Securing the Foundations of 6G: Innovative Intelligent Controls at the Physical Layer for Trustworthiness and Resilience

Elva Leka [1,2], Luis Lamani[1], Enkeleda Hoxha [2]
[1]Polytechnic University of Tirana, Tirane, Albania
[2] Albanian University, Tirane, Albania
elva.leka@fgjm.edu.al

***Abstract* — In the dynamic landscape of communication technologies, the imminent arrival of 6G networks promises a transformative change that requires a proactive strategy to strengthen the underlying infrastructure. This research is driven by the mission to ensure the security, trustworthiness, and resilience of 6G networks by introducing innovative, intelligent controls at the physical layer. This involves integrating adaptive systems that dynamically adjust to evolving network conditions while alerting to and remediating security risks in real-time. This study aims to provide a robust foundation for 6G networks by eliminating vulnerabilities that could be exploited by malicious entities, with a focus on the physical layer. The proposed intelligent controls utilise advanced machine learning and adaptive algorithms to assess and improve the network's security posture continuously. Based on a theoretical analysis, this research aims to contribute to the conceptual development of 6G networks that drive technological innovation and embody a secure and resilient architecture essential for the upcoming era of wireless communications. It will explore how intelligent physical layer controls, adaptive algorithms, and machine learning have improved the security of 6G networks.**

Keywords - Intelligent Controls; 6G Security; Adaptive Algorithms; Wireless Communication Evolution; Physical Layer Resilience.

I. INTRODUCTION

The advent of fifth generation (5G) has ushered in a new era of technological advancement in wireless communications. The integration of public key encryption-based authentication into private 5G networks has led to a convergence of wireless security methods with those in core networks. This progress has enabled the emergence of new use cases in areas such as factories, autonomous vehicles and smart cities. The integration of Massive Machine-Type Communications (mMTC) and Internet of Things (IoT) applications into the field of ultra-reliable, low-latency communications was a precursor to a new wave of smart devices and sub-networks that formed the basis for 5G and its successors [1]. With the transition to 6G, the complexity of application scenarios increases, bringing new security challenges that are difficult to overcome with classical complexity-based cryptography. These challenges make it necessary to re-evaluate security paradigms and explore new possibilities in the evolving landscape of 6G technologies [2].

It is expected that the development towards 6G will significantly improve and expand the capabilities demonstrated in 5G. The aim is to create communication channels that operate at terahertz (THz) frequencies and enable data transfer rates that exceed those of 5G by a factor of one hundred [3]. Potential transmission speeds of this kind are in the range of several tens of terabits per second. The significant acceleration in speed and reduction in response time are of paramount importance for time-critical applications such as remote surgical procedures and sophisticated interactions in virtual and augmented reality [4]. In addition, advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) are expected to be integrated into the framework of 6G networks. The result of this integration will produce networks that have enhanced adaptability and intelligence so that they can handle complicated tasks efficiently.

This article is organised as follows. Section 2 presents the architecture of the 6G network. Section 3 discusses the security challenges of 6G. Section 4 introduces physical layer security in 6G and continues with the privacy and trust aspects in Section 5. The last section contains the conclusion.

II. 6G NETWORK ARCHITECTURE

The architecture of 6G consists of an extensive network of cutting-edge technologies. The integration of physical and digital space should be seamless. This technology should support autonomous systems, networked automation, the Internet of Things, virtual reality experiences and communication at the speed of light.

A. Terrestrial and non-terrestrial ecosystem integration

The integration of non-terrestrial networks and terrestrial network networks, commonly referred to as NTNs, represents a noteworthy achievement in the progression of the 6G project. Compared with previous network architectures, this integration represents a major shift in order to maximize network resilience and enable wide-scale global communication. Collaboration will occur between NTNs, which consist of conventional cellular base stations, terrestrial networks (LEO satellites, high-altitude platform stations (HAPS), and unmanned aerial vehicles

(UAVs), including drones [5]. Figure 1 presents the integration of Terrestrial and NTNs in 6G.

