6G Security Vision - A Concise Update

Gürkan Gür*, Pawani Porambage†‡, Diana Moya Osorio‡, Attila A. Yavuz§, Madhusanka Liyanage‡¶
*Zurich University of Applied Sciences (ZHAW) InIT, Switzerland
†VTT Technical Research Centre, Finland
‡Centre for Wireless Communications, University of Oulu, Finland
§University of South Florida, Tampa, FL
¶School of Computer Science, University College Dublin, Ireland
Email: *gueu@zhaw.ch,†pawani.porambage@vtt.fi,‡[firstname.lastname]@oulu.fi, §attilaayavuz@usf.edu, ¶madhusanka@ucd.ie

***Abstract*—The vision and key elements of the 6th generation (6G) ecosystem are being discussed very actively in academic and industrial circles. In this work, we provide a timely update to the 6G security vision presented in our previous publications to contribute to these efforts. We elaborate further on some key security challenges for the envisioned 6G wireless systems, explore recently emerging aspects, and identify potential solutions from an additive perspective. This speculative treatment aims explicitly to complement our previous work through the lens of developments of the last two years in 6G research and development.**

***Index Terms*—6G, Security, DLT, Quantum security, AI/ML, Physical Layer Security (PLS), Post-Quantum Cryptography (PQC), Security threats**

I. Introduction

5G specifications are still maturing, and 5G networks are still being deployed. Nevertheless, 6G networks are already in the development pipeline and are actively being discussed in industrial and academic communities [1]. For instance, the EU is at the forefront with initiatives such as 6G Smart Networks and Services Joint Undertaking (SNS JU)[1] and various industrial initiatives such as the 6G Smart Networks and Services Industry Association (6G-IA)[2] with a dedicated security work group[3]. As part of R&D efforts, various pan-European projects have been implemented with security aspects on Beyond 5G or 6G networks [2]. The critical infrastructure protection perspective has also led to important EU legislations and regulations like the 5G Security Toolbox and EU Cybersecurity Act. Similarly, the Next G Alliance is an initiative to advance North America in research and development, manufacturing, standardization, and market readiness for 6G[4].

These organizations and initiatives envision a hyper-connected and -intelligent ubiquitous network accompanied by advanced communication and Artificial Intelligence (AI) technologies [3]. In that vein, 6G will create seamless digital services and connectivity by integrating various heterogeneous networks in the physical dimension (e.g., UAVs acting as aerial base stations, integrated space networks, and cell-free communications) and novel techniques in the technology dimension, aiming for a universal communication system [4]. Moreover, offloading conventional apps formerly served by wired access while entailing new apps to be supported, such as xR and Metaverse, will require an optimized and cohesive network design [5]. Specifically, the 6G performance is targeted to support sub-ms latency and 1000 km/h users. Moreover, the peak data rate is going to reach above 1 Tbps with 1 GB/m^2 area traffic efficiency. It is also expected to provide ultra-low-power networking and zero-net operation with 100x network efficiency and compliance with UN SDG (Sustainable Development Goals) for sustainable and inclusive development.

However, this vision also brings forth questions about the security of these systems. The integration of primary enablers such as AI, blockchain, Reconfigurable Intelligent Surfaces (RIS), and quantum communications in this heterogeneous architecture will be feasible with a unified framework designed by security considerations from the start [6]. For instance, AI being a native foundational building block in 6G does not inherently translate to improved security and resilience. It may also weaponize nefarious actors and thus become an enabler to impair network operation. The recent surge of very powerful and generally applicable Generative AI models such as ChatGPT complicates this situation. From a historical perspective, the evolution of the security landscape in past network generations has been intertwined and convoluted with the applications, technologies, cost, and requirements of those systems [7].

In this work, we provide an update to our previous works [1] and [7], which entail our 6G security vision. For the sake of brevity, we focus on the aspects recently gaining more attention or prominence in technical discussions. However, we also present our contribution as a self-contained description of the 6G security vision for any interested reader, albeit not being exhaustive.

II. 6G Security Landscape

6G is envisioned to provide an intelligent connectivity and service fabric relying on novel physical, network, and application layer technologies. With 6G networks, security considerations will entail new aspects such as physical layer security, network information security, and AI-related security [8] with deep integration of novel technologies such as

[1] https://smart-networks.europa.eu/
[2] https://6g-ia.eu/
[3] https://5g-ppp.eu/5g-ppp-work-groups/
[4] https://www.nextgalliance.org/

DOI: 10.1109/FNWF58287.2023.10520627

RIS, blockchain, native AI, ubiquitous cloudification, Internet of Everything (IoE), and quantum computing/communication features in such a way to tackle the pressing security issues.

