apps or actions can be a problem when using Open Flow for SDN

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

implementation.

There are security concerns with NFV services since they move resources around. Additional privacy concerns arise from a wide variety of 5G network-useful application scenarios and service types. The open nature of the 5G technology makes user data freely accessible to the public [27]. The privacy concerns surrounding 5G will definitely emerge as an issue in the next years that needs to be resolved. Various features make up the 5G CN. Numerous risks and weaknesses have emerged as a consequence of the increased dynamism of networks brought about by NFV, SDN, and cloud computing. New 6G applications will have higher criteria and more capacity than current 5G networks, as the number of devices and services that surpass the signalling load increases [28]. Compared to the current 5G networks, the new 6G applications will require higher network capacity and have more criteria. On top of that, they significantly affect 6G operations. As a result, ERLLC ensure both service continuity and quality through security measures. We will also handle the latency effect that is caused by security processes. To guarantee the availability and continuity of services and resources, effective security solutions are highly required. From 1G to 6G, changes and security concerns are summarised in Figure 2.

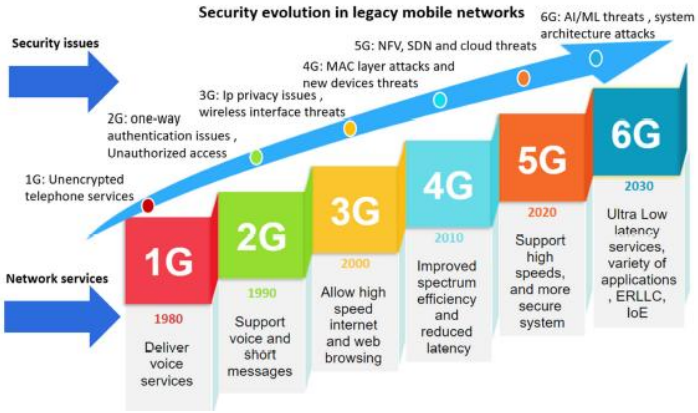

Figure 2. The security evolution of mobile communications from 1G to the predicted future 6G

The 6G Essential Projects

The creation of comprehensive plans for the 6G wireless network's future is currently the focus of all efforts. There will be over EUR 95 million invested in B5G and 6G research from 2017 to 2025, according to [28]. Horizon2020, the European Union's program for research and innovation, is funding these endeavours. Plus, the majority of them have only just begun to develop. Several of these trials and the lessons they have taught us on 6 G securities are the topic of this section.

Hexa-x

In 2021, Ericsson initiated the Hexa-x project [29]. This project is an effort to bring cutting-edge innovations to market through collaboration between several research institutions and universities. 6G network infrastructure is what the Hexa-x project is trying to build. Also, it hopes to be the global leader in R&I for the upcoming generation. To better provide 6G networks to Europe, this initiative is trying to develop tools that are important. Connecting intelligence, a network of networks, sustainability, worldwide service coverage, trustworthiness, and extreme experience are the six difficulties that will be addressed in

innovative ways. Hexa-x will address these issues by developing many axs [30]. If we want better connection quality when humans and electronics communicate, we need to use new technologies like AI and ML. One network of networks must be established by the worldwide digital ecosystem. This network ought to be diverse, smart, and adaptable. Efficient utilisation of resources is crucial for a network to last. For the 6G network to have full coverage around the world, practical and affordable solutions are needed. For top-notch protection, the following generation must provide secrecy, operational resilience, data privacy, and communication integrity. To further improve 6G's performance, many technologies will be developed, including design of networks, air interfaces powered by AI, THz radio access, and virtualisation of networks. Using these innovative communication tools, the initiative will bring the digital, physical, and human realms closer together.

