6G Security Challenges and Potential Solutions

Pawani Porambage*, Gürkan Gür†, Diana Pamela Moya Osorio*, Madhusanka Liyanage*‡, Mika Ylianttila*
*Centre for Wireless Communications, University of Oulu, Finland
†Zurich University of Applied Sciences (ZHAW) InIT, Switzerland
‡School of Computer Science, University College Dublin, Ireland
Email: *[firstname.lastname]@oulu.fi, †gueu@zhaw.ch, ‡madhusanka@ucd.ie

***Abstract*—Although the fifth generation wireless networks are yet to be fully investigated, the vision and key elements of the 6th generation (6G) ecosystem have already come into discussion. In order to contribute to these efforts and delineate the security and privacy aspects of 6G networks, we survey how security may impact the envisioned 6G wireless systems with the possible challenges and potential solutions. Especially, we discuss the security and privacy challenges that may emerge with the 6G requirements, novel network architecture, applications and enabling technologies including distributed ledger technologies, physical layer security, distributed artificial intelligence (AI)/ machine learning (ML), Visible Light Communication (VLC), THz bands, and quantum communication**

***Index Terms*—6G, Security, Privacy, DLT, Quantum security, AI/ML, Physical Layer Security, Security threats**

I. Introduction

Sixth generation (6G) of mobile communication is already envisioned despite of the fact that 5G specifications are still developing and 5G coverage is not yet fully provided. The most significant driving force in 6G leap is the inherent connected intelligence in the telecommunication networks accompanied with advanced networking and Artificial Intelligence (AI) technologies [1]. However, the tight coupling between 6G and AI does not by definition lead to better security and privacy. It may also become a means or an apparatus to infringe them in various cases. The evolution of security landscape of telecommunication networks from 1G to 5G and then to the envisioned 6G is illustrated in Figure 1. Moreover, there are many efforts/proposals on blending novel technologies such as blockchain, visible light communication (VLC), THz, and quantum computing/communication features in 6G intelligent networking paradigms in such a way to tackle the security and privacy issues. Therefore, 6G security considerations need to be analyzed in terms of physical layer security, network information security and advanced learning (e.g., deep learning) related security [2].

Since the standard functions and specifications of 6G are yet to be defined, there is still very limited literature that clearly provides security and privacy insights of 6G networks. In this article, we try to shed the light on how security may impact the envisioned 6G wireless systems with a concise discussion of challenges and then related potential solutions. In particular, we survey the security and privacy challenges that may arise with the expected 6G requirements, novel network architecture, new applications and enabling technologies. We also discuss the potential security solutions for 6G along the directions of Distributed Ledger Technology (DLT), physical layer security, quantum security, and distributed AI.

II. Security Challenges in 6G Networks

This section provides the possible security challenges and threat landscape in future 6G wireless systems.

A. New 6G Requirements

Future 6G applications will pose stringent requirements and require extended network capabilities compared to currently developed 5G networks [1]. These requirements are summarized in Figure 2. They are established to enable the wide range of key 6G use cases and thus can be categorized accordingly. They also have major implications on how 6G security is implemented. For *Enhanced Ultra-Reliable, Low-Latency Communication (ERLLC/eURLLC)*, the latency impact of security workflows will be considered to ensure service quality. Similarly, high reliability requirements call for very efficient security solutions protecting availability of services and resources. With *Further enhanced Mobile Broadband (FeMBB)*, extreme data rates will pose challenges regarding traffic processing for security such as attack detection, AI/ML pipelines, traffic analysis and pervasive encryption. That issue can be alleviated with distributed security solutions since traffic should be processed locally and on-the-fly in different segments of the network, ranging from the edge to the core service cloud. At this point, DLT will be instrumental with transparency, security and redundancy attributes. *Ultra massive Machine Type Communication (umMTC)* will serve critical use-cases which impose much more stringent security requirements compared to 5G. In particular, Internet of Everything (IoE) with very diverse capabilities will challenge the deployment and operation of security solutions such as distributed AI/ML and privacy concerns. An important aspect is how to integrate novel security enablers in an abundance of resource constrained devices. Nevertheless, the security enforcement will be more complex since network entities will be much more mobile, changing their edge networks frequently and getting services in different administrative domains.