6G is expected to provide ultra-reliable and low latency connectivity, where security solutions such as attack detection and mitigation should be optimized from the perspective of latency impact to provide adequate service quality. Security schemes should also be very effective regarding the protection of availability and resilience to satisfy the ultra-reliability requirements. For extreme data rates in cases such as xR and 8K streaming, security requirements will lead to design and implementation challenges since wire-speed traffic processing for security functions (e.g., AI/ML-based analytics, deep traffic analysis, and post-quantum cryptography) is taxing. In that regard, traffic should be processed locally and on-the-fly in different segments of the network, i.e., in the edge-to-cloud continuum. Distributed security solutions will be instrumental in minimizing traffic overhead, and process flows hierarchically. For this setting, DLT is a promising technology due to its characteristics, namely, transparency, security, and redundancy.

For ultra-large scale networks and machine-type communications in 6G, critical use cases such as autonomous vehicles and collaborative robots impose guaranteed security assurance and defense. Certification of 6G-related hardware and software will be an important aspect of the 6G security framework. In particular, the heterogeneous IoE devices will complicate the deployment and operation of security solutions such as distributed AI/ML, given that they have diverse capabilities and potential resource limitations. Nevertheless, security enforcement and management of secure identities will be more complex since network end devices will have much higher mobility, attaching to different networks and using a plethora of access technologies and services in different administrative domains. The 6G security design should heed the usability and societal aspects, as well — 6G should be transparent, which means the security component should also not hinder usability.

The 6G threat landscape entails attacks on the 6G architecture itself, such as physical attacks and physical layer attacks on specific network elements. Additionally, attacks on key 6G technologies are possible (e.g., AI attacks, including poisoning attacks or eavesdropping on data exchange). From the software security perspective, attacks on 6G applications are possible. Infusion of typical IT security and vulnerabilities are also evident since 6G will be a seamless system with the current Internet. However, the Internet architecture and protocols were not conceived with the ”secure by design” principle. It was built with a premium on openness and interoperability. Therefore, the incumbent threats there will also be valid for 6G networks. Moreover, state actors and international cyber conflicts will have an impact on 6G security as witnessed in current conflicts. Overall, a viable 6G vision should strike a workable balance between enhanced security and openness and backward compatibility.

Following this paper’s foundational rationale, we focus on six specific aspects as an update in this work: *Open RAN*, *Metaverse*, *DLT and blockchain*, *explainable AI*, *physical layer security*, and *quantum-safety for post-quantum communications* in future 6G.

III. 6G Security Challenges and Solutions

This section discusses 6G technologies and the related security challenges with some potential solutions entailing their major aspects and future research directions.

A. Open RAN and RAN-Core convergence

Open RAN, alternatively known as ORAN or O-RAN, revolutionizes traditional radio access network (RAN) technology by disaggregating hardware from software, creating a multi-supplier platform with open interfaces and cloud-based controls. This separation offers increased flexibility for mobile operators during the deployment and upgrade of their RAN. As illustrated in Fig.1, Open RAN aims to achieve cloudification by supporting cloud-native functions, integrating advanced AI/ML capabilities for intelligent automation, and facilitating open internal RAN interfaces as defined by organizations like 3GPP [9].

1) Key security and privacy challenges: One of the major issues is the increased complexity and interdependency of Open RAN. This complexity makes it challenging to identify and isolate security threats. Moreover, vendors may evade responsibility for security flaws due to the complexity and interdependency of the entire system. Moreover, the security of the complete lifecycle process, assessment strategy, and verifying trusted assets and supply chains is a major challenge for Open RAN. Also, it is vital to identify, locate, authenticate, and verify the origin of relevant assets in the system, as some hardware vendors might compromise on security features to maintain lower costs and ensure higher performance. Open RAN also faces risks from predominant attacks and supply chain concerns. If entities from a specific country or region dominate Open RAN’s development and standardization process, it could lead to potential imbalances and espionage possibilities, disrupting the intended openness [9].

Due to the introduction of new technologies, Open RAN also faces security threats associated with cloud computing, network virtualization, and AI [10]. For example, ML attacks such as adversarial training, data or model poisoning could jeopardize the function of automated systems such as RAN Intelligence Controllers (RICs). Network function virtualization-related attacks could be linked to unauthorized access to virtualized resources, while cloud computing-related threats could involve data breaches or denial of service attacks [9].