RISE 6G

One of the notable projects that was announced in 2021 is RISE 6G, which stands for Reconfigurable Intelligent Sustainable Environments for 6G wireless networks [31]. This project makes use of RIS technology, which stands for Reconfigurable Intelligent Surfaces. RIS has the potential to grow into a formidable emerging technology. Controlling the propagation of radio waves is an area that RIS focuses on. It paves the way for wireless environments to be perceived as services. By utilising RIS, RISE 6G aims to enhance 6G capabilities for an intelligent, adaptable, and environmentally friendly wireless ecosystem. There are four RIS-related obstacles that the project must overcome. The real transmission of the signal helped by RIS will first be modelled. Second, a number of RISs will be included into the redesigned network architecture. Third, in order to enhance quality of service, various use cases will be developed. These use cases will address issues such precise localisation, environmentally friendly communication, power consumption, and large capacity within a dynamic wireless programmable environment. In the fourth place, two supplementary sessions will be used to propose a prototype standard for originality. Incorporating its technological concept into industrial implementation, the initiative takes part in standardisation [32].

New-6G

The focus of the NEW-6G project is the nanoscale universe. As stated in the project description, it brings together "microelectronic with telecom, network with equipment, and software with hardware." In essence, the project's goal is to improve the network's performance by creating new techniques and technologies, such [64]:

Next G Alliance

The Next G Alliance was established in the US by ATIS (Alliance for Telecommunications Industry Solutions) toward the year 2020's close. ATIS's mission is to bring 6G to North America and establish 6G as a leader in the industry [33]. Commercialisation of technology is its primary aim; this process includes R&D output, standardisation, and market preparedness. Future standards may be significantly impacted by the member organisations' influence on important actors in mobile communications. Innovations and standards in industry will be strategically examined by the Next G Alliance. The goal is to start a global conversation about standards and the need for government and business to work together. The expansion of numerous large companies is directly related to the rise of mobile technologies. Growing

reliance on mobile technology is a nationwide trend in numerous industries, including aerospace, agribusiness, defence, education, healthcare, manufacturing, media, energy, and transportation. It is imperative that North America continues to lead the way in mobile technology for these vital sectors.

G Security Requirements and Proposed Security Architecture

This section discusses the 6G security requirements and the security architecture.

6G Security Architecture Requirements

Transparency is key to the 6G system security architecture's design. As 6G is designed to be a more open network compared to 5G, the boundary between the network and the outside world will gradually fade. Consequently, the network will be vulnerable to intrusions beyond the capabilities of present network security solutions like IPsec and firewalls. To address this, the 6G security architecture should bolster the mobile communication network's foundational security principle of zero trust (ZT). The primary focus of the Zero Trust security paradigm is the safeguarding of system resources. In zero-trust scenarios, an attacker resides inside the network and the network's design is either easily accessible or unreliable from the outside. To lessen the likelihood of internal asset loss, such an evaluation has to be conducted on a frequent basis and measures must be implemented. Network entities (NEs), protocol processes, and access rules are all parts of zero trust architecture (ZTA), a security architecture based on the zero trust concept (ZT). For that reason, 6G security architecture should revolve around ZTA. The ZT idea can help with managing some security requirements for 6G networks. We outline the 6G networks' security architecture's management and handling responsibilities in the following paragraphs.

Virtualization Security Solution: If you're worried about hidden malicious software like root kits, you should use a system with a secure virtualisation layer. This layer will detect and prevent virtualisation security breaches. Furthermore, the hypervisor needs to make it possible to completely separate the storage, computation, and network of various network services through the use of secure protocols like TLS, SSH, VPN, and others. The hypervisor's virtual machine introspection (VMI) function checks each VM's register information, file IO, and communication packets for signs of tampering and other security issues. The operating system should restrict the mounting of essential system directories and direct access to the host device file container when employing containerisation, and it should suitably set the rights of the individual containers.

Automated Management System: The most critical step in fixing open source security problems is controlling vulnerabilities that arise from using, updating, and removing open sources. Since this is the case, an automated management system that can find security holes and install fixes is essential for rapid threat detection. To make sure the patched software is applied securely and swiftly utilising the secure OTA technique, an extra step is required. In addition, a security governance framework needs to be put in place to deal with three things: (1) long-term open source vulnerabilities, (2) changes in developer perspective, and (3) security solution deployment.

Using AI for data security: In order to ensure that AI systems are free from anti-money laundering risks, companies must be open and honest about the measures they take to protect

their users and the mobile communication system. The initial stage is to build AI models in a reliable system. Also, digital signatures or some other way needs to be put in place to check if the core, RAN, and user equipment (UE) AI models have been updated or changed maliciously. System recovery or self-healing procedures are required in the event that a malicious AI model is detected. Furthermore, the system should only collect data from reliable network components in order to train AI.

