University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

MSc Digital Systems Security

Thesis

Roadmap to risk assessment on 6G

Supervisor Professor: Prof. Christos Xenakis

Dimitris Gastouniotis | gastouniot@gmail.com | MTE2104

Piraeus

03/04/2024

Introduction

The inception of wireless communication can be traced back to the emergence of first-generation cellular networks (1G) during the 1980s. Since then, the telecommunication and networking sectors have achieved remarkable advancements with the introduction of 2G, 3G, and 4G cellular networks. Presently, there is ongoing progress in the development of fifth generation (5G) wireless technologies, which are expected to be fully operational by 2025, relying extensively on software-driven solutions. A key element of 5G is the implementation of a microservice-based architecture, which transforms networks into cloud-based systems. This innovative approach facilitates the virtualization of physical resources, resulting in the creation of virtual and logical environments that seamlessly provide automated learning management functions as needed.

Passage: Even as 5G coverage continues to expand, experts are already looking ahead to the next phase of mobile communication: 6G. While the standardization process for 6G is set to begin in 2026, researchers are already delving into innovative approaches to turn this vision into a reality. In the realm of networking and communication, industry professionals anticipate that 6G wireless networks will be distinguished by intelligent management and coordination, achieved through the utilization of cutting-edge technologies such as reconfigurable intelligent surfaces (RIS), visible light communications (VLC), electromagnetic–orbital angular momentum, cell-free communications, and quantum computing. The building blocks of 5G advancement, including virtual radio access networks (vRANs) and cloud-based core networks, are laying the foundation for the architecture of 6G. This architectural framework is continuously evolving, incorporating enhancements to platforms, improvements in functional architecture, advancements in specialization, and refinements in coordination. To ensure optimal execution of Network Functions (NF), a heterogeneous cloud infrastructure is expected to be seamlessly integrated into the 6G architecture (Viswanathan & Mogensen, 2020).

Staying informed about the constantly evolving functions and services offered by different cloud platforms is of utmost importance. It is essential to have the ability to recognize and understand the diverse range of services provided. The functional structure requires the integration of new elements, including the combination of RAN-

core, cell-free radio, and data aggregation for AI at both the physical and administrative levels. Moreover, advancements in this field demand innovative approaches to specialization, such as customized subnetworks, extensive slicing, and flexible workload offloading. To effectively manage 6G cognitive networks, orchestration is achieved through a cognitive closed-loop system and automation (Wijethilaka & Liyanage, 2021).

To ensure the protection and confidentiality of data in the upcoming 6G networks, it is imperative to address concerns surrounding security and privacy across different domains. The unique architecture of 6G networks presents specific challenges in terms of security, as previously stated. Additionally, there is a growing interest in incorporating advanced technologies like blockchain, VLC, TeraHertz (THz), and quantum computing into intelligent 6G networking to effectively combat security and privacy issues. Therefore, it is essential to conduct a comprehensive examination of security considerations in the context of 6G, encompassing aspects such as physical layer security (PLS), network information security, application security, and the security implications associated with deep learning (Porambage, et al., 2021).

Main Part

Chapter 1: Mobile Security

1.1 Evolution of Mobile Security

Throughout the development of mobile networks, encompassing 1G, 2G, and 3G, numerous challenges surrounding security and privacy emerged. These challenges encompassed issues such as cloning, physical attacks, eavesdropping, encryption complications, authentication and authorization problems, and privacy concerns (Wang, et al., 2020). As time progressed, the security threat landscape underwent a transformation, resulting in more intricate attack scenarios and formidable adversaries. The introduction of 4G networks brought forth fresh security and privacy threats, primarily related to the implementation of wireless applications. Examples of these threats included vulnerabilities in the Media Access Control (MAC) layer, such as denial of service (DoS) attacks, eavesdropping, and replay attacks. Furthermore, the rise of malware applications, including viruses and hardware tampering, posed significant risks.

Numerous concerns regarding security and privacy permeate the domain of 5G architecture, impacting various aspects such as access, backhaul, and core networks (Liyanage, et al., 2018). The primary focus in terms of security within the realm of 5G revolves around safeguarding critical infrastructure from cyber threats. Additionally, apprehensions arise in relation to Network Functions Virtualization (NFV), Software-Defined Networking (SDN), and cloud computing (Liyanage, et al., 2018). Specifically, SDN has the potential to introduce vulnerabilities by exposing critical Application Programming Interfaces (APIs) to unintended software, implementing OpenFlow, and centralizing network control, thereby rendering it susceptible to DoS attacks (Khan, et al., 2019).

The advancement of telecommunication networks in 6G is driven by the integration of state-of-the-art networking and AI/ML technologies (Schneier, 2018). However, it is important to recognize that the collaboration between AI and 6G comes with both benefits and drawbacks, as it has the potential to enhance security and privacy while also introducing potential risks (Schneier, 2018).