Another Open RAN feature, open-source software, although advantageous in many ways, can present certain risks. They include known vulnerabilities and potential backdoors, which malicious actors could exploit. Moreover, these concerns add to the absence of trusted coding standards and potential disputes over software patents [11]. Adopting open interfaces also carries its own risks, such as not adhering to industry best security practices. Additionally, strict performance requirements can limit the use of certain security features, leading to increased processing delays [9].

New privacy issues arising from new interfaces, shared environments, and different stakeholders with varying views and objectives on privacy can also pose challenges. These could manifest as ambiguity in responsibility, loss of governance and control, conflicts in objectives for trust, and potential sources for legal disputes [9].

Lastly, ensuring the identification, authentication, and trustworthiness of all stakeholders involved with the Open RAN system is essential. This involves clearly defining and assessing each stakeholder's roles and responsibilities and ensuring that vendors have proven, well-designed and transparent security practices integrated into their engineering processes [9], [12]. Figure 1 presents the key security threats and attacks on the 6G Open RAN system.

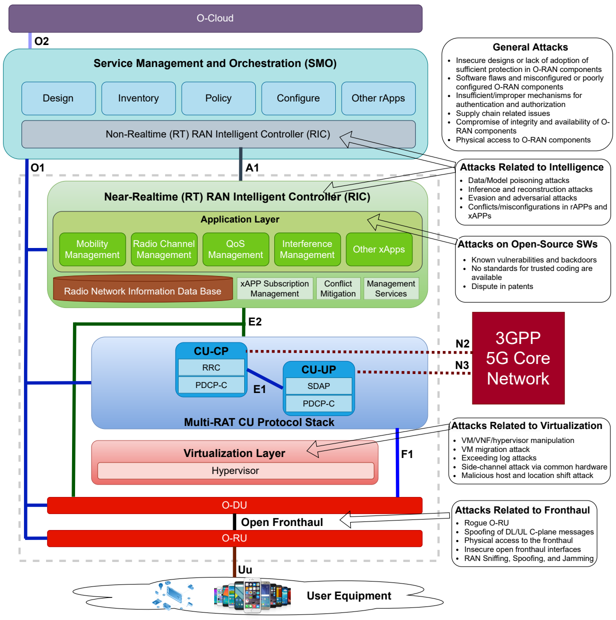
O-Cloud
O2
Service Management and Orchestration (SMO)
Design
Inventory
Policy
Configure
Other rApps
Non-Realtime (RT) RAN Intelligent Controller (RIC)
O1
A1
Near-Realtime (RT) RAN Intelligent Controller (RIC)
Application Layer
Mobility Management
Radio Channel Management
QoS Management
Interference Management
Other xApps
Radio Network Information Data Base
xAPP Subscription Management
Conflict Mitigation
Management Services
E2
CU-CP
RRC
PDCP-C
E1
CU-UP
SDAP
PDCP-C
Multi-RAT CU Protocol Stack
N2
N3
3GPP 5G Core Network
Virtualization Layer
Hypervisor
F1
O-DU
Open Fronthaul
O-RU
Uu
User Equipment
General Attacks
Insecure designs or lack of adoption of sufficient protection in O-RAN components
Software flaws and misconfigured or poorly configured O-RAN components
Insufficient/improper mechanisms for authentication and authorization
Supply chain related issues
Compromise of integrity and availability of O-RAN components
Physical access to O-RAN components
Attacks Related to Intelligence
Data/Model poisoning attacks
Inference and reconstruction attacks
Evasion and adversarial attacks
Conflicts/misconfigurations in rAPPs and xAPPs
Attacks on Open-Source SWs
Known vulnerabilities and backdoors
No standards for trusted coding are available
Dispute in patents
Attacks Related to Virtualization
VM/VNF/hypervisor manipulation
VM migration attack
Exceeding log attacks
Side-channel attack via common hardware
Malicious host and location shift attack
Attacks Related to Fronthaul
Rogue O-RU
Spoofing of DL/UL C-plane messages
Physical access to the fronthaul
Insecure open fronthaul interfaces
RAN Sniffing, Spoofing, and Jamming

Fig. 1: Security threats and attacks on 6G Open RAN system.

2) Security of Open RAN and RAN-Core convergence: Open RAN also comes with a myriad of security benefits. It provides full visibility as virtualization and disaggregated components allow operators to have direct access to all network performance and operational telemetry data from various network functions connected through open interfaces. The network's modularity enables operators to switch to a CI/CD (continuous integration and continuous delivery/deployment) operating model. This makes bug fixes and patch management for remedying any detected security vulnerability more seamless and effective [13].