B. New Architecture

1) Intelligence radio: State-of-the-art circuits, antennas, meta-material-based structures, and the dramatic improvement of AI chips have shed light on a paradigm-shift for hardware

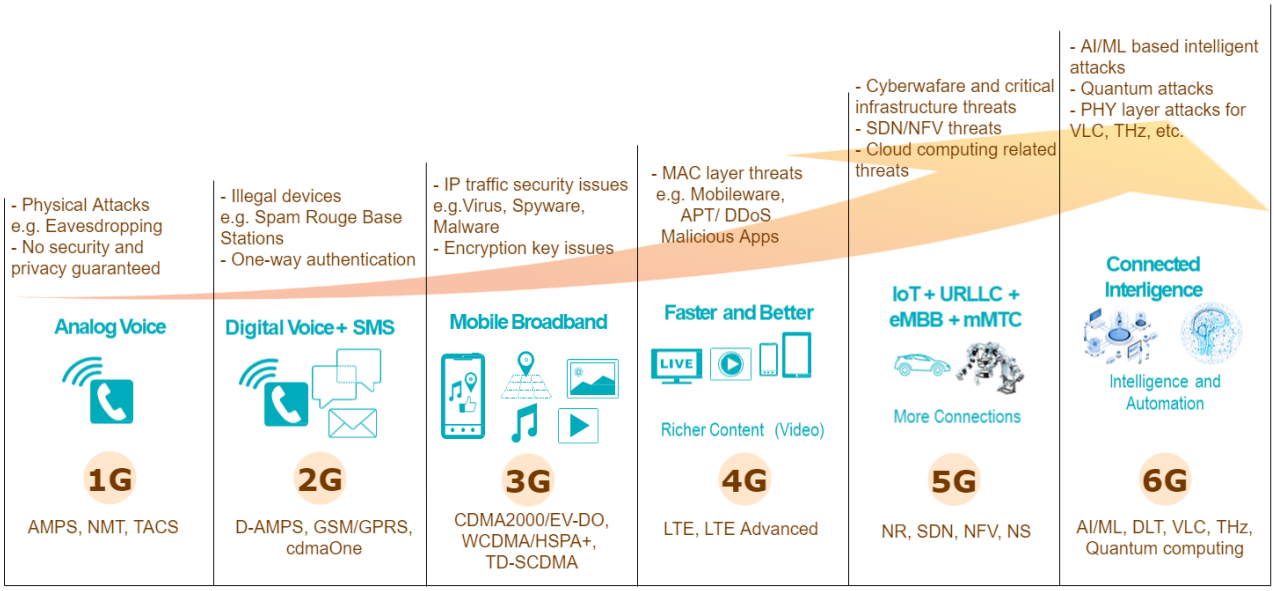

Fig. 1: Evolution of communication network security landscape.

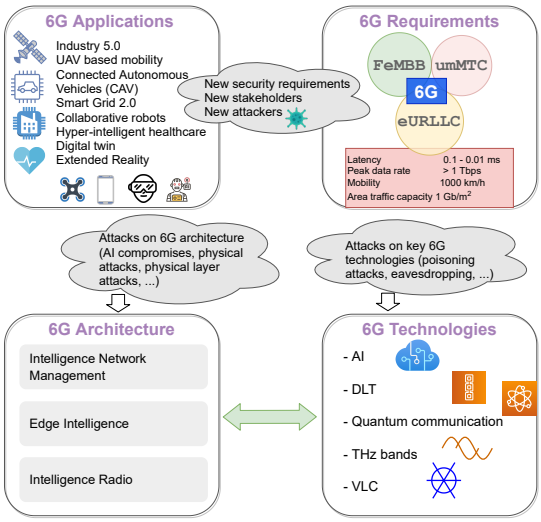

Fig. 2: 6G landscape and security composition.

architecture of 6G transceivers, where hardware can be separated from the transceiver algorithms. Hence, the transceiver algorithms could dynamically configure and update themselves based on environment and hardware information. Intelligent radio will involve cutting-edge AI/ML techniques in order to address accurate channel modeling, agile physical layer design, dynamic spectrum access, advanced network deployment, optimization, and autonomous orchestration issues in the wireless domain [1]. Thus, suspicious activities by malicious nodes need to be predicted during communication processes for secure radios [3].