1.2 Motivation

The reliability and resilience of networks continue to be of utmost importance, despite the advancements in networking and communication technologies. It is crucial for the research community to determine the research directions related to security in the forthcoming 6G networks. Although the specific functions and specifications of 6G are yet to be defined, there is limited literature accessible that provides insights into the security and privacy aspects of networks beyond 5G. To ensure security in 6G, it is vital to build upon the research conducted on 5G and consolidate the emerging research. While numerous 6G vision papers have been published, only a handful of surveys have concentrated specifically on 6G security and privacy. None of the existing surveys offer a comprehensive overview of 6G security, considering the expected advancements in architecture, technology, and application areas. Consequently, the primary aim of this essay is to assess the potential impact of security on future 6G wireless systems. This encompasses addressing challenges, suggesting potential solutions, and identifying areas for future research.

1.3 Security requirements 6G

The forthcoming advancements in 6G technology will impose substantial demands on network capabilities, surpassing the abilities of current 5G networks. These networks have been meticulously crafted to support a wide array of critical 6G use cases, which can be categorized accordingly.

- The attainment of Further Enhanced Mobile Broadband (FeMBB) necessitates achieving an unparalleled peak data rate at the terabits per second (Tbps) level for mobile connections (Nayak & Patgiri, 2020).
- The incorporation of Ultra Massive Machine Type Communication (uMTC) in 6G will augment connection density through the innovative concept of Internet of Everything (IoE), signifying the next stage in the evolution of Internet of Things (IoT).
- These devices will independently and collaboratively establish communication with each other and the infrastructure, enabling collaborative services (Jameel, et al., 2020).

- In the Enhanced Ultra-Reliable, Low-Latency Communication (eURLLC) use case, tailored specifically for latency-sensitive 6G applications, the end-to-end latency must be reduced to an unprecedented level of microseconds (μs).
- To meet the rigorous requirements of 6G, there is an imperative to enhance network energy efficiency by a factor of 10 compared to 5G and 100 compared to 4G.
- Moreover, it is anticipated that this technology will provide a means of communication that is not only efficient but also energy-saving for devices that have limited capabilities. Additionally, advanced mobility management systems will intelligently and proactively ensure smooth and immediate transitions, even at speeds exceeding 1000 km/h (Zhang et al., 2019).
- In order to maintain the delivery of exceptional service, ERLLC will evaluate how security workflows impact latency.
- The significance of reliability compels the adoption of efficient security measures to protect the availability of resources and services.
- The extensive amount of data associated with FeMBB presents unique obstacles for security protocols, including identifying attacks, utilizing AI/ML pipelines, analyzing traffic, and implementing pervasive encryption.

However, these challenges can be overcome by implementing distributed security solutions that allow for local and real-time processing of traffic across different segments of the network, spanning from the edge to the core service cloud (Ranaweera, et al., 2021). In this context, DLT will play a crucial role in ensuring transparency, security, and redundancy. Additionally, umMTC will address critical use-cases that have even more stringent security requirements compared to 5G. Lastly, the diverse capabilities of IoE will pose deployment and operational challenges for security solutions, particularly regarding distributed AI/ML and privacy concerns.

As the number of devices with limited resources continues to grow, it is imperative to prioritize and maintain the highest level of security. However, ensuring the safety of these devices becomes increasingly intricate when network entities are highly mobile, frequently moving between edge networks and accessing services within various administrative domains.

The realm of 6G networks encompasses a vast array of advancements and innovations, spanning architecture, applications, technologies, policies, and standardization. Similar to the overarching vision of 6G, which builds upon the intelligence of cloud-based and software-driven 5G networks, the security aspect of 6G is intricately intertwined with artificial intelligence, resulting in automated security measures. However, it is essential to recognize that adversaries are growing increasingly sophisticated and capable of generating novel security threats. The ongoing challenge lies in the detection of zero-day attacks, while prioritizing the prevention of their propagation is a more feasible objective. Hence, the integration of intelligent and adaptable security mechanisms into 6G networks holds utmost significance in anticipating, identifying, mitigating, and proactively addressing security breaches, as well as minimizing the dissemination of vulnerabilities. Moreover, safeguarding privacy and fostering trust among stakeholders within their respective domains are equally vital goals.

The close connection between security and privacy is evident, as the primary objective of security is to safeguard data, while privacy focuses on maintaining the confidentiality of individuals. Although these two concepts are separate, privacy cannot be effectively maintained without the implementation of robust security measures to protect sensitive information.

To truly comprehend the vast potential of 6G, it is crucial to thoroughly examine Key Performance Indicators (KPIs) and Key Value Indicators (KVIs), as they offer a comprehensive evaluation that surpasses simple performance metrics (Latva-Aho & Leppanen, 2019). The forthcoming 6G systems are expected to integrate state-of-the-art components, including integrated sensing, artificial intelligence, local computation and storage, and embedded devices. These elements will not only enhance existing KPIs but also necessitate the development of new KPIs and KVIs that have traditionally not been associated with mobile networks. Innovative indicators, such as sensing accuracy, computational round-trip time, and AI model convergence time, are some examples of these novel metrics. The KVIs will play a critical role in quantifying the value of 6G technologies in terms of sustainability, security, inclusiveness, and trustworthiness, aligning with the UN sustainable development goals (Ziegler & Yrjola, 2020). As a result, the introduction of these groundbreaking aspects will significantly impact the design and measurement of security KPIs, as depicted in Table II. To effectively

characterize security within the realm of 6G, it is vital to consider various factors, including PLS, network information security, and AI/ML-related security.