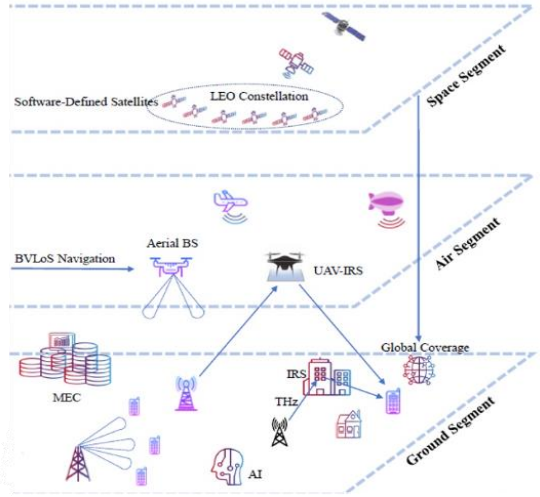

Figure 1. Integration of Terrestrial and NTNs in 6G [6].

Integrating terrestrial and NTNs in 6G is a forward-looking approach that promises to revolutionise global connectivity, making the dream of universal and resilient network coverage a reality. Overcoming the associated challenges like (1) *Seamless Connectivity*, (2) *Latency and Bandwidth*, (3) *Network Management and Control* will require innovative engineering and network management solutions, but the potential benefits in terms of coverage, capacity, and service reliability are immense [7].

B. Dynamic Network Slicing in 6G

The diverse range of applications expected to function on 6G networks, including low-latency tasks like autonomous driving and high-bandwidth activities like virtual reality broadcasting, necessitates a network that dynamically adjusts to changing service demands. Figure 2 presents the 6G multi-slice network environment.

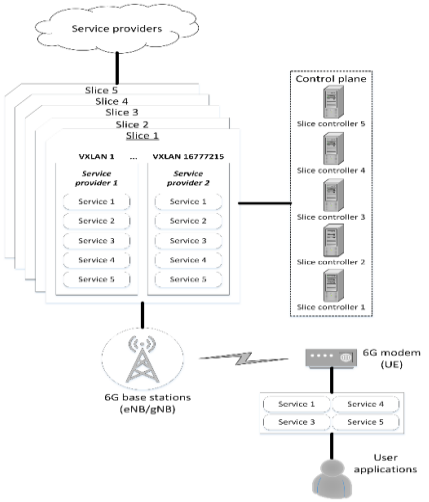

Figure 2. Multi-slice network environment in 6G [8].

Dynamic network segmentation enables this adaptability, thereby facilitating the following:

– To satisfy the demands of a given service, it is viable to design an individualised network segment that considers variables, including *latency*, *bandwidth*, *security*, and *dependability* [9].

– Network slicing dynamically allocates resources in response to real-time demand, resulting in more efficient resource utilisation. Consequently, the risk of inadequate or extensive infrastructure utilisation is averted [10].

Dynamic slicing will play a pivotal role in facilitating the complete realisation of the capabilities of next-generation wireless communication as 6G networks progress. Despite certain obstacles, like Hardware Complexity and Energy Consumption, that must be taken into consideration [11], most notably those related to energy management and hardware complexity, continuous research and development in this domain holds the potential to unveil groundbreaking resolutions that will empower the complete actualisation of 6 G's capabilities. Table 1 below presents a summary of critical technological innovations in 6G.