2) Edge Intelligence: When AI/ML algorithms are used to acquire, storage or process data at the network edge, it is referred to as edge intelligence (EI) [4]. In EI, an edge server aggregates data generated by multiple devices associated with it while sharing them with other edge servers for training models, and later used for analysis and prediction, thus devices can benefit from faster feedback, reduced latency and lower costs while enhancing their operation. However, as data is gathered from multiple sources, and the outcome of AI/ML algorithms is highly data-dependent, EI is highly prone to several security attacks. Attackers can exploit this dependency to launch different attacks like data poisoning/evasion or privacy violations, thus affecting the outputs of the AI/ML applications and undermining the benefits of EI.

3) Intelligence Network Management: The extreme range of 6G requirements and the envisioned full end-to-end (E2E) automation of network and service management (i.e., use of AI) demand a radical change in network service orchestration and management in 6G architecture [5], [6]. ETSI ZSM (Zero-touch network and Service Management) [7] architecture for 5G is a promising initiative to pave the path towards this intelligence network management deployment.

Several security challenges have been identified in such intelligence network management deployments. First, closed loop network automation may introduce security threats such as Denial of Service (DoS), deception and Man-In-The-Middle (MITM) attacks [8]. DoS attacks can be performed by gradually adding fake heavy load in virtual network functions (VNFs) to increase the capacity of virtual machines (VMs). MITM attacks can be performed by triggering fake fault events and intercepting the domain control messages to reroute traffic via malicious devices. Deception attacks can be performed by tampering the transmitted data. Secondly, if 6G networks use Intent-Based Interfaces similar to ZSM which can be vulnerable for information exposure, undesirable configuration and abnormal behavior attacks can occur. Intercepting information of intents by unauthorized entities can also harm system security objectives (e.g., privacy, confidentiality) and lead to further subsequent attacks. Undesirable configuration in Intent-Based Interfaces such as changing the mapping from intent to action or decreasing the security level can jeopardize

the security of the whole management system. A malformed intent could also have similar effects.

C. New Applications

6G will be the key communication infrastructure to satisfy the demands of future needs of hyper-connected human society by 2030 and beyond. It is foreseen that 6G paves the way to the development of many new technologies such as smart surfaces, zero-energy IoT devices, advanced AI techniques, possible quantum computing systems, AI-powered automated devices, AI-driven air interfaces, humanoid robots, and self-sustained networks [1]. Moreover, the future trends of digital societies such as massive availability of small data, increasing elderly population, convergence of communication, sensing, and computing, gadget-free communication will also demand new applications. The key 6G applications are identified as UAV based mobility, Connected Autonomous Vehicles (CAV), Smart Grid 2.0, Collaborative Robots, Hyper-Intelligent Healthcare, Industry 5.0, Digital Twin and Extended Reality [9]. The given applications may accommodate different stakeholders and demand different levels of 6G security requirements. Due to the novelty of these application domains and the powerful attackers, the security requirements and the challenges may hugely vary in 6G rather than in 5G (Table I).

D. Privacy

Privacy protection is a basic performance requirement and a key feature in wireless communications in the envisioned era of 6G [3], [10], which poses three key challenges:

- The extremely large number of small chunks of data exchanges in 6G may impose a greater threat on peoples' privacy with an extensive attention attracted by governmental and other business entities. The easier the data is accessible and collectable in 6G era, the greater risk they may impose on protecting user privacy and causing regulatory difficulties.
- When the intelligence is moving to the edge of the network, more sophisticated applications will run on mobile devices increasing the threats of attacks. However, incorporating privacy protecting mechanisms in resource-constrained devices will be challenging.
- Keeping balance between maintaining the performance of high-accurate services and the protection of user privacy is noteworthy. Location information and identities are needed to realize many smart applications. This requires careful consideration of data access rights and ownership, supervision and regulations for protecting privacy.