1.4 Security Threat Landscape for 6G Architecture

With the impending advent of 6G networks, there is an unavoidable anticipation of heightened apprehension surrounding security and privacy. This is primarily due to the extensive network of connections that will be established. Within the scope of 6G architecture, a multitude of inventive concepts have been suggested by scholars and experts in the field. One such proposal, put forth by Nokia Bell Labs, presents a pragmatic yet ambitious vision that enables a thorough examination of the security landscape within the framework of 6G architecture.

Ziegler et al. (2020) conducted a comprehensive study exploring the possibilities for advancements in 6G architecture. Their research identified four essential elements that make up the data and information architecture: platform, functions, orchestration, and specialization. The platform component of 6G architecture requires the development of multiple clouds capable of creating a runtime environment that is open, scalable, and agnostic. This environment will not only optimize hardware performance but also enhance the efficiency of data transmission.

Within the realm of architecture, there exist a wide range of subjects that must be addressed in order to ensure the seamless integration and operation of various functionalities within the 6G network. This includes the merging of the RAN core and the incorporation of intelligent radio, both of which play a critical role. The primary objective of architectural design is to enable flexibility by redistributing functions, sub-networks, and implementing extensive segmentation. These design features are of utmost importance as they cater to the diverse requirements and demands within the 6G ecosystem. Furthermore, the coordination component involves intelligent network management, as well as the cognitive closed loop and automation of 6G networks. These elements are vital for effectively overseeing and enhancing the performance of 6G networks.

To sum up, Nokia Bell Labs offers a comprehensive framework that extensively examines the security landscape within the 6G architecture. By taking into account the

platform, functions, orchestration, and specialization, researchers and industry professionals can collaborate to create a network that is both secure and efficient.

In addition, the progression of technology not only signifies advancements but also opens doors for proficient assailants who possess the ability to carry out intricate attacks alongside the development of 6G infrastructure. This occurrence is demonstrated through the application of distributed learning techniques to forecast and preempt malevolent actions driven by artificial intelligence in ever-changing settings, presenting encouraging prospects for detecting such behaviors (Gui, et al., 2020).

The dawn of the 6G era brings with it a multitude of technological advancements, including circuits, antennas, metamaterial-based structures, and AI techniques such as ML, data mining, and data analysis. These advancements present exciting opportunities for overcoming challenges in radio networks. One particular area of focus is enhancing intelligent spectrum access in cognitive radio networks, which necessitates the integration of cutting-edge AI/ML techniques. These techniques will play a vital role in various aspects of radio network operations, encompassing precise channel modeling and estimation, modulation, beamforming, resource allocation, optimal spectrum access, and automated network deployment and management. By incorporating intelligent radio (IR) into the 6G framework, we can anticipate accelerated implementation times and substantial cost reductions for new algorithms and hardware (Letaief, et al., 2019). However, it is crucial to acknowledge that as we embrace the advantages of IR, the importance of prioritizing security and privacy concerns becomes even more paramount, particularly given the increasing demand for mission-critical services in wireless networks.

By infiltrating spectrum access systems with deceptive signals, it becomes possible to manipulate the training of artificial intelligence. This malicious activity grants nefarious entities the ability to take advantage of a substantial portion of the spectrum, thereby depriving other users of its benefits. Furthermore, the wireless channel serves as an entry point for various attacks, such as denial-of-service, spoofing, and the injection of harmful data, all of which can disrupt the functionality of AI. Consequently, it is crucial to efficiently identify and detect instances of malevolent training in order to maintain optimal performance in information retrieval (Yao et al., 2019).

The imminent arrival of the 6G network promises to revolutionize network architecture, bringing forth a transformative change. This will be achieved by seamlessly merging RAN and core functions, resulting in a profound impact. The integration process involves the dispersion and virtualization of various core functions, strategically placing them in closer proximity to RAN for optimal performance of low-latency services. Simultaneously, higher-layer RAN functions will be centralized. This convergence, known as RAN-Core convergence, aims to simplify the network and streamline the implementation of specific services. However, it is of utmost importance that we proactively tackle the security and privacy challenges and opportunities that arise from this convergence as we prepare for the advent of 6G (Viswanathan & Mogensen, 2020).