TABLE I. SUMMARY OF KEY TECHNOLOGICAL INNOVATIONS IN 6G AND THEIR IMPLICATIONS

Technology	***Description***	***Implications***
Artificial Intelligence (AI)	Embedded at the core of 6G networks for network optimization, predictive maintenance, and autonomous decision-making processes.	Enables efficient handling and processing of massive data, driving improved data analytics and network management.
Edge Computing	Brings computational resources closer to the data source, thereby reducing latency and improving response times.	Real-time processing applications like driverless vehicles and augmented reality improve user experience and operational efficiency.
Millimeter Wave (mmWave) and Beamforming	Utilization of higher frequencies for higher bandwidth and data rates. Beamforming focuses wireless signals in concentrated beams.	Addresses signal propagation challenges, allowing for faster data transmission and increased network capacity.
Decentralized Architecture	Shift from a centralized model to a distributed model where intelligence and processing power are spread across the network.	Improves network resilience and performance; however, introduces new security challenges and requires robust protocols for a dynamic network environment.

The functionalities of 6G will grant these technologies unprecedented prospects, facilitating their operation in a more streamlined, intelligent, and pervasive fashion. As society progresses towards this forthcoming situation, the convergence of 6G and these nascent technologies will presumably incite innovation in various industries, resulting in more intelligent, responsive, and efficient systems.

III. SECURITY CHALLENGES IN 6G NETWORKS

This section examines multiple security concerns arising from the use of 6G technology. These concerns encompass

the integration of artificial intelligence and machine learning and the urgent need for encryption resistant to quantum attacks.

A. *Emerging Threats to Security*

Given the increasing number of linked systems and devices, installing 6G is expected to increase the network's vulnerability significantly (see Table 1). The development of Internet of Things (IoT) devices increases the risk of data invasions and large-scale Distributed Denial of Service (DDoS) assaults, both of which can serve as entry points for cyber threats [12]. Furthermore, dynamic network slicing introduces distinct susceptibilities, given that individual slices might exhibit unique security characteristics, potentially providing adversaries with a circumvented route [13]. Additional concerns arise from Advanced Persistent Threats (APTs), which exploit the intricacy of the network to execute protracted espionage, data theft, or sabotage. Table 2 presents the overview of emerging security threats in 6G networks.

TABLE II. OVERVIEW OF EMERGING SECURITY THREATS IN 6G NETWORKS

Threat Category	*Specific Threats*	*Implications*
IoT Vulnerabilities	- Device-level security inconsistencies - Insecure interfaces and APIs	Increased attack surface, enabling unauthorized access and data breaches
Slice-Specific Risks	- Isolation failure between network slices - Misconfigured slice policies	Compromised data integrity and privacy across different network functions and services
Advanced Persistent Threats (APTs)	- Multi-vector attacks targeting the core and edge of the network	Advanced Persistent Threats (APTs)

B. *AI and Machine Learning's Impact on the World*

Both AI and ML, which are essential to optimising and managing 6G networks, have a twofold impact on the security of the networks [14]. Even though these technologies have previously unimaginable possibilities for increasing security measures using real-time threat detection and automated responses, they also pose new vulnerabilities. There is a growing concern regarding adversarial assaults aimed at tricking artificial intelligence systems. These attacks can compromise networks' integrity and confidentiality [15]. On the other hand, using artificial intelligence to construct sophisticated threat detection models highlights the potential for these technologies to strengthen network defences against assaults that are becoming increasingly complicated [16].

C. *Quantum Resistance and Quantum Cryptography*

The emergence of quantum computation poses a dual threat to network security, particularly to cryptography [17]. A considerable proportion of the cryptographic algorithms currently utilised to protect digital communications, including those integrated into 6G networks, could be effortlessly bypassed by quantum computers. Quantum computers exhibit the capacity to solve intricate mathematical problems at speeds that are beyond all previous records. The pursuit of quantum-resistant encryption is not solely motivated by the need to protect communications; it also serves to preserve the foundational trust model of digital interaction in the quantum computing era [18].

Implementing 6G networks presents an intricate array of security concerns, which demand novel strategies to guarantee strong safeguards against emergent risks. Incorporating artificial intelligence and the progression of quantum-resistant cryptography emerge as pivotal elements in constructing a dependable and secure 6G ecosystem.