Users' Privacy-preserving: Service providers, mobile network operators (MNOs), subscribers, and MNOs should all work together to safeguard users' personal information by storing and using it in line with agreed-upon standards. While using the 6G system, personal information is kept secure in a trustworthy execution environment (TEE) and reliable SW. Additionally, the quantity of information that is made publicly available is reduced or anonymised. Verification of identity and permission is necessary prior to MNO disclosing any personally identifiable information. Utilising homo morphi cencryption (HE) is another alternative for encrypting user data before accessing it. Another option for protecting the user's location and usage habits is to employ AI-based solutions, including a privacy-aware offloading scheme that is learning-based.

Post-Quantum Cryptography: Because of the security risks posed by quantum computers, the 6G system must do away with current asymmetric key encryption solutions. A lot of people have been looking on post-quantum cryptography (PQC) solutions, which include approaches like hash-based signatures, code-based cryptography, multivariate polynomial cryptography, and lattice-based cryptography. The United States' National Institute of Standards and Technology (NIST) plans to select the top PQC algorithms for its study sometime between 2022 and 2024. The key length being considered for PQC is expected to be significantly longer than Rivest-Shamir-Adleman (RSA). Compared to the existing RSA approach, the computational cost of PQCs is anticipated to be higher. There must be proper integration of PQC into the 6G network's HW/SW performance and service requirements for this reason.

2. LITERATURE REVIEW

Ara et al. (2024) Emphasis on Physical Layer Security (PLS) as a core 6G network security mechanism. According to the research, ultra-dense 6G settings necessitate integrated security starting from the communication phase. Lightweight protection for heterogeneous devices and support for safe data transmission in networks with limited resources are both provided by PLS [34].

Chorti et al. (2022) delivered an extensive analysis of 6G network Physical Layer Security methods that leverage machine learning. Secure transmission, authentication, anti-jamming, and key generation were all covered in the study that was based on artificial intelligence. It also mapped out where the field should go from here in order to develop 6G communication systems that are both smart and secure [35].

Chou et al. (2024) explore 6G-IoT network Physical Layer Security with the help of Reconfigurable Intelligent Surfaces (RIS). Through optimised beamforming and resource allocation, the study showed that RIS increases protection against eavesdropping and jamming. Future optimisation difficulties for security enabled by RIS were also covered. [36].

Irram et al. (2022) suggested an architecture for Physical Layer Security that takes context into account for communication systems that go beyond 5G and 6G. Security techniques that are adaptable, versatile, and simple enough to be used in intelligent wireless environments were the focus of the study. It demonstrated how important QoSec will be for the future of network security [37].

Kelley et al. (2022) introduced an AI-assisted Physical Layer Security framework using deep neural networks for 6G communication. The proposed model significantly improved signal quality and secrecy performance compared with conventional methods. The study also presented an AI-enabled secure O-RAN architecture [38].

Khalid et al. (2024) reviewed channel-based Physical Layer Security for future wireless networks. The authors discussed advanced sensing, signal processing, and channel control techniques to strengthen communication security. The study also outlined challenges and future research opportunities [39].

Kihero et al. (2024) examined RIS-assisted NOMA communication to improve Physical Layer Security in 6G networks. The proposed beamforming and power allocation strategies enhanced secrecy performance against internal and external eavesdroppers. Simulation results confirmed the effectiveness of the proposed approach [40].

Lu et al. (2023) reviewed reinforcement learning-based physical and cross-layer security for 6G communication systems. The study showed that RL algorithms effectively protect against jamming, spoofing, and privacy attacks without requiring prior attack models. Future research directions were also discussed [40].