The clear and undeniable connection between artificial intelligence (AI) and edge computing is most apparent in the realm of 6G wireless applications. To achieve optimal performance, it is essential to shift computational tasks to the edge of the network, a concept known as edge intelligence (EI). EI involves utilizing AI and machine learning (ML) algorithms to acquire, store, and process data at the network's edge (Plastiras, et al., 2018). Within the realm of EI, the aggregation of data generated by multiple devices is a crucial function performed by edge servers. These edge servers then share the aggregated data among themselves for model training, analysis, and prediction purposes. By adopting this approach, devices can experience faster feedback, reduced latency, and lower costs, ultimately enhancing overall performance. However, it is important to recognize that the collection of data from various sources and heavy reliance on AI/ML algorithms also expose EI to security attacks. In such scenarios, establishing trust in EI services becomes of utmost importance to ensure user authentication, access control, model, and data integrity, as well as mutual platform verification.

The utilization of Blockchain in protecting distributed edge services from malicious nodes is effectively showcased in the research conducted by Xu et al. (2020). This innovative technology guarantees the reliability of segmented tasks and crucial data used in the execution of artificial intelligence, thus establishing a secure structure for resource transactions.

Malicious actors can exploit the distributed and interconnected nature of edge computing technology to carry out attacks like data poisoning, data evasion, and privacy

breaches. These illicit activities have the potential to disrupt AI/ML applications and undermine the advantages of Edge Intelligence (EI) (Mukherjee, et al., 2020). To ensure the security of EI, it is vital to develop innovative secure routing schemes and trust network topologies for delivering EI services. Privacy is closely linked to security in the context of EI, as edge devices can gather sensitive information such as user location, health records, activity logs, and manufacturing data. Researchers are exploring various approaches, including federated learning, to address these privacy concerns. Federated learning enables privacy-conscious distributed data training in edge AI models. Furthermore, secure multiparty computation and homomorphic encryption are being considered as methods to design privacy-preserving mechanisms for sharing AI model parameters in EI services.

According to Ziegler et al. (2020), the transition from 5G to 6G will be characterized by the adoption of a cloud-native and microservice framework, resulting in a significant transformation of the overall architecture. This shift towards a cloud-based infrastructure will require the integration of various cloud platforms, including public, private, on-premises, and edge clouds. As a result, effective coordination of communication resources and distributed computing will be crucial, necessitating the orchestration and control of networks. It is important to note that security considerations will vary across different cloud environments and stakeholders, leading to unique challenges. These challenges may involve breaches in access control policies, violations of data privacy, concerns regarding information security, insecure interfaces and APIs, denial of service (DoS) attacks, and the potential for data loss, as highlighted by Kalaiprasath et al. (2017).

According to a survey conducted by Ziegler et al. (2020), the concept of vertical industries in the realm of 5G for industrial automation will persist in the upcoming era of 6G, albeit in a modified form referred to as subnetworks. These specialized systems will function as self-contained and compact units, catering to various application verticals such as in-body, in-car, in-robot, and subnetworks of drones. However, the incorporation of wireless interfaces for these subnetworks may introduce security vulnerabilities, highlighting the need for robust yet lightweight authentication and encryption algorithms, as well as intrusion detection systems to monitor network security. To effectively manage trust boundaries between larger networks and smaller subnetworks, a hierarchical and adaptable authorization mechanism would be more

appropriate. Furthermore, the use of trusted execution environments (TEE) can ensure the confidentiality and integrity of enclosed subnetwork environments.

As we approach the arrival of 6G networks, there is an undeniable sense of excitement mingled with concerns about security and privacy. This is mainly due to the vast web of connections that will be established. Scholars and experts in the field have put forward numerous innovative ideas within the realm of 6G architecture. Among these proposals, Nokia Bell Labs has presented a practical yet ambitious vision that allows for a comprehensive analysis of the security landscape within the framework of 6G architecture.

In their extensive investigation, Ziegler et al. (2020) delved into the potential advancements that can be made in the architecture of 6G. Their study pinpointed four crucial components that constitute the architecture's data and information framework: platform, functions, orchestration, and specialization. The platform aspect of 6G architecture necessitates the establishment of numerous clouds capable of generating a runtime environment that is both open and scalable, while also remaining agnostic. This environment not only maximizes the performance of hardware but also boosts the effectiveness of data transmission.

In the realm of architecture, there is a wide array of topics that must be addressed to ensure the smooth integration and operation of various functionalities within the 6G network. Key aspects include the merging of the RAN core and the integration of intelligent radio, both of which are essential. The main goal of architectural design is to promote flexibility by redistributing functions, sub-networks, and implementing extensive segmentation. These design elements are crucial as they cater to the diverse needs and demands within the 6G ecosystem. Additionally, the coordination aspect encompasses intelligent network management, as well as the cognitive closed loop and automation of 6G networks. These components are vital for effectively overseeing and enhancing the performance of 6G networks.

In conclusion, Nokia Bell Labs presents a comprehensive framework that thoroughly analyzes the security landscape within the context of the 6G architecture. Through a consideration of the platform, functions, orchestration, and specialization, researchers and industry experts can work together to establish a network that is not only secure but also highly efficient.