IV. PHYSICAL LAYER SECURITY IN 6G

Physical Layer Security (PLS) leverages the inherent difficulties associated with interception and surveillance in wireless communication to ensure security in 6 G networks. Due to the threat posed by quantum computation, conventional encryption techniques may prove inadequate in the 6G-envisioned environment of ubiquitous connectivity, where this method is indispensable [19]. Key-based or SINR-based (keyless) approaches comprise most physical-layer security classification categories. Power allocation, beamforming, and the injection of artificial noise algorithms are all examples of keyless methods.

A. *PLS Techniques and Applications*

PLS techniques play a critical role in wireless communications as they ensure the security of data transmission over airwaves, a medium inherently vulnerable to interception. PLS can guarantee secure communication in various environments, including satellite communications and cellular networks, by capitalising on the unpredictability of wireless channels rather than exclusively relying on higher-layer encryption techniques.

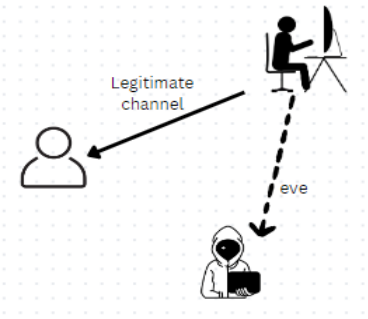

Figure 3. PLS Techniques in 6G Security.

– *Quantum Key Distribution (QKD)*

The secure exchange of encryption keys between two entities, commonly known as Alice and Bob, is achieved through the utilisation of Quantum Key Distribution (QKD), which takes advantage of the intrinsic quantum characteristics of particles, specifically photons. Although a potential eavesdropper, Eve, is present, this procedure guarantees that the communication remains private [20]. Fundamental tenets underlying the protection of QKD are as follows:

1. The capacity of a particle's quantum state to exist simultaneously in multiple states before being measured is referred to as the phenomenon of quantum superposition [21].
2. It is theoretically impossible to surveil without being detected, as Heisenberg's Uncertainty Principle dictates that measuring a quantum system invariably induces a state change [22].

– *Waveform Design and Coding*

Waveform development and coding require complex techniques to modify signal properties, enhancing communication systems' privacy, specifically in the imminent 6G networks.

These modifications make it more difficult for unauthorised interceptors to decipher transmitted messages, thereby fortifying the communication's security.

1. ***Spread Spectrum:*** This method distributes the signal over a greater frequency range than is strictly necessary. Direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) protect the transmission against interception and jamming and impede eavesdroppers' ability to discern the spreading code [23].
2. ***Chirp Spread Spectrum (CSS):*** CSS employs time-varying chirp pulse frequencies. This characteristic enhances the signal's resilience to prevalent Doppler effects and multipath fading in mobile environments while introducing complexity into unauthorised interception [24].
3. ***Secure Coded Modulation:*** This is achieved by combining modulation and coding to increase the channel's capacity for secrecy. Its purpose is to minimise information leakage to potential eavesdroppers while maximising the data rate for the authorised recipient [25].
4. **Secure Coding in Orthogonal Frequency-Division Multiplexing (OFDM):** OFDM partitions a data signal among several closely spaced carriers. When combined with secure coding, it can obscure the presence of the transmitted signal, thereby increasing the difficulty for interceptors in identifying and decoding the transmission [26].
5. **Low Probability of Intercept (LPI) Techniques:** LPI techniques aim to maximise the difficulty for unauthorised receivers in detecting the signal. This is accomplished via power regulation, frequency hopping, or implementing covert methods that reduce the signal's susceptibility to detection [27].
6. **LiFi Integration:** Basic integration of LiFi into an existing WiFi system can occur in one of two ways: centrally or autonomously. One potential strategy is expanding WiFi's autonomous network architecture to encompass LiFi. The user can select an AP from either network domain, and the AP can utilise any available channel. Although this methodology provides a simplified approach to network management, it compromises the efficacy of the network [28].