Moreover, having open interfaces at different levels increases exposure, leading to more scrutiny and, thus, higher overall security. Diversity is another key advantage. By integrating independent and individual modules (both hardware and software), the risk that common coding errors or practices of one single entity have an impact on large parts of a network is decreased, thus reducing the potential range of attacks [9].

In addition, using open-source software can be a boon regarding security. Multiple independent parties often verify that such software is rigorously and variedly tested, ensuring it can be customized to guard against threats effectively. Also, Open RAN's intelligence can be used to automate security management and control through big data analysis, AI and ML, which helps eliminate human errors [9]. There is less dependency between network software and hardware in Open RAN, which facilitates performing the required upgrades faster. This also helps to avoid risks associated with isolated security breaches [9], [12].

In conclusion, Open RAN holds the potential to significantly transform the network technology landscape, resolving many existing issues in Radio Access Networks, primarily through its increased openness and intelligence. Nevertheless, this innovative approach, which enables simultaneous integration of technology from multiple vendors, creates a more complex ecosystem, bringing along a host of new risks and opportunities. Addressing these challenges early in the development phase is crucial to maximize the benefits of Open RAN.

B. Metaverse Security in 6G

The emergence of a fully functional metaverse alongside 6G networks is uncertain. Nevertheless, 6G is poised to play a crucial role in advancing the metaverse by enabling seamless connections between human, physical, and digital realms, potentially leading to a holographic society. The metaverse could encompass diverse human activities such as gaming, social interactions, conferences, and immersive narratives [14] (see Figure 2). The metaverse inherently requires constant user and avatar interactions, necessitating authentication to prevent unauthorized access [16]. Illicit activities such as identity theft, impersonation, and cross-domain authentication challenges can compromise the security of user and avatar identities. Hostile actors might employ AI bots to fabricate avatar identities that mimic human behavior. Malicious entities could exploit

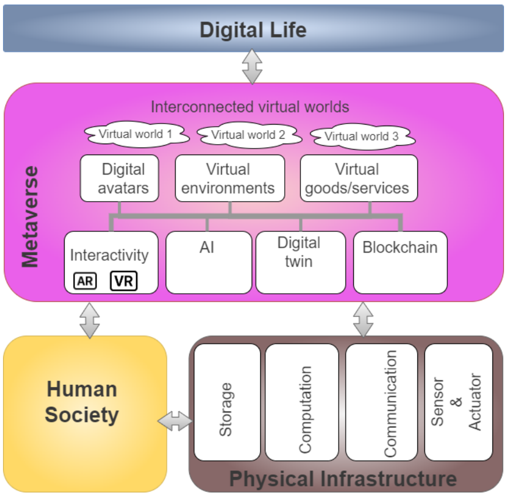

Fig. 2: A conceptual outline for Metaverse architecture [15]

unauthorized data access to manipulate information originating from users and avatars. Wearable device-generated data, along with data from users and avatars, collected for future use, are susceptible to various attacks such as data tampering, false data injection, provenance tracing, and intellectual property breaches. The introduction of novel sensitive data types in the metaverse, coupled with threats to data integrity during collection and transmission, could lead to inferior user experiences and privacy risks. Privacy breaches might manifest during data collection, processing, storage, or transmission. If end devices in metaverse are compromised, they could expose users' privacy-sensitive data, undermining their seamless integration across physical, human, and virtual realms. In a Sybil attack, compromised avatars flood metaverse services with connection requests, impeding access for legitimate avatars of genuine users. For instance, a Sybil attacker might generate multiple fake avatars to manipulate digital voting services and gain control. The metaverse also faces additional threat categories, including breaches of trust, challenges to economic equity, jeopardized personal, infrastructure, and social safety, and governance-related risks [17].

Efficient identity management is a crucial security measure in the metaverse, forming the foundation for user-avatar interactions and service delivery. Digital identities can be overseen by a centralized entity, various institutions, or federations, or held as self-controlled. Within the metaverse, identity management must possess resilience against node damage, scalability to accommodate a vast user/avatar populace and interoperability across multiple sub-metaverses. Establishing secure communication links between wearable devices intertwined with their real-world counterparts requires key management. Equally important is identity authentication across devices and domains to ensure seamless device and user engagement within the metaverse. To mitigate unauthorized access, the implementation of meticulous, precise access controls and comprehensive audit schemes for usage can be adopted.