Furthermore, as technology continues to advance, it not only represents progress but also provides opportunities for skilled attackers who can execute complex attacks in tandem with the evolution of 6G infrastructure. This phenomenon is exemplified by the utilization of distributed learning methods to predict and prevent malicious actions fueled by artificial intelligence in dynamic environments, offering promising possibilities for identifying such behaviors (Gui, et al., 2020).

With the advent of 6G, a wave of technological advancements emerges, encompassing circuits, antennas, metamaterial-based structures, and AI techniques like ML, data mining, and data analysis. These advancements offer exciting prospects for tackling obstacles in radio networks. A specific area of interest lies in enhancing intelligent spectrum access in cognitive radio networks, which mandates the integration of state-of-the-art AI/ML techniques. These techniques will play a crucial role in various facets of radio network operations, including precise channel modeling and estimation, modulation, beamforming, resource allocation, optimal spectrum access, and automated network deployment and management. By integrating intelligent radio (IR) into the 6G framework, we can expect faster implementation times and significant cost reductions for new algorithms and hardware (Letaief, et al., 2019). However, it is essential to recognize that as we embrace the benefits of IR, the need to prioritize security and privacy concerns becomes even more critical, particularly due to the growing demand for mission-critical services in wireless networks.

The manipulation of artificial intelligence training can be achieved by infiltrating spectrum access systems using deceptive signals. This nefarious activity allows malicious entities to exploit a significant portion of the spectrum, resulting in the deprivation of its advantages for other users. Additionally, the wireless channel serves as a vulnerable point for different types of attacks, including denial-of-service, spoofing, and the injection of harmful data. These attacks have the potential to disrupt the functionality of AI. Therefore, it is of utmost importance to efficiently identify and detect instances of malevolent training in order to ensure optimal performance in information retrieval (Yao et al., 2019).

The forthcoming arrival of the 6G network holds the potential to completely transform the structure of networks, ushering in a revolutionary shift. This monumental change will be accomplished by seamlessly merging the functions of RAN and core, resulting

in a significant and far-reaching impact. The integration process will involve the dispersion and virtualization of various core functions, strategically placing them in closer proximity to RAN to optimize the performance of low-latency services. At the same time, higher-layer RAN functions will be centralized. This convergence, referred to as RAN-Core convergence, aims to simplify the network and streamline the implementation of specific services. However, it is crucial that we proactively address the security and privacy challenges and opportunities that arise from this convergence as we prepare for the arrival of 6G (Viswanathan & Mogensen, 2020).

The undeniable link between artificial intelligence (AI) and edge computing is most evident in the domain of 6G wireless applications. To achieve optimal results, it is crucial to transfer computational tasks to the network's edge, a concept known as edge intelligence (EI). EI involves the utilization of AI and machine learning (ML) algorithms to acquire, store, and process data at the edge of the network (Plastiras, et al., 2018). Within the realm of EI, the aggregation of data from multiple devices is a vital function performed by edge servers. These servers then exchange the aggregated data among themselves for purposes such as model training, analysis, and prediction. By adopting this approach, devices can benefit from quicker feedback, reduced latency, and lower costs, ultimately improving overall performance. However, it is important to acknowledge that the gathering of data from various sources and heavy reliance on AI/ML algorithms also expose EI to security breaches. In such situations, establishing trust in EI services becomes paramount in order to ensure user authentication, access control, model and data integrity, as well as mutual platform verification.

Xu et al. (2020) have successfully demonstrated the application of Blockchain technology in safeguarding distributed edge services against malicious nodes. Their research highlights the effectiveness of this innovative technology in ensuring the integrity of segmented tasks and vital data utilized in artificial intelligence operations, thereby establishing a robust framework for secure resource transactions.

The interconnected and distributed nature of edge computing technology can be exploited by malicious individuals to carry out attacks such as data poisoning, data evasion, and privacy breaches. These illicit activities have the potential to disrupt AI/ML applications and undermine the benefits of Edge Intelligence (EI) (Mukherjee, et al., 2020). In order to safeguard the security of EI, it is crucial to develop innovative routing

schemes and trust network topologies that ensure the delivery of secure EI services. Privacy is closely intertwined with security in the realm of EI, as edge devices have the capability to collect sensitive information such as user location, health records, activity logs, and manufacturing data. Researchers are exploring various approaches, including federated learning, to address these privacy concerns. Federated learning facilitates privacy-conscious distributed data training within edge AI models. Additionally, secure multiparty computation and homomorphic encryption are being considered as means to design mechanisms that preserve privacy when sharing AI model parameters in EI services.

The forthcoming transition from 5G to 6G, as discussed by Ziegler et al. (2020), will bring about a notable transformation in the overall architecture, marked by the implementation of a cloud-native and microservice framework. This shift towards a cloud-based infrastructure necessitates the integration of diverse cloud platforms, such as public, private, on-premises, and edge clouds. Consequently, the coordination of communication resources and distributed computing becomes vital, requiring efficient network orchestration and control. It is crucial to recognize that security considerations will differ across various cloud environments and stakeholders, presenting distinct challenges. These challenges encompass breaches in access control policies, violations of data privacy, concerns regarding information security, insecure interfaces and APIs, denial of service (DoS) attacks, and the potential for data loss, as emphasized by Kalaiprasath et al. (2017).