TABLE III. COMPARISON OF WAVEFORM DESIGN TECHNIQUES AND THEIR EFFECTIVENESS IN VARIOUS 6G SCENARIOS

Technique	*Urban Dense Networks*	*Rural Areas*	*High-Speed Mobility*	*IoT Applications*	*Energy Efficiency*	*Eavesdropper Resistance*
Spread Spectrum	High	Moderate	High	High	Low	High
Chirp Spread Spectrum (CSS)	Moderate	High	High	Moderate	Moderate	Moderate
OFDM with Secure Coding	High	High	Moderate	High	Moderate	High
Low Probability of Intercept (LPI)	High	High	High	Moderate	High	Very High
Time-Hopping (TH)	Moderate	Moderate	Low	High	High	Moderate
Secure Coded Modulation	High	High	High	High	Moderate	Very High
Spread Spectrum	High	Moderate	High	High	Low	High

Table 3 presents a structured approach to comprehending how various waveform design and coding strategies can be implemented to bolster the confidentiality and integrity of communications in 6G networks. It encompasses many use cases and environments, considering urban dense networks, rural areas, high-speed mobility, IoT Applications, energy efficiency, and eavesdropper resistance.

B. Artificial Noise Implementation

It is an intelligent security measure to incorporate Artificial Noise (AN) into the physical layer of communication networks. Enhancing the confidentiality and integrity of the information transmitted is the primary objective. Anodising the communication channel with noise on purpose substantially complicates the task of potential eavesdroppers in discerning and deciphering the legitimate signal [29]. By strategically deploying AN, this noise effectively obstructs unauthorised receivers while leaving the intended recipient's ability to decipher the message unaffected. The following is a comprehensive analysis of AN's operation and implementation strategies [30-32]:

– *Signal and Noise Transmission:* The transmitter emits both legitimate and artificial signals. The key to AN's effectiveness lies in the transmission's spatial or temporal characteristics, which allow the legitimate receiver to differentiate between the signal and the noise.

– *Spatial Focusing of Noise:* In systems employing multiple antennas, such as MIMO (Multiple Input Multiple Output) configurations, AN can be spatially directed towards potential eavesdroppers' locations or spread in a way that minimally impacts the legitimate receiver. This technique requires precise Channel State Information (CSI) knowledge of the intended receiver but not necessarily of the eavesdropper.

– *Temporal Variation:* AN can also be varied over time, leveraging the dynamic nature of wireless channels. By synchronising the noise transmission with the legitimate receiver's expected channel conditions, the system can ensure that the noise has minimal impact on the intended communication [33]. Figure 4 presents the architecture of artificial noise channel implementation.

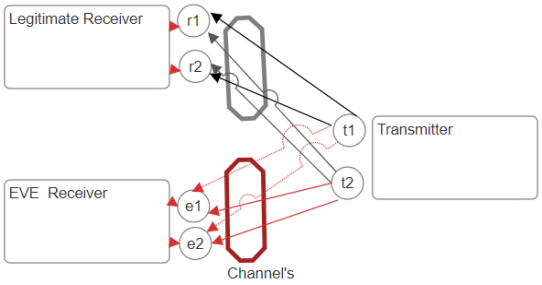

Figure 4. Artificial Noise channel Implementation

The efficacy of AN is predicated on the adept and dynamic administration of transmission attributes, which guarantees secure correspondence notwithstanding the existence of sophisticated surveillants.

V. Ensuring Privacy and Trust in 6G

Data privacy and security assurance must be improved to establish confidence in 6G networks. It includes the ethical application of technology, the dependability of services, and the integrity of communication [34]. A multidimensional strategy is necessary to establish this trust:

– Adopting sophisticated security protocols, including zero-trust designs and quantum-resistant algorithms, is necessary to ensure the security of 6G networks against current and future vulnerabilities. These measures successfully protect against emerging cyber threats [35].
– Blockchain and other decentralised ledger technologies can be utilised to implement trust mechanisms to guarantee the integrity and transparency of 6G apps and services. Consequently, this can enhance trust in the authentication of identities and transactions [36].
– In the realm of 6G network and service management, the ethical implications of AI and ML become ever more significant. To preserve user confidence and societal approval, these systems must be transparent, answerable, and by ethical standards [37].
– Adherence to international standards and regulations, including the General Data Protection Regulation (GDPR) [38], can facilitate trust building and guarantee that 6 G technologies uphold user rights and data sovereignty.