Regarding data management in metaverse, devising security countermeasures to enhance data reliability, quality, and provenance is imperative. Elevating privacy preservation techniques, confidentiality safeguards, digital footprint protection, and personalized privacy-preserving approaches take precedence in addressing privacy concerns in the metaverse. Similar to personal boundaries in the physical world, avatars in the virtual realm necessitate their own individual space. For comprehensive security monitoring and early prediction of threats in the metaverse, both global and local situational awareness prove indispensable. Augmenting these technical security countermeasures and introducing economic fairness through strategies like game theory, blockchain, auctions, and AI/ML tools can deter manipulation in the metaverse.

C. Distributed Ledger Technologies (DLTs) and Blockchain

As a heterogeneous and multiparty critical infrastructure, 6G ecosystem should support accountability and liability for its constituents. For this purpose, blockchain and DLT are instrumental to enable the security, surveillance, and governance of these systems [18]. This capability stems from the characteristics of the distributed ledger concept as an immutable and transparent pervasive log and allows postmortem auditing of security and fault events for secure and trustworthy operation.

Moreover, the intelligence aspects of a 6G network, such as distributed AI and AI-driven management, imply the implementation of blockchain technologies for the security landscape to ensure the integrity and accountability of AI/ML models. They can also be used to protect the integrity and non-repudiation of ML data sets [19]. With the dominant role of AI in 6G networks, the deployment of proactive security mechanisms and detection of AI-related compromises will be primary security challenges [20]. Thus, blockchain can be used for protecting AI assets as a preventive technology from such threats.

Blockchain can also serve for authentication, authorization, and key management functions in communication networks [21]. It facilitates a common communications channel for multiple tenants operating in a 6G network for cooperation and orchestration. Heterogeneous 6G tenants will restrain authentication and access control systems in 6G due to resource-intensive operation and may cause bottlenecks in related services. The scalability of access control in centralized systems is also constrained. As a result, designing future networks will present a major difficulty for centralized access control [6]. Due to the assessment requirements of a large number of network tenants (such as managing network slices among various renters), auditing will be another difficult security and resilience aspect. It will also be important to develop a secure and decentralized infrastructure as well as a commercial model because 6G calls for interaction between numerous geographically dispersed players [22]. Blockchain can play a primary role in that regard.

Using blockchain characteristics like immutability, transparency, non-repudiation, and provenance, blockchain-based 6G networks may be able to fend against hazards like eavesdropping and hijacking. Furthermore, this integration will lessen the possibility of data manipulation and man-in-the-middle attacks because only the participating nodes may view or add new transactions. For confidential computing, it may serve as a data collection and storage substrate for functions like remote attestation and compliance monitoring to regulations and certification requirements.

Moreover, blockchain can be used as a tool for Secure Service Level Agreement (SSLA) management in future networks. Since 6G networks will use cloud-native technologies, various security-related deployments of blockchain for network softwarization , such as automatic slice brokering, intelligent VNF placement, and proactive service migrations to the edge domain, are also envisaged.

D. Explainable AI

The increasing popularity of opaque decision methods like Deep Neural Networks (DNNs) has made interpretability challenging. DNNs are considered black-box models with hundreds of layers and millions of parameters [23]. The demand for explainability is rising as black-box ML algorithms are used for critical predictions [24], posing risks due to the lack of transparency [25].

Interpretability can enhance ML models in three ways [26]: ensuring objectivity by rectifying bias in training data, improving resilience against adversarial events, and guaranteeing relevant variables for predictions based on actual causation. XAI offers a suite of ML techniques to enable human users to understand, trust, and manage AI systems effectively [26]. This dichotomy is also known as transparent models and post-hoc explainability [27].

1) XAI for 6G Security: In the Beyond 5G (B5G) era, human-centric AI-powered telecommunication attracts various stakeholders who need assurance in trusting these systems. The technical knowledge gap and opacity of AI/ML models pose challenges in providing convincing evidence of their decision-making processes, especially concerning the security of telecommunication technology. Security in data communications has gained significant attention from both malevolent and benevolent agents across all network layers.

With further enhancement of network softwarization (NS) in the B5G era, data is collected through IoT devices in the first B5G architecture layer to support real-time services in higher layers. XAI can address differences in data usage and security/privacy concerns by providing more details about how collected data is used in AI models throughout the pipeline. It is also instrumental in identifying the performance of each device running in the AI system [28].

The RAN, edge, core, and backhaul layers play a vital role in reaching ultra-high bitrates and delivering services with high and assured quality via enhanced virtualization techniques in 6G. Since these layers will handle massive data volumes, their security is envisioned to be addressed through AI/ML-based closed-loop schemes. Therefore, automated feedback on AI/ML system performance is essential to ensure resilience by recognizing false predictions and diagnosing system issues. These aspects are important for informing non-technical stakeholders. In E2E slicing and ZSM, AI/ML components' security is integral to the system architecture. For example, ZSM's E2E service intelligence relies on data collected in the domain and standard data services, making it vulnerable to attacks targeting these data streams. XAI can be highly useful in estimating the overall impact of attacks and identifying the responsible module.