According to a survey conducted by Ziegler et al. (2020), the concept of vertical industries in the realm of 5G for industrial automation will persist in the upcoming era of 6G, albeit in a modified form called subnetworks. These specialized networks will function as self-contained and compact systems, catering to various application verticals such as in-body, in-car, in-robot, and subnetworks of drones. However, the implementation of wireless interfaces for these subnetworks may introduce security vulnerabilities, emphasizing the need for robust yet lightweight authentication and encryption algorithms, as well as intrusion detection systems to ensure network security. To effectively manage trust boundaries between larger networks and smaller subnetworks, a hierarchical and adaptable authorization mechanism would be more appropriate. Additionally, the use of trusted execution environments (TEE) can guarantee the confidentiality and integrity of enclosed subnetwork environments. The

emergence of 6G technology necessitates increased capacity, minimal latency, improved reliability, and extensive machine-to-machine communication.

To fulfill these criteria, a comprehensive revamp of network service orchestration and management will be imperative in the domain of 6G. The forthcoming 6G framework strives to attain intelligent automation for the complete management of networks and services by harnessing the capabilities of artificial intelligence. Spearheading the advancement in facilitating such intelligent network management for networks surpassing 5G is the ETSI ZSM (Zero-touch Network and Service Management) architecture (ETSI, 2020).

In the realm of architecture, there are numerous subjects that hold immense significance within the context of the 6G network. Among these subjects are the integration of the RAN core and the utilization of intelligent radio, both of which play a pivotal role in ensuring the seamless operation and integration of various functionalities within the network. The primary goal of architectural design is to foster flexibility by redistributing functions, implementing extensive segmentation, and establishing sub-networks. These design elements are vital for meeting the diverse requirements and demands within the 6G ecosystem. Additionally, the coordination aspect encompasses intelligent network management, as well as the cognitive closed loop and automation of 6G networks. These components are essential for effectively overseeing and enhancing the performance of 6G networks.

In a nutshell, Nokia Bell Labs presents an all-encompassing structure that meticulously analyzes the security landscape within the 6G framework. By considering the platform, functionalities, orchestration, and specialization, experts from the research and industry sectors can join forces to develop a network that is not only secure but also exceptionally efficient.

Furthermore, the advancement of technology not only facilitates the rise of adept assailants but also empowers them to execute intricate assaults in conjunction with the evolution of 6G infrastructure. This pattern is exemplified by the utilization of distributed learning methods to predict, and proactively counter malevolent activities propelled by artificial intelligence in dynamic environments, offering promising possibilities for the identification of such behaviors (Gui et al., 2020).

The advent of 6G ushers in a new era of cutting-edge technology, encompassing circuits, antennas, metamaterial-based structures, and AI techniques like ML, data mining, and data analysis. These technological advancements offer exciting possibilities for addressing the challenges faced by radio networks. A key area of focus is the enhancement of intelligent spectrum access for cognitive radio networks, which requires the integration of state-of-the-art AI/ML techniques. These techniques will play a crucial role in various aspects of radio network operations, including precise channel modeling and estimation, modulation, beamforming, resource allocation, optimal spectrum access, and automated network deployment and management. By incorporating intelligent radio (IR) into the 6G framework, we can expect faster implementation times and significant cost reductions for both algorithms and hardware (Letaief, et al., 2019). However, it is vital to recognize that as we embrace the benefits of IR, the need to prioritize security and privacy concerns becomes even more essential, especially considering the growing demand for mission-critical services in wireless networks.

The manipulation of artificial intelligence training through the introduction of deceptive signals in spectrum access systems allows malicious actors to exploit a significant portion of the spectrum, depriving legitimate users of its benefits. Additionally, the wireless channel serves as a vulnerable point for attacks, including denial-of-service, spoofing, and the injection of harmful data, all of which have the potential to disrupt AI functionality. Therefore, it is imperative to effectively identify and detect instances of malicious training to ensure optimal performance in information retrieval (Yao et al., 2019).

The imminent arrival of the 6G network is on the verge of completely transforming network architecture. This revolutionary shift will be accomplished by seamlessly merging RAN and core functions, resulting in a convergence that will have far-reaching effects. The integration process involves dispersing and virtualizing various core functions, strategically placing them closer to RAN to enhance the performance of low-latency services. At the same time, higher-layer RAN functions will be centralized. This convergence, known as RAN-Core convergence, aims to streamline the network and facilitate the implementation of specific services. However, it is crucial that we proactively address the security and privacy challenges and opportunities that arise from this convergence as we prepare for the arrival of 6G (Viswanathan & Mogensen, 2020).