Table 1 Summary of Literature on Physical Layer Security in 6G Networks

No.	uthor(s) & Year	Study Focus	Methodology / Technology	Key Findings	Research Gap
	a et al. (2024)	ysical Layer Security (PLS) for 6G	view of PLS techniques	pposed PLS as the first line of defense for heterogeneous 6G networks.	nited implementation of intelligent real-time security mechanisms.
	orti et al. (2022)	-enabled PLS in 6G	mprehensive survey	viewed ML-enabled PLS for MIMO, THz, VLC, RIS, IoT and anti-jamming.	ck of practical deployment and benchmark evaluation.
	ou et al. (2024)	S-assisted PLS for 6G IoT	S, beamforming, artificial noise	S significantly improves secrecy against jamming and eavesdropping.	timization complexity and channel estimation remain challenging.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

	am et al. (2022)	ntext-aware security	Sec and PLS framework	roduced adaptive context-aware physical layer security for Beyond-5G/6G.	nited real-world implementation and validation.
	lley et al. (2022)	-based PLS	ep Neural Network-based detection	proved BER and secrecy with 10–15 dB SNR gain.	mputational complexity for large-scale networks.
	alid et al. (2024)	annel characteristics for PLS	rvey	scussed new channel features and sensing technologies for future PLS.	ndardized channel selection criteria unavailable.
	hero et al. (2024)	S-NOMA Security	amforming and power allocation	hanced secrecy performance using optimized RIS configuration.	I uncertainty affects system performance.
	et al. (2023)	inforcement Learning for Security	-based cross-layer security	effectively mitigates spoofing, jamming and privacy attacks.	gh computational overhead and slow convergence.
	hmoud et al. (2024)	cure URLLC	-enabled PLS	viewed PLS techniques for secure URLLC and HRLLC.	ture 6G applications require adaptive security models.
	cchi et al. (2024)	ge AI for 6G NTN	-enhanced PLS	ge AI strengthens physical layer protection in non-terrestrial networks.	egration issues in heterogeneous environments.
	dhan et al. (2024)	ep Learning Security Framework	brid Deep Learning	proved attack detection accuracy and BER significantly.	rge datasets and lightweight models still needed.
	aji et al. (2026)	C Authentication	lti-RIS architecture	hieved transmitter authentication using channel variability.	alability and mobility support remain open issues.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

	deri et al. (2024)	S Fundamentals	rvey and coding techniques	plained secrecy capacity, coding, and wiretap channels.	actical deployment challenges remain unresolved.
	deri et al. (2022)	C Security	atermark Blind PLS	mbined watermarking with RGB LED jamming to improve secrecy.	rformance under dynamic environments not studied.
	ese et al. (2026)	S in 5G/6G	mprehensive review	viewed AI/ML-enabled PLS across HetNets, IoT, UAV and NOMA.	ified AI-based security architecture absent.
	ang et al. (2024)	-enabled PLS	rvey	substantially enhances detection, privacy and intelligent security.	plainable AI and trustworthy models require further study.
	ng et al. (2024)	elligent 6G Security	ep Learning + PLS	posed native AI-driven privacy layer for 6G air interface.	perimental validation in large-scale networks lacking.
	mpong et al. (2023)	egular RIS	bu Search Optimization	IS improves secrecy rate and spatial diversity.	rdware implementation complexity remains high.
	meed et al. (2025)	S-assisted IoT Security	S with Controlled Jamming	hanced PLS performance for WPCN-based IoT applications.	ergy-efficient optimization requires further investigation.
	eed et al. (2025)	Security Architecture	mprehensive Survey	viewed physical, connection and service layer security solutions.	ndardized integrated security framework is still unavailable.

3. CONCLUSION

Based on the findings of the assessment, security measures for 6G networks will need to be much more sophisticated than those of earlier mobile generations. 6G environments that are enabled by AI, highly dynamic, and heterogeneous pose security challenges that traditional cryptographic techniques cannot solve on their own. When it comes to safeguarding future wireless communications from ever-changing cyber threats, emerging technologies like

Reconfigurable Intelligent Surfaces, Artificial Intelligence, Physical Layer Security, and Reinforcement Learning provide encouraging alternatives. There are still unanswered questions about practical implementation, privacy protection, computational difficulty, compatibility, and scalability. As a result, researchers should put their energy into creating standardised security frameworks that are smart, adaptable, and lightweight so that they can guarantee privacy, availability, confidentiality, and integrity across all 6G services and applications. Potential for the Future