AI and machine learning (ML) technologies show a greater impact on privacy in two ways [10]. In one way, the correct application of ML can enhance privacy in 6G, whereas in another way privacy violations may occur on ML attacks. The privacy attacks on ML models can be occurred on training (e.g., poisoning attack) and testing phases (e.g., reverse, membership interference, adversarial attacks).

E. New Technologies and Threat Landscapes

Considering the above technological, architectural and application specific aspects of the future 6G networks, they may encounter a wide range of security challenges as threat landscapes. Since the attacks can be generalized based on the technologies rather than the applications, we are taking this step forward to give the reader an insight about the most novel and specific attacks in 6G technologies (Table II). The advent and advancements of technologies may also pave the way to generate more powerful attackers who can create sophisticated attacks on different parts of 6G architecture. In addition to the attacks in Table II, each technology may also face many variants of well-known attacks such as Distributed DoS, MITM, sybil, scanning and spoofing attacks.

TABLE I: 6G Applications: Security requirement and Possible Challenges.

Potential 6G Applications	Security Requirements								Expected Security and Implantation Challenges									
	Ultra Lightweight Security	Extremely Low latency	Extreme Scalability	Zero-touch Security	High Privacy	Proactive Security	Security via Edge	Domain specific security	Limited resources	Diversity of Devices	High Mobility	Physical Tempering	Terrorist Attacks	Intermittent Connectivity	Localized environment	Lack of Security Standards	E2E Security orchestration	Energy Efficiency
UAV based mobility	M	H	H	H	L	M	H	L	H	M	H	M	H	L	L	L	H	H
Connected Autonomous Vehicles	L	H	H	H	M	H	H	H	L	M	H	M	H	L	L	L	H	M
Smart Grid 2.0	H	L	H	M	M	H	L	H	H	L	L	H	H	H	L	L	L	M
Collaborative Robots	M	H	M	H	L	L	H	H	M	L	M	M	L	L	H	L	M	M
Hyper-Intelligent Healthcare	H	H	H	M	H	M	H	H	H	H	M	M	L	M	H	M	H	H
Industry 5.0	M	H	H	H	L	H	H	H	H	H	M	L	M	L	H	M	H	H
Extended Reality	H	H	H	M	H	L	H	L	H	M	M	H	L	L	L	H	H	H

L Low Level Requirement/Impact M Medium Level Requirement/Impact H High Level Requirement/Impact

TABLE II: Security threats and key 6G technologies.

Key Tech.	Security Threat	Description
AI	Poisonous attacks	Training data tampering via intentionally prepared malicious samples (e.g., manipulation of labelled data or weak labelling), and thus influencing the learning outcomes and leading to misclassification and wrong regression outcomes
	Evasion attacks	Target the test phase by attempting to circumvent the learned model by injecting disorders to the test data.
	ML API-based Attacks	When an adversary queries and attack an API of a ML model to obtain predictions on input feature vectors. This may include model inversion (recover training data), model extraction (reveal model architecture compromising model confidentiality) and membership inference (exploit model output to predict on training data and ML model) attacks.
	Infrastructure physical attacks & communication tampering	Intentional outages and impairments in the communication and computational infrastructure lead to impairments in decision-making/data processing and may even put entire AI systems offline.
	Compromise of AI frameworks	Most AI solutions utilize existing AI/ML frameworks. Vulnerabilities in those artefacts or traditional attack vectors towards their software, firmware and hardware environments (especially, cloud-centric operation) target integrity of AI/ML functions.
DLT	The eclipse attack possibility	When blockchain node communications are disrupted or disseminated, it may end up accepting false information that may result in the confirmation of fake transactions.
	Centralization of miners (51% Attack)	Cybercriminals compromise public blockchain applications and acquire or gain control over at least 51% of its mining power, they will be able to manipulate the blockchain.
	End-user vulnerabilities	Individuals can lose or misplace their private keys, compromising their blockchain stored assets (e.g., identity theft, malware, phishing attacks.).
	Software Vulnerability	When certain DLT projects deploy inadequately tested code on live blockchains, the vulnerabilities and bugs can be detrimental to the decentralized model of many blockchain solutions.
Quantum Comm.	Quantum cloning attack	Take a random quantum state of an information and make an exact copy without altering the original state of the information.
	Quantum collision attack	A quantum collision attack occurs when two different inputs of a hash function provide the same output in a quantum setting.
THz	Access control attacks	Adversaries break access controls, steal data or user credentials in order to access unauthorized resources or modify system parameters.
	Eavesdropping	Although transmissions with high directionality in narrow beams are robust to interception attacks, there is still a possibility for malicious nodes intercepting the signal
VLC	Eavesdropping	As vulnerable as RF when nodes are deployed in public areas and/or the presence of large windows in the coverage areas, and in presence of cooperating eavesdroppers. Also, high throughput indoor VLC systems.
	Jamming or data modification attacks	In VLC or hybrid VLC-RF systems, malicious transmitters can pass undetected. Highly directed transmitter, such as by using optical beamforming techniques, increases the successful attack probability.