The close relationship between artificial intelligence (AI) and edge computing is prominently evident in the realm of 6G wireless applications. To enhance efficiency, it is crucial to shift computational tasks towards the network's edge, a concept known as edge intelligence (EI). EI encompasses the utilization of AI and machine learning (ML) algorithms to gather, store, and process data at the edge of the network (Plastiras, et al., 2018). Within the context of EI, the aggregation of data from multiple devices is a vital aspect fulfilled by edge servers. These servers then collaborate to share the aggregated data, enabling model training, analysis, and predictions. This approach facilitates faster feedback, reduced latency, cost savings, and improved overall performance for devices. However, it is important to recognize that the collection of data from diverse sources and heavy reliance on AI/ML algorithms also expose EI to potential security breaches. In such scenarios, establishing trust in EI services becomes crucial to ensure user authentication, access control, model, and data integrity, as well as platform verification.

Xu et al. (2020) present a remarkable demonstration of how Blockchain can safeguard distributed edge services against the threats posed by malicious nodes. This groundbreaking advancement ensures the dependability of fragmented tasks and vital data used in the incorporation of artificial intelligence, thus establishing a fortified framework for resource exchange.

The interconnected and distributed nature of edge computing technology presents an opportunity for malicious actors to exploit and carry out harmful actions, such as data poisoning, data evasion, and breaches of privacy. These malicious activities have the potential to disrupt the functionality of AI/ML applications and undermine the benefits of Edge Intelligence (EI) (Mukherjee, et al., 2020). In order to ensure the security of EI, it is crucial to develop innovative routing schemes and trust network topologies that prioritize the delivery of secure EI services. Privacy is intimately connected to security within the realm of EI, as edge devices have the ability to collect sensitive information, including user location, health records, activity logs, and manufacturing data. Researchers are actively exploring various approaches, such as federated learning, to address these privacy concerns. Federated learning allows for privacy-conscious distributed data training in edge AI models. Additionally, secure multiparty computation and homomorphic encryption are being considered as potential methods for designing privacy-preserving mechanisms that facilitate the sharing of AI model parameters in EI services.

The progression from 5G to 6G will involve a complete transformation of the underlying architecture, as indicated by Ziegler et al. (2020). This transformation will be characterized by the adoption of a cloud-native and microservice framework. To achieve this, various cloud platforms, such as public, private, on-premises, and edge clouds, will need to be integrated. Consequently, effective coordination of communication resources and distributed computing will become crucial, requiring the orchestration and control of networks. It is worth noting that security considerations will differ across different cloud environments and their respective stakeholders, posing unique challenges. These challenges may encompass breaches in access control policies, violations of data privacy, concerns regarding information security, insecure interfaces and APIs, denial of service (DoS) attacks, and the potential for data loss, as outlined by Kalaiprasath et al. (2017).

According to a survey conducted by Ziegler et al. (2020), the concept of vertical industries in the realm of 5G for industrial automation will continue to exist in the upcoming era of 6G. However, these industries will be transformed into subnetworks, operating as self-contained and compact networks that serve specific application verticals such as in-body, in-car, in-robot, and subnetworks of drones. Nonetheless, the introduction of wireless interfaces for these subnetworks raises concerns about security vulnerabilities. Therefore, it is crucial to implement lightweight yet robust authentication and encryption algorithms, as well as intrusion detection systems to ensure continuous monitoring of network security. To effectively manage trust boundaries between larger networks and smaller subnetworks, a hierarchical and adaptable authorization mechanism would be more appropriate. Additionally, the use of trusted execution environments (TEE) can guarantee the confidentiality and integrity of enclosed subnetwork environments.

In order to accommodate the advancements of 6G technology, certain prerequisites must be fulfilled, such as the expansion of capacity, reduction of latency, enhancement of reliability, and facilitation of machine-to-machine communication. To meet these requirements, a complete overhaul of network service orchestration and management in the realm of 6G is imperative. The upcoming 6G framework strives to achieve intelligent automation for the management of networks and services from end to end, harnessing the capabilities of artificial intelligence. Leading the way in enabling such intelligent network management for networks beyond 5G is the ETSI ZSM (Zero-touch Network

and Service Management) architecture (ETSI, 2020). As we approach the era of 6G networks, concerns regarding security and privacy will undoubtedly surge due to the multitude of connections involved. Within the domain of 6G architecture, numerous innovative concepts have been put forth by both academic researchers and industry experts. Among these proposals, Nokia Bell Labs presents a pragmatic yet ambitious vision that allows for a comprehensive exploration of the security landscape within the framework of 6G architecture.

Ziegler et al. (2020) conducted a thorough examination of the potential advancements in 6G architecture, uncovering four essential components that constitute the data and information architecture. These components encompass platform, functions, orchestration, and specialization. The platform aspect of 6G architecture necessitates the creation of diverse cloud systems capable of establishing a dynamic setting characterized by openness, scalability, and agnosticism. This setting aims to not only optimize the performance of hardware but also improve the effectiveness of data transmission.