The next generation of 6G networks will have security frameworks that are intelligent, adaptive, and lightweight; these will be able to protect communication in very dynamic and heterogeneous situations. Research in the future should focus on integrating AI, ML, PLS, and ZTA to tackle issues like real-time threat detection, authentication, and privacy preservation. More study into blockchain-enabled security, secure edge computing, Post-Quantum Cryptography (PQC), and reconfigurable intelligent surfaces (RIS) is required to address emerging cyber threats. Secure, reliable, and resilient next-generation wireless communication systems should be the goal of future research. To get there, we need to standardise, scale, implement security mechanisms that are energy efficient, and validate these solutions using large-scale 6G deployments.

References

1. Khan, R.; Kumar, P.; Jayakody, D.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Commun. Surv. Tutor. 2020, 22, 196–248.
2. Yazar, A.; Dogan-Tusha, S.; Arslan, H. 6G vision: An ultra-flexible perspective, ITU. J. Future Evol. Technol. 2020, 1, 121–140.
3. Alwis, C.; Kalla, A.; Pham, Q.-V.; Kumar, P.; Dev, K.; Hwang, W.-J.; Liyanage, M. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. IEEE Open J. Commun. Soc. 2021, 2, 836–886.
4. Ray, P.; Kumar, N.; Guizani, M. A Vision on 6G-Enabled NIB: Requirements, Technologies, Deployments, and Prospects. IEEE Wirel. Commun. 2021, 28, 120–127.
5. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening new horizons for integration of comfort, security, and intelligence. IEEE Wirel. Commun. 2020, 27, 126–132.
6. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.-J.A. The Roadmap to 6G: AI Empowered Wireless Networks. IEEE Commun. Mag. 2019, 57, 84–90.
7. Sheth, K.; Patel, K.; Shah, H.; Tanwar, S.; Gupta, R.; Kumar, N. A taxonomy of AI techniques for 6G communication networks. Comput. Commun. 2020, 161, 279–303.
8. Yang, H.; Alphones, A.; Xiong, Z.; Niyato, D.; Zhao, J.; Wu, K. Artificial-Intelligence-Enabled Intelligent 6G Networks. IEEE Netw. 2020, 34, 272–280.
9. Huang, T.; Yang, W.; Wu, J.; Ma, J.; Zhang, X.; Zhang, D. A Survey on Green 6G Network: Architecture and Technologies. IEEE Access 2019, 7, 175758–175768.
10. Rupprecht, D.; Dabrowski, A.; Holz, T.; Weippl, E.; Popper, C. On security research towards future mobile network generations. IEEE Commun. Surv. Tutor. 2018, 20, 2518–2542.
11. Pereira, V.; Sousa, T. Evolution of Mobile Communications: From 1G to 4G; Department