The application layer requires high-level explanations to instill trust and confidence in end-users. Techniques like counterfactual explanations are ideal for achieving this objective. When designing a system with explainable security, evaluating the traditional 6W questions (Why, Who, What, Where, When, and HoW) is crucial for generating security explanations. Identifying the purpose, recipients, content granularity, and layer-specific requirements for explanations helps tailor the system effectively. Decisions on accessibility, timing, and XAI methods complete the groundwork for providing high-quality explanations [25].

E. Physical Layer Security

6G world is already exacerbating the concerns for security and privacy in communication networks as billions of devices are expected to be collecting and transmitting data, which may contain highly vulnerable information in certain applications. At the same time, the pervasive use of AI/ML in 6G networks and the rapid advancement in quantum computing will enable novel and unexpected threats toward 6G architecture and services. In many applications in the IoT domain, devices are highly heterogeneous, with extreme constraints in terms of resources and capabilities, which imposes significant challenges to well-established security approaches, mostly performed at higher layers of the communication stack. After several decades of research, physical layer security (PLS) is being placed as a potential solution to emancipate networks from complex security approaches [29]. Thus, the role of PLS is strongly resonating for the 6G era to provide confidentiality, data integrity, and authentication by exploring the inherent characteristics of wireless channels and devices [30].

Toward 6G, a number of disruptive key technologies such as massive multiple-input-multiple-output (MIMO), cell-free MIMO, reconfigurable intelligent surfaces (RIS), and sub-THz transmissions are promising to design more effective PLS techniques. Indeed, with high directional links at sub-THz band, high-resolution sensing and imaging capability can be enabled. Thus, an accurate location of users may be possible. Ultimately, enabling environmental awareness by exploiting the new paradigm of integrated sensing and communications (ISAC) will be the key to overcoming some of the main drawbacks for the pragmatization of PLS solutions

Indeed, in the future, networks will become sensors enabling the paradigm of Perceptive Mobile Networks (PMN), as illustrated in Fig. 3, where various nodes of the network, including unmanned aerial vehicles (UAVs), will operate cooperatively to realize highly accurate sensing [31]. On the one hand, the additional sensing functionality of the network can be exploited to learn about the adversary and monitor the environment [32]. On the other hand, ISAC systems may increment the concerns on security and privacy as sensed targets may eavesdrop on information and positions, trajectories, or activities of sensed targets may be exposed [33].

From another perspective, enabling the controllability of the wireless propagation environment will benefit PLS techniques, which are entirely based on the properties and characteristics of those. In that sense, the potentiality of RIS will open significant degrees of freedom for efficient security design based on PLS, once reflected signals can either be added coherently at the intended receiver to improve the received signal power or be added destructively at the non-desired directions [34]. However, we need to question which vulnerabilities are being opened with the introduction of this new technology and how it influences the design of 6G [35].

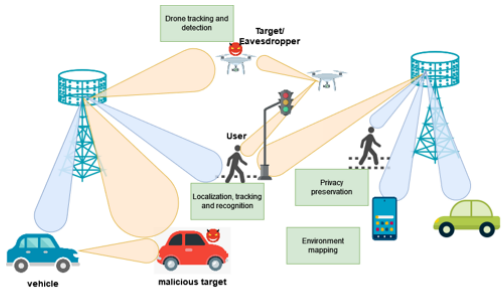

Fig. 3: Opportunities and challenges on PMN from the PLS perspective.

F. *Quantum-Safety and Distributed Resiliency for 6G*

At the heart of trustworthy 6G networks will lie foundational cryptographic services (e.g., digital signatures) and standards (e.g., NIST FIPS [36]). The backbone of such services is Public Key Infrastructures (PKI) that support secure communication (e.g., TLS) and standard encryption suites. However, the existing standards and PKIs are at severe risk of not fulfilling the security and performance needs of 6G in the wake of the post-quantum era and increased attack vectors of hyperconnected 6G applications.

The emergence of quantum computers will render current conventional-secure cryptographic primitives insecure. This threat requires a timely transition to Post-Quantum Cryptography (PQC) for 5/6G networks [37]. The recent NIST-PQC standards [38] and their integration into secure communication protocols (e.g., PQ-TLS [39]) will be key requirements for 6G applications. However, it is well-known that NIST-PQC standards are not designed with mobile networks in mind, and their practical deployment of 6G applications is a challenging task. NIST initiated a new call for alternative PQC schemes to open more options for the future.