The advent of the 6G offers a distinct prospect of integrating privacy and trust at the core of the upcoming generation of communication networks. By embracing a comprehensive and forward-thinking strategy regarding these matters, stakeholders can not only reduce risks but also unleash the complete potential of the 6G to empower societies and foster sustainable prosperity.

VI. Conclusion

Developing 6G technology indicates society's dedication to appropriately using technology. A new age in wireless communication is dawning, and 6G privacy and trust conversations reflect a shared recognition of the difficulties and opportunities ahead. This paper explores how to keep our digital society's core ideals in mind as we move forward. Advanced security protocols, decentralised architectures, and ethical AI are needed to generate confidence in 6G networks, highlighting the need for attention, openness, and accountability throughout the technical ecosystem. As we look ahead, a safe and trustworthy 6G network will face foreseen and unforeseen problems. Privacy-by-design-guided technological and policy innovation and international collaboration will be essential to addressing these challenges. By involving stakeholders from policymakers and technologists to end-users and civil society, 6G technology will evolve with a balanced consideration of its societal implications.

References

[1] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, C. Del-Valle-Soto, "Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review," *Sensors 2023*, 23, 3876. https://doi.org/10.3390/s23083876.

[2] A. Salameh and M. Tarhuni, "From 5G to 6G—Challenges, Technologies, and Applications," *Future Internet*, vol. 14, no. 117, April 2022. DOI: 10.3390/fi14040117.

[3] W. Jiang and H. D. Schotten, "Dual-beam intelligent reflecting surface for millimeter and THz communications," in *Proc. IEEE 95thVeh. Technol. Conf. (VTC-Spring)*, 2022, pp. 1–6.

[4] H. F. Ahmad, W. Rafique, R. U. Rasool, A. Alhumam, Z. Anwar, and J. Qadir, "Leveraging 6G, extended reality, and IoT big data analytics for healthcare: A review," *Computer Science Review*, vol. 48, 2023, Art. no. 100558, ISSN 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2023.100558.

[5] M. Ozger et al., "6G for Connected Sky: A Vision for Integrating Terrestrial and Non-Terrestrial Networks," *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Gothenburg, Sweden, 2023, pp. 711-716, doi: 10.1109/EuCNC/6GSummit58263.2023.10188330.

[6] M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, J. F. Mendoza Montoya, S. Pollin, A. Haqiqatnejad, A. Mostaani, E. Lagunas, and B. Ottersten, "Evolution of Non-Terrestrial Networks From 5G to 6G: A Survey," *arXiv*:2107.06881, 9 Aug 2022. DOI: https://doi.org/10.48550/arXiv.2107.06881.

[7] R. Gupta, D. Reebadiya, and S. Tanwar, "6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission," in *Computer Standards & Interfaces*, vol. 77, 2021, 103521, ISSN 0920-5489, doi: 10.1016/j.csi.2021.103521.

[8] Bojović, P.D.; Malbašić, T.; Vujošević, D.; Martić, G.; Bojović, Ž. Dynamic QoS Management for a Flexible 5G/6G Network Core: A

Step toward a Higher Programmability. *Sensors 2022*, 22, 2849. https://doi.org/10.3390/s22082849

[9] I. Ahmad, F. Rodriguez, J. Huusko, and K. Seppänen, "On the Dependability of 6G Networks," *Electronics*, vol. 12, pp. 1-19, 2023. DOI: 10.3390/electronics12061472.