III. Technologies and Security Considerations

This section discusses 6G technologies and the related security issues/ solutions(i.e., current and future work).

A. Distributed and Scalable AI/ML security

6G envisions autonomous networks which will perform Self-X (self-configuration, self-monitoring, self-healing and self-optimization) without minimal human involvement [11]. The ongoing specification efforts to integrate AI/ML as a native element in future networks such as ETSI ZSM architecture entailing closed-loop operation and AI/ML techniques with pervasive automation of network management operations including security are important steps towards that goal [7]. Since the pervasive use of AI/ML will be realized in a distributed and large-scale system for various use cases including network management, distributed AI/ML techniques are supposed to enforce rapid control and analytics on the extremely large amount of generated data in 6G networks.

In 6G, AI/ML will be spatially pushed closer to the source of data-of-interest for ultra-low latency while distributing ML functions over the network to attain performance gains due to optimized models and ensemble decision making. However, overcoming practical constraints of some network elements (e.g., IoT) such as computational shortcomings and intermittent connectivity is an open challenge [4].

Distributed AI/ML can be used for security for different phases of cybersecurity protection and defense in 6G. The utility of AI/ML driven cybersecurity lies on the advantages in terms of autonomy, higher accuracy and predictive capabilities for security analytics. Nevertheless, there are also difficult challenges for the pervasive use of AI/ML from the cybersecurity aspect, either as cybersecurity enabler or a technique that may lead to security issues under certain circumstances [12]:

- Trustworthiness An eager reliance on AI/ML in future networks raises an evident question: Are ML components trustworthy? This is a more important issue when critical network functions including security are AI-controlled. For this purpose, trusted computing enablers, formal verification techniques and integrity checks are important tools.

- Visibility For controllability and accountability, visibility is crucial. Security experts and monitoring require clear and intelligible insight into AI based schemes, more than black-box operation. A research question is how to timely monitor for security-violating AI incidents.

- AI ethics and liability Once AI/ML is integrated into 6G security, one question becomes fairness and ethical AI: Does AI based optimization starve some users or applications? Specifically, for security, the question becomes whether AI driven security solutions protect all users the same. Another vague point is Who is liable if AI controlled security functions

fail. Liability management is a complicated task with autonomous entities operating in an ICT environment, including 6G security operations.

- Scalability and feasibility For distributed ML setups such as federated learning, data transmissions should be secured and preserve privacy. For AI/ML controlled security functions, scalability is challenging in terms of required computation, communication and storage resources. For instance, FeMBB leads to huge data flows. Integrated with AI/ML based security controls, these flows may cause significant overhead.

- Model and data resilience Models should be secured and robust in the learning and inference phases (e.g., against poisoning attacks). Blockchain is a potential remedy for a distributed, transparent and secure data sharing framework [13].

- Privacy Different ML techniques (e.g., neural networks, deep learning, supervised learning) can be applied for privacy protection in terms of data, image, location, and communication (e.g., Android, intelligent vehicles, IoT).