6G-enabled systems harbor resource-limited IoT devices yet expect to serve low-latency applications such as digital twins, virtual reality, and autonomous vehicular networks. Hence, it is expected that the heavy end-to-end delay introduced by PQ-PKI and large PQ certificate chains will be major challenges in the adaptation of PQC in 6G. We envision that lattice-based PQC alternatives (e.g., Dilithium/Kyber in [38]) will be prominent candidates for PQ-TLS in 6G. We further envision that current and emerging PQC standards will be enhanced with algorithmic optimizations akin to their conventional-secure counterparts to overcome these performance hurdles. Among potential solutions, we consider offline-online transformations (e.g., [40]) and hardware acceleration [41] to be of importance by shifting message-independent operations into the offline phase while speeding up real-time cryptographic operations on demand. Furthermore, we envision certificateless cryptography to be a potential solution to mitigate the PQ certificate burden, although the current research demonstrates the challenges of adapting such techniques in lattice settings.

Another critical weakness of current mobile networks is that they suffer from algorithmic and architectural centrality. A prominent example of such weakness is PKI breaches, in which a compromised root Certificate Authority (CA) can make catastrophic impacts on millions of users. Although one may consider implementing basic distributed solutions (e.g., secret sharing, replicated CAs), the execution of cryptographic algorithms remains still centralized. Standardization institutions recently promoted distributed cryptographic solutions (i.e., NIST IR 8214C [42]) that can be coupled with future decentralized deployments of 6G systems. NIST's threshold (distributed) cryptography efforts initially aim at transforming current conventional-secure standards with an eye to advanced primitives. Hence, we envision that thresholding emerging PQC standards (e.g., via secure multi-party computation) will be a primary research effort toward enabling resilient and trustworthy 6G networks. Finally, the integration of physical Quantum Key Distribution (QKD) (e.g., optical or wireless) and PQC solutions may play a role in enhancing the security of 6G networks. There are synergies among PQC, distributed architectures, and QKD systems that can enable a myriad of 6G-enabled applications (e.g., machine learning, virtual reality), and such integrated solutions are promising to be a part of trustworthy 6G networks [43].

IV. Conclusion

This paper presented the key aspects, such as envisioned new technologies and requirements for 6G networks, from the perspective of security challenges. Herein, we provided a concise update on our vision of the new security landscape for these networks as well as some salient technologies that are relevant or promising towards a holistic security framework in 6G networks. However, please note that, as the specifications of 6G networks have not yet been defined, this is a fluidic domain where the final big picture may deviate from the envisaged architecture, applications, and role of various technologies. Eventually, these discussions are instrumental in converging to the most efficient and secure 6G specifications, design, and implementation.

Acknowledgment

Pawani Porambage has been supported by VTT Technical Research Centre of Finland, Business Finland funded SUNSET-6G project and Academy of Finland funded XcARet project. The work of Diana Osorio has been supported by the Academy of Finland, project FAITH under Grant 334280. The work of Attila A. Yavuz has been supported by the unrestricted gift from the Cisco Research Award (220159), and the NSF CAREER Award CNS-1917627. Madhusanka Liyanage has been partly supported by European Union in SPATIAL (Grant No: 101021808), CONFIDENTIAL-6G (Grant No: 101096435), and Science Foundation Ireland under CONNECT phase 2 (Grant no. 13/RC/2077_P2) projects.

References

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[2] J. Ortiz et al., "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020.

[3] 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.

[4] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020.

[5] A. Kalla, C. de Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *Journal of Industrial Information Integration*, vol. 30, p. 100404, 2022.

[6] 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.

[7] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627.

[8] 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*, vol. 27, no. 5, pp. 126–132, 2020.

[9] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, 2023.

[10] C. de Alwis, Q.-V. Pham, and M. Liyanage, *6G Frontiers: Towards Future Wireless Systems*. Wiley-IEEE Press, 2023, ch. 6G Radio Access Networks, pp. 99–114.

[11] C. De Alwis, P. Kumar, Q.-V. Pham, K. Dev, A. Kalla, M. Liyanage, and W.-J. Hwang, "Towards 6G: Key technological directions," *ICT Express*, vol. 9, no. 4, pp. 525–533, 2023.

[12] P. Porambage and M. Liyanage, *Security and Privacy Vision in 6G: A Comprehensive Guide*. Wiley-IEEE Press, 2023, ch. Open RAN and RAN-Core Convergence, pp. 59–88.