of Informatics Engineering, University of Coimbra: Coimbra, Portugal, 2004.
12. Goyal, J.; Singla, K.; Singh, S. A Survey of Wireless Communication Technologies from 1G to 5G. In Seond International Conferenceon Computer Networks and Inventive Communication Technologies; Springer: Berlin/Heidelberg, Germany, 2019; pp. 613–624. 13. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. Comput. Netw. 2019, 162, 106871.
13. Li, Y.; Yu, Y.; Susilo, W.; Hong, Z.; Guizani, M. Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. IEEE Wirel. Commun. 2021, 28, 63–69
14. Kato, N.; Mao, B.; Tang, F.; Kawamoto, Y.; Liu, J. Ten Challenges in Advancing Machine Learning Technologies toward 6G. IEEE Wirel. Commun. 2020, 27, 96–103. [CrossRef]
15. Ramezani, P.; Jamalipour, A. Toward the Evolution of Wireless Powered Communication Networks for the Future Internet of Things. IEEE Netw. 2017, 31, 62–69.
16. Pelkmans, J. The GSM Standard: Explaining a success story. J. Eur. Public Policy 2001, 8, 432–453.
17. Cattaneo, G.; Maio, G.; Faruolo, P.; Petrillo, U.F. A review of security attacks on the gsm standard. In Information and Communication Technology; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; pp. 507–512.
18. Gope, P.; Hwang, T. Enhanced secure mutual authentication and key AGREEMENT scheme preserving user anonymity in global mobile networks. Wirel. Pers. Commun. 2015, 82, 2231–2245.
19. Brookson, C. Gsm security: A description of the reasons for security and the techniques. In Proceedings of the IEE Colloquium on Security and Cryptography Applications to Radio Systems, London, UK, 3 June 1994; pp. 2/1–2/4.
20. Arapinis, M.; Mancini, L.I.; Ritter, E.; Ryan, M. Privacy through pseudonymity in mobile telephony systems. In Proceedings of the 2014 Network and Distributed System Security Symposium, San Diego, CA, USA, 23–26 February 2014.
21. Karjaluoto, H. An investigation of third Generation (3g) mobile technologies and services. Contemp. Manag. Res. 2007, 2, 91.
22. Saxena, N.; Chaudhari, N.S. Secure-aka: An efficient aka protocol for umts networks. Wirel. Pers. Commun. 2014, 78, 1345–1373
23. Jefferies, N. Security in Third-Generation mobile systems. In Proceedings of the IEE Colloquiumon Security in Networks, London, UK, 3 February 1995.
24. La Porta, T.F. Security and IP-based 3G wireless networks. In Proceedings of the 14th International Conference on Computer Communications and Networks, San Diego, CA, USA, 17–19 October 2005; p. 211.
25. Zahariadis, T.; Kazakos, D. (R) evolution toward 4G mobile communication systems. IEEE Wirel. Commun. 2003, 10, 6–7.
26. Bikos, A.N.; Sklavos, N. LTE/SAE security issues on 4G wireless networks. IEEE Secur. Priv. 2013, 11, 55–62.
27. Park, Y.; Park, T. A survey of security threats on 4G networks. In Proceedings of the 2007 IEEE Globecom Workshops, Washington, DC, USA, 26–30 November 2007; IEEE:

Piscataway, NJ, USA, 2007; pp. 1–6.
28. Goyal, P.; Batra, S.; Singh, A. A literature review of security attack in mobile ad-hoc networks. Int. J. Comput. Appl. 2010, 9, 11–15.
29. Kim, S.J.; Lee, H.; Lee, M. A Study of 4G Network for Security System. Int. J. Adv. Cult. Technol. 2015, 3, 77–86.
30. Mohapatra, S.K.; Swain, B.R.; Das, P. Comprehensive survey of possible security issues on 4G networks. Int. J. Netw. Secur. Its Appl. 2015, 7, 61–69.
31. Panwar, N.; Sharma, S.; Singh, A.K. A survey on 5G: The next generation of mobile communication. Phys. Commun. 2016, 18, 64–84.
32. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A surveyon 5G networksfor the internetof things: Communication technologies and challenges. IEEE Access 2018, 6, 3619–3647.
33. Wang, C.-X.; Haider, F.; Gao, X.; You, X.-H.; Yang, Y.; Yuan, D.; Aggoune, H.; Haas, H.; Fletcher, S.; Hepsaydir, E. Cellular architecture and key technologies for 5G wireless communication networks. IEEE Commun. Mag. 2014, 52, 122–130.
34. Ara, I., & Kelley, B. (2024). Physical layer security for 6G: Toward achieving intelligent native security at Layer-1. IEEE Access, 12, 82800–82824. https://doi.org/10.1109/ACCESS.2024.3413047
35. Chorti, A., Barreto, A. N., Köpsell, S., Zoli, M., Chafii, M., & Sehier, P. (2022). Context-aware security for 6G wireless: The role of physical layer security. IEEE Communications Standards Magazine, 6(1), 102–108. https://doi.org/10.1109/MCOMSTD.0001.2000082
36. Chou, H.-F., Solanki, S., Ha, V. N., Chen, L., Ma, S. L., Al-Hraishawi, H., Eappen, G., & Chatzinotas, S. (2024). Edge AI empowered physical layer security for 6G NTN: Potential threats and future opportunities. arXiv. https://arxiv.org/abs/2310.01725
37. Irram, F., Ali, M., Naeem, M., & Mumtaz, S. (2022). Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions. Journal of Network and Computer Applications, 206, 103431. https://doi.org/10.1016/j.jnca.2022.103431
38. Kelley, B., & Ara, I. (2022). An intelligent and private 6G air interface using physical layer security. In Proceedings of the 2022 IEEE Military Communications Conference (MILCOM) (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM55135.2022.10017638
39. Khalid, W., Ur Rehman, M. A., Chien, T. V., Kaleem, Z., Lee, H., & Yu, H. (2024). Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances. IEEE Internet of Things Journal, 11(2), 3599–3613. https://doi.org/10.1109/JIOT.2023.3297241
40. Kihero, A. B., Furqan, H. M., Sahin, M. M., & Arslan, H. (2024). 6G and beyond wireless channel characteristics for physical layer security: Opportunities and challenges. IEEE Wireless Communications, 31(3), 295–301. https://doi.org/10.1109/MWC.002.2300002
41. Lu, X., Xiao, L., Li, P., Ji, X., Xu, C., & Yu, S. (2023). Reinforcement learning-based physical cross-layer security and privacy in 6G. IEEE Communications Surveys & Tutorials, 25(1), 425–466. https://doi.org/10.1109/COMST.2022.3224279
42. Mahmoud, H., Ismail, T., Baiyekusi, T., & Idrissi, M. (2024). Advanced security framework for 6G networks: Integrating deep learning and physical layer security.