B. Distributed Ledger Technology (DLT)

As a DLT, recently Blockchain has gained the highest attention in the telecommunication industry. The added advantages of DLTs such as disintermediation, immutability, non-repudiation, proof of provenance, integrity and pseudonymity are particularly important to enable different services in 6G networks with trust and security [14]. The use of AI/ML, and other data analytic technologies, can be a source for new attack vectors (e.g., poisoning attacks in training phase, evasion attacks in testing phase) [15]. Since data is the facilitator of AI algorithms, it is crucial to ensure their integrity and provenance from the trusted sources [16]. DLT has the potential of protecting the integrity of AI data via immutable records and distributed trust between different stakeholders, by enabling the confidence in AI-driven systems in a multi-tenant/multi-domain environment.

While trust provides the needed confidence for users for adopting autonomic AI based security management systems in 6G networks, it may not prevent their breach and failure in AI based systems. Thus, to prevent the failure of AI systems, liability and the responsibility should be carefully addressed. Therefore, trust with liability are complementing to ensure E2E secured service delivery in 6G networks. DLT based Smart contracts can be utilized to define Trust Level Agreement (TLA) [17] and liability of each party or between components in case of TLA violations.

Furthermore, in order to support the role of DLT/blockchain to comply with 6G requirements, most of the current 5G service models need to be significantly evolved. For instance DLT can be used in secure VNF management, secure slice brokering, automated Security SLA management, scalable IoT PKI management, and secure roaming and offloading handling [14]. Blockchain is also a key candidate for privacy preservation in content-centric 6G networks. Having a common communication channel in blockchain may allow network users to be identified by pseudo names instead of direct personal identities or location information.

C. Quantum security

Quantum computing is envisioned to use in 6G communication networks for detection, mitigation and prevention of security vulnerabilities. Quantum computing assisted communication is a novel research area that investigates the possibilities of replacing quantum channels with noiseless classical communication channels to achieve extremely high reliability in 6G. With the advancements of quantum computing, it is foreseen that quantum-safe cryptography should be introduced in the post-quantum world. The discrete logrithmic problem, which is the basis of current asymmetric cryptography, may become solvable in polynomial time with the development of quantum algorithms (e.g., Shor) [18].

Since quantum computing tends to use the quantum nature of information, it may intrinsically provide absolute randomness and security to improve the transmission quality [18]. Integrating post-quantum cryptography schemes with physical layer security schemes may ensure secure 6G communication links. Novel research eras may open up by introducing ML-based cyber-security and quantum encryption in communication links in 6G networks. Quantum ML algorithms may enhance security and privacy in communication networks with the quantum improvements in supervised and unsupervised learning for clustering and classification tasks. There are promising 6G applications where there are potentials in applying quantum security mechanisms. For instance, many 6G applications such as ocean communication, satellite communication, terrestrial wireless networks, and THz communications systems have potentials of using quantum communication protocols such as quantum key distribution (QKD) [19]. QKD is applicable in the conventional key distribution schemes by providing quantum mechanics to establish a secret key between two legitimate parties.

D. Physical Layer Security (PLS)

Since security mechanisms are embedded in different layers of a network, they can be used jointly across these layers to implement redundant protection or in a subset of layers for resource-constrained applications. PLS methods will be leveraged by 6G to provide an adaptive additional layer of protection in the context of new enabling technologies, as discussed next.

1) TeraHertz (THz) technology: THz communication (1 GHz to 10 THz) is envisioned to be a key technology for 6G. In such frequencies, there exist an increased directionality of transmitted signals that allows to confine unauthorized users to be on the same narrow path of the legitimate user for intercepting signals, thus offering stronger security at the physical layer. However, the authors in [20] prove that an eavesdropper can also intercept signals, in line-of-sight (LoS) transmissions, by placing an object in the path of the transmission to scatter radiation towards him. A countermeasure against this eavesdropping technique, which works by characterizing the backscatter of the channel, was designed in order to detect some, although not all, eavesdroppers. Indeed, THz communications are prone to access control attacks,

malicious behavior, and data transmission exposure. Then, new PLS solutions are required for secure THz transmissions, e.g., electromagnetic signature of materials and devices at THz frequencies can be used for authentication methods [3].