[13] D. Attanayaka, P. Porambage, M. Liyanage, and M. Ylianttila, "Peer-to-peer federated learning based anomaly detection for open radio access networks," in *IEEE International Conference on Communications (ICC) 2023*. IEEE, 2023.

[14] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6G for the Metaverse," *IEEE Wireless Communications*, vol. 30, no. 4, pp. 72–81, 2023.

[15] P. Porambage and M. Liyanage, *Security and Privacy Vision in 6G: A Comprehensive Guide*. John Wiley & Sons, 2023.

[16] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, 2022.

[17] R. Di Pietro and S. Cresci, "Metaverse: security and privacy issues," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2021, pp. 281–288.

[18] A. Kalla, C. De Alwis, G. Gur, S. P. Gochhayat, M. Liyanage, and P. Porambage, "Emerging directions for blockchainized 6G," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2022.

[19] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[20] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2019.

[21] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based authentication for 5G networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 189–194.

[22] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147 029–147 044, 2020.

[23] D. Castelvecchi, "Can we open the black box of AI?" *Nature News*, vol. 538, no. 7623, p. 20, 2016.

[24] A. Preece, D. Harborne, D. Braines, R. Tomsett, and S. Chakraborty, "Stakeholders in Explainable AI," *arXiv e-prints*, p. arXiv:1810.00184, Sep. 2018.

[25] T. Senevirathna, V. H. La, S. Marchal, B. Siniarski, M. Liyanage, and S. Wang, "A survey on XAI for beyond 5G security: technical aspects, use cases, challenges and research directions," *arXiv preprint arXiv:2204.12822*, 2022.

[26] A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins *et al.*, "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.

[27] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A survey of methods for explaining black box models," *ACM computing surveys (CSUR)*, vol. 51, no. 5, pp. 1–42, 2018.

[28] C. Sandeepa, T. Senevirathna, B. Siniarski, M.-D. Nguyen, L. Vinh-Hoa, S. Wang, and M. Liyanage, "From opacity to clarity: Leveraging XAI for robust network traffic classification," in *2023 Asia-Pacific Advanced Network (APAN) 56 Conference*. IEEE, 2023.

[29] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101 437–101 447, 2020.

[30] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023.

[31] X. A. Flores Cabezas, D. P. Moya Osorio, and M. Juntti, "A Framework for UAV-based Distributed Sensing Under Half-Duplex Operation," *arXiv e-prints*, p. arXiv:2302.10673, Feb. 2023.

[32] N. Su, F. Liu, and C. Masouros, "Sensing-assisted physical layer security," in *WSA & SCC 2023; 26th International ITG Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding*, 2023, pp. 1–6.

[33] I. W. G. da Silva, D. P. M. Osorio, and M. Juntti, "Privacy performance of MIMO dual-functional radar-communications with internal adversary," in *Proceedings of ICC workshops*, 2023.

[34] E. N. Egashira, D. P. M. Osorio, N. T. Nguyen, and M. Juntti, "Secrecy capacity maximization for a hybrid relay-RIS scheme in mmwave MIMO networks," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–6.

[35] H. Alakoca, M. Namdar, S. Aldirmaz-Colak, M. Basaran, A. Basgumus, L. Durak-Ata, and H. Yanikomeroglu, "Metasurface manipulation attacks: Potential security threats of RIS-aided 6G communications," *IEEE Communications Magazine*, vol. 61, no. 1, pp. 24–30, 2023.

[36] National Institute of Standards and Technology, "Digital signature standard (DSS)," FIPS PUB 186-5 (Draft), October 2019, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf.

[37] T. C. Clancy, R. McGwier, and L. Chen, "Tutorial post quantum cryptography and 5G security," *WiSec 19*, 2019.

[38] NIST - PQC, "Status report on the third round of the nist post-quantum cryptography standardization process (nist ir 8413)," July 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf.

[39] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-quantum authentication in TLS 1.3: A performance study," in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

[40] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "Fast authentication from aggregate signatures with improved security," in *International Conference on Financial Cryptography and Data Security*. Springer, 2019, pp. 686–705.

[41] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, "Real-time digital signatures for time-critical networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2627–2639, 2017.

[42] L. Brandao and R. Peralta, "NIST first call for multi-party threshold schemes," https://csrc.nist.gov/pubs/ir/8214/c/ipd, 2023.

[43] A. A. Yavuz, S. E. Nouma, T. Hoang, D. Earl, and S. Packard, "Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era," in *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. IEEE, 2022, pp. 29–38.