Network, 4(4), 453–467. https://doi.org/10.3390/network4040023

43. Mucchi, L., Jayousi, S., Caputo, S., Panayirci, E., Shahabuddin, S., & Bechtold, J. (2024). Physical-layer security in 6G networks. Proceedings of the IEEE.
44. Pradhan, A., Das, S., Piran, M. J., & Han, Z. (2024). A survey on physical layer security of ultra/hyper reliable low latency communication in 5G and 6G networks: Recent advancements, challenges, and future directions. IEEE Access, 12, 112320–112353. https://doi.org/10.1109/ACCESS.2024.3429285
45. Shaji, L., Luo, Y., Yin, C., & Lin, J. (2026). Machine learning-based physical layer security for 5G/6G-enabled electric vehicle charging network. Electronics, 15(4), 865. https://doi.org/10.3390/electronics15040865
46. Soderi, S., Brighente, A., Xu, S., & Conti, M. (2024). Multi-RIS aided VLC physical layer security for 6G wireless networks. IEEE Transactions on Communications.
47. Soderi, S., & De Nicola, R. (2022). 6G networks physical layer security using RGB visible light communications. IEEE Access, 10, 5482–5496. https://doi.org/10.1109/ACCESS.2021.3139456
48. Wiese, M., Pehl, M., Pohle, D., Torres-Figueroa, L, Voichtleitner, J., Mönich, U. J., Seifert, D., Boche, H., Czarske, J. W., Schaefer, R. F., & Sigl, G. (2026). Physical layer security for 6G networks. In Unveiling the Future of Technological Sovereignty, Sustainability, and Trustworthiness (pp. 467–485). Elsevier.
49. Zhang, S., Zhu, D., & Liu, Y. (2024). Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities. Computer Networks, 245, 110255. https://doi.org/10.1016/j.comnet.2024.110255
50. Zhang, Z., Zhang, C., Jiang, C., Jia, F., Ge, J., & Gong, F. (2024). Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks. IEEE Transactions on Wireless Communications.
51. Frimpong, E. O., Oh, B.-H., Kim, T., & Bang, I. (2023). Physical-layer security with irregular reconfigurable intelligent surfaces for 6G networks. Sensors, 23(4), 1881. https://doi.org/10.3390/s23041881
52. Hameed, I., Afridi, A., Baek, M.-S., & Song, H.-K. (2025). Enhancing physical layer security in WPCNs with IRS and controlled jamming for 6G IoT applications. IEEE Access, 13, 4670–4682. https://doi.org/10.1109/ACCESS.2024.3525036
53. Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., Shahzad, T., Khan, S., & Hamam, H. (2025). A comprehensive survey on 6G-security: Physical connection and service layers. Discover Internet of Things, 5, Article 28. https://doi.org/10.1007/s43926-025-00028-0