2) Visible Light Communication (VLC) technology: VLC is an optical wireless technology that has attracted high interest due to its advantages compared to radio frequency (RF) systems, such as high data rates, large available spectrum, robustness against interference, and inherent security. VLC systems can offer a higher level of security compared to RF systems due to the fact that light cannot penetrate walls. However, due to the broadcast nature and LoS propagation of VLC systems, they are also vulnerable to eavesdropping from unauthorized nodes located in the coverage area of transmitters. Confidentiality of VLC systems is a crucial issue for the design of practical VLC systems, where PLS techniques can provide interesting solutions. For instance, the accurate localization capabilities of VLC joint with ML techniques can be used for anomaly detection [21].

3) Molecular communication (MC): In MC, bionanomachines communicate using chemical signals or molecules in an aqueous environment, thus being a promising technology for 6G in many healthcare applications. However, MC tackles highly sensitive information, with several security and privacy challenges related to the communication, authentication and encryption process, thus providing secure MC is imperative. Therefore, the notion of biochemical cryptography was introduced in [22], where a biological macro-molecule composition and structure could be utilized as a medium to maintain information integrity. In [23], the primary benefits and limits of PLS in diffusion-based channels are investigated, where the secrecy capacity is derived to obtain insights on the number of secure symbols a diffusion-based channel can afford.

IV. Conclusion

This paper summarized the envisioned main requirements, paradigms, new architectural challenges, new applications, and enabling technologies that are expected to shape the future generation of wireless networks, 6G, from the perspective of the security and privacy challenges. Herein, we provided our vision on the new threat landscape expected for these networks as well as the promising security solutions and technologies that have the potential to evolve and be part of a holistic solution to protect 6G networks. However, as the specifications of 6G networks have not yet been defined, there is not adequate literature to support very insightful discussions. In future, we intend to make a more detailed survey to investigate the security and privacy aspects of 6G and related technologies.

Acknowledgment

This work is supported by 6Genesis Flagship (grant 318927) and 5GEAR projects. The research leading to these results partly received funding from European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

References

[1] C. de Alwis, A. Kalla, Q. V. Pham, P. Kumar, K. Dev, W. J. Hwang, and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2021.

[2] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Communications*, 2020.

[3] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[4] G. Plastiras, M. Terzi, C. Kyrkou, and T. Theocharidcs, "Edge intelligence: Challenges and opportunities of near-sensor machine learning applications," in *2018 IEEE 29th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, 2018, pp. 1–7.

[5] N. Khurana, S. Mittal, A. Piplai, and A. Joshi, "Preventing poisoning attacks on AI based threat intelligence systems," in *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 2019, pp. 1–6.

[6] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks," *Future Generation Computer Systems*, vol. 110, pp. 148–154, 2020.

[7] ETSI ISG ZSM, "ETSI GS ZSM 002: ZSM reference architecture," 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[8] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.

[9] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[10] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, 2020.

[11] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities," *Computer Networks*, vol. 183, p. 107556, 2020.

[12] ENISA, "Artificial intelligence cybersecurity challenges," ENISA, Tech. Rep., December 2020.

[13] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Network*, vol. 34, no. 6, pp. 31–37, 2020.

[14] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit*. IEEE, 2020.

[15] S. Nayak and R. Patgiri, "6G Communication Technology: A Vision on Intelligent Healthcare," *arXiv e-prints*, p. arXiv:2005.07532, Apr. 2020.

[16] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "On-device federated learning via blockchain and its latency analysis," *arXiv preprint arXiv:1808.03949*, 2018.

[17] P. Varalakshmi and T. Judgi, "Multifaceted trust management framework based on a trust level agreement in a collaborative cloud," *Computers & Electrical Engineering*, vol. 59, pp. 110–125, 2017.

[18] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, 2019.

[19] S. Tarantino, B. Da Lio, D. Cozzolino, and D. Bacco, "Feasibility of quantum communications in aquatic scenarios," *Optik*, p. 164639, 2020.

[20] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, E. K. Zahed Hossain, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 8, pp. 89–93, 2018.

[21] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1887–1908, 2020.

[22] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks*, vol. 3, no. 3, pp. 151 – 160, 2012.

[23] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, 2019.