[10] Lin,J.-Y.; Chou,P.-H.; Hwang, R.-H. Dynamic Resource Allocation for Network Slicing with Multi-Tenants in 5G Two-Tier Networks. *Sensors 2023*, 23,4698.https://doi.org/10.3390/s23104698

[11] L. Wei, C. Huang, G. C. Alexandropoulos, A. M. Elbir, Z. Yang, Z. Zhang, M. Di Renzo, M. Debbah, and C. Yuen, "Wireless communications empowered by reconfigurable intelligent surfaces: Model-based vs model-free channel estimation," *Journal of Information and Intelligence*, vol. 1, issue 3, pp. 253-266, 2023, ISSN 2949-7159. DOI: https://doi.org/10.1016/j.jiixd.2023.06.010.

[12] Tariq U, Ahmed I, Bashir AK, Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*. 2023; 23(8):4117. https://doi.org/10.3390/s23084117.

[13] A. Thantharate, A. Tondwalkar, C. Beard, and A. Kwasinski, "ECO6G: Energy and Cost Analysis for Network Slicing Deployment in Beyond 5G Networks," in *Sensors*, vol. 22, 8614, 2022, doi: 10.3390/s22228614.

[14] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," in *Digital Communications and Networks*, vol. 6, no. 3, pp. 281-291, 2020, ISSN 2352-8648, doi: 10.1016/j.dcan.2020.07.003.

[15] Son, Bui & Nguyen, Hoa & Chien, Trinh & Khalid, Waqas & Ferrag, Mohamed Amine & Choi, Wan & Debbah, mérouane. (2024). Adversarial Attacks and Defenses in 6G Network-Assisted IoT Systems. 10.48550/arXiv.2401.14780.

[16] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," in *Computer Networks*, vol. 212, 2022, 109032, ISSN 1389-1286, doi: 10.1016/j.comnet.2022.109032.

[17] J. Partala, "Post-quantum Cryptography in 6G," 2021, doi: 10.1007/978-3-030-72777-2_20.

[18] M. Zulfiqar Ali, A. Abohmra, M. Usman, A. Zahid, H. Heidari, M. A. Imran, and Q. H. Abbasi, "Quantum for 6G communication: A perspective," *IET Quantum Communication*, 2023, doi: 10.1049/qtc2.12060.

[19] Ur Rasool R, Ahmad HF, Rafique W, Qayyum A, Qadir J, Anwar Z. Quantum Computing for Healthcare: A Review. *Future Internet*. 2023; 15(3):94. https://doi.org/10.3390/fi15030094.

[20] Ali, Muhammad & Abohmra, Abdoalbaset & Zahid, Adnan & Heidari, Hadi & Imran, Muhammad & Abbasi, Qammer. (2023). Quantum for 6G communication: A perspective. IET Quantum Communication. 4. n/a-n/a. 10.1049/qtc2.12060.

[21] A. Sigov, L. Ratkin, and L. A. Ivanov, "Quantum Information Technology," in Journal of Industrial Information Integration, vol. 28, 2022, 100365, ISSN 2452-414X, doi: 10.1016/j.jii.2022.100365.

[22] E. Benítez Rodríguez and L. M. Arévalo Aguilar, "A Survey of the Concept of Disturbance in Quantum Mechanics," in *Entropy (Basel)*, vol. 21, no. 2, Feb 2, 2019, 142, doi: 10.3390/e21020142. PMID: 33266858; PMCID: PMC7514626.

[23] A. Bensky, "Chapter 11 - Wireless local area networks," in *Short-range Wireless Communication (Third Edition)*, ed. A. Bensky, Newnes, 2019, pp. 273-315, ISBN 9780128154052, doi: 10.1016/B978-0-12-815405-2.00011-7.

[24] T. Nguyen, H. Nguyen, R. Barton, and P. Grossetete, "Efficient Design of Chirp Spread Spectrum Modulation for Low-Power Wide-Area Networks," in *IEEE Internet of Things Journal*, pp. 1-1, 2019, doi: 10.1109/JIOT.2019.2929496.