In conclusion, Nokia Bell Labs presents a comprehensive framework that provides a thorough analysis of the security environment in the 6G architecture. Through consideration of the platform, functions, orchestration, and specialization, researchers and industry experts can join forces to establish a network that is not only secure but also highly effective.

Furthermore, the forward movement of technology not only enables progress but also provides opportunities for skilled attackers who have the capability to execute complex assaults in tandem with the growth of 6G infrastructure. This phenomenon is exemplified by the utilization of distributed learning methods to predict and prevent malicious AI-driven actions in dynamic environments, offering optimistic possibilities for identifying such behavior (Gui, et al., 2020).

The arrival of the 6G era presents numerous opportunities to tackle challenges in radio networks by leveraging cutting-edge technology. Revolutionary advancements in circuits, antennas, metamaterial-based structures, and AI techniques like ML, data mining, and data analysis have opened up new horizons. A key focus area is the improvement of intelligent spectrum access for cognitive radio networks, which requires the integration of advanced AI/ML techniques. These techniques will play a crucial role

in various aspects of radio network operations, including precise channel modeling and estimation, modulation, beamforming, resource allocation, optimal spectrum access, and automated network deployment and management. By incorporating intelligent radio (IR) into the 6G framework, we can expect faster implementation times and substantial cost reductions for both new algorithms and hardware (Letaief, et al., 2019). However, it is essential to recognize that as we embrace the benefits of IR, the need to prioritize security and privacy concerns becomes even more significant, especially given the growing demand for mission-critical services in wireless networks.

The manipulation of artificial intelligence training can be achieved by introducing deceptive signals into spectrum access systems. This nefarious action enables malicious entities to exploit a significant portion of the spectrum, depriving other users of its benefits. Additionally, the wireless channel serves as a pathway for a range of attacks, including denial-of-service, spoofing, and the insertion of harmful data, which have the potential to disrupt AI functionality. Therefore, it is imperative to effectively identify and detect instances of malicious training in order to uphold optimal performance in information retrieval (Yao et al., 2019).

The imminent arrival of the 6G network is on the cusp of revolutionizing network architecture in a truly transformative manner. This groundbreaking shift will completely transform the landscape by seamlessly integrating RAN and core functions, resulting in a convergence that will have wide-ranging implications. To optimize the performance of low-latency services, the integration process involves dispersing and virtualizing various core functions, strategically positioning them in closer proximity to RAN. At the same time, higher-layer RAN functions will be centralized. Known as RAN-Core convergence, this convergence aims to simplify the network infrastructure and streamline the implementation of specific services. However, as we eagerly anticipate the advent of 6G, it is crucial that we proactively address the security and privacy challenges and opportunities that arise from this convergence (Viswanathan & Mogensen, 2020).

The undeniable and apparent partnership between artificial intelligence (AI) and edge computing is particularly evident in the field of 6G wireless applications. In order to achieve the best possible performance, it is crucial to shift computational tasks towards the edge of the network, a concept referred to as edge intelligence (EI). EI involves the

utilization of AI and machine learning (ML) algorithms to acquire, store, and process data at the network's edge (Plastiras, et al., 2018). Within the realm of EI, the aggregation of data produced by multiple devices is a vital function carried out by edge servers. These aggregated datasets are then shared among different edge servers for the purpose of model training, analysis, and prediction. This approach allows devices to benefit from faster feedback, reduced latency, and cost savings, all while enhancing overall performance. However, it is crucial to recognize that the collection of data from various sources and heavy reliance on AI/ML algorithms also expose EI to potential security risks. In such situations, establishing trust in EI services becomes paramount in order to ensure user authentication, access control, model and data integrity, as well as mutual platform verification.

The groundbreaking study by Xu et al. (2020) demonstrates the effective utilization of Blockchain in safeguarding distributed edge services against the threats posed by malicious nodes. This cutting-edge technology ensures the dependability of fragmented tasks and vital data employed in the implementation of artificial intelligence, thereby establishing a robust framework for resource transactions.

Exploitation of the interconnected and widely distributed nature of edge computing technology by malicious actors can result in a range of detrimental attacks, including data poisoning, data evasion, and breaches of privacy. These malicious activities have the potential to disrupt AI/ML applications and undermine the inherent benefits of Edge Intelligence (EI) (Mukherjee, et al., 2020). In order to safeguard the security of EI, it is imperative to develop innovative routing schemes and network topologies that prioritize trust and ensure the delivery of secure EI services. Privacy is intrinsically linked to security within the realm of EI, as edge devices possess the capacity to collect sensitive information such as user location, health records, activity logs, and manufacturing data. To address these privacy concerns, researchers are actively exploring diverse approaches, including federated learning, which facilitates privacy-conscious distributed data training in edge AI models. Furthermore, secure multiparty computation and homomorphic encryption are being considered as viable methods for designing privacy-preserving mechanisms that enable the sharing of AI model parameters in EI services.