[25] Megha S. Kumar, R. Ramanathan, and M. Jayakumar, "Keyless physical layer security for wireless networks: A survey," in *Engineering Science and Technology, an International Journal*, vol. 35, 2022, 101260, ISSN 2215-0986, doi: 10.1016/j.jestch.2022.101260.

[26] Y. Wan, J. Ren, B. Liu, Y. Mao, S. Chen, X. Wu, Y. Li, Y. Wu, L. Zhao, T. Sun, and R. Ullah, "Secure OFDM transmission scheme based on chaotic encryption and noise-masking key distribution," in *Optics Letters*, vol. 47, no. 11, pp. 2903-2906, Jun 1, 2022, doi: 10.1364/OL.460052. PMID: 35648960.

[27] Park D-H, Jeon M-W, Shin D-M, Kim H-N. LPI Radar Detection Based on Deep Learning Approach with Periodic Autocorrelation Function. *Sensors*. 2023; 23(20):8564. https://doi.org/10.3390/s23208564.

[28] X. Wu, M. Dehghani Soltani, L. Zhou, M. Safari, and H. Haas, "Hybrid LiFi and WiFi Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, pp. 1-1, 2021, doi: 10.1109/COMST.2021.3058296.

[29] F. Xu, S. Ahmad, M.N. Khan, M. Ahmed, S. Raza, F. Khan, Y. Ma, and W.U. Khan, "Beyond encryption: Exploring the potential of physical layer security in UAV networks," in *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 8, 2023, 101717, ISSN 1319-1578, doi: 10.1016/j.jksuci.2023.101717.

[30] A. Halamandaris, M.S. Alam, I. Ahmed, K. Hasan, and G. Kaddoum, "Performance Analysis of 6G Communication *Links in the Presence of Phase Noise*," pp. 1-6, 2023, doi: 10.1109/LATINCOM59467.2023.10361876.

[31] W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334-366, 2021, doi: 10.1109/OJCOMS.2021.3057679.

[32] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T.H. Nguyen, F. Liu, T. Hewa, M. Liyanage, A. Ijaz, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, A. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, B.O. Ozparlak, and J. Röning, "6G White paper: Research challenges for Trust, Security and Privacy," 2020, *arXiv*:2004.11665v2, doi: 10.48550/arXiv.2004.11665.

[33] Ó. Seijo, I. Val and J. A. López-Fernández, "Portable Full Channel Sounder for Industrial Wireless Applications With Mobility by Using Sub-Nanosecond Wireless Time Synchronization," in *IEEE Access*, vol. 8, pp. 175576-175588, 2020, doi: 10.1109/ACCESS.2020.3025896.

[34] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[35] A.V.R. Mayuri, J. Chauhan, A. Gadgil, O. Rajani, and S. Rajadhyaksha, "6G Systems in Secure Data Transmission," in *Book Title: Security in 6G Communication Networks*, 2023, doi: 10.1002/9781119910619.ch10.

[36] Y. Wang, X. Kang, T. Li, H. Wang, C. -K. Chu and Z. Lei, "SIX-Trust for 6G: Toward a Secure and Trustworthy Future Network," in *IEEE Access*, vol. 11, pp. 107657-107668, 2023, doi: 10.1109/ACCESS.2023.3321114.

[37] V. Chamola, V. Hassija, A. R. Sulthana, D. Ghosh, D. Dhingra and B. Sikdar, "A Review of Trustworthy and Explainable Artificial Intelligence (XAI)," in *IEEE Access*, vol. 11, pp. 78994-79015, 2023, doi: 10.1109/ACCESS.2023.3294569.

[38] S. R. Garzon, H. Yildiz and A. Küpper, "Decentralized Identifiers and Self-Sovereign Identity in 6G," in *IEEE Network*, vol. 36, no. 4, pp. 142-148, July/August 2022, doi: 10.1109/MNET.009.2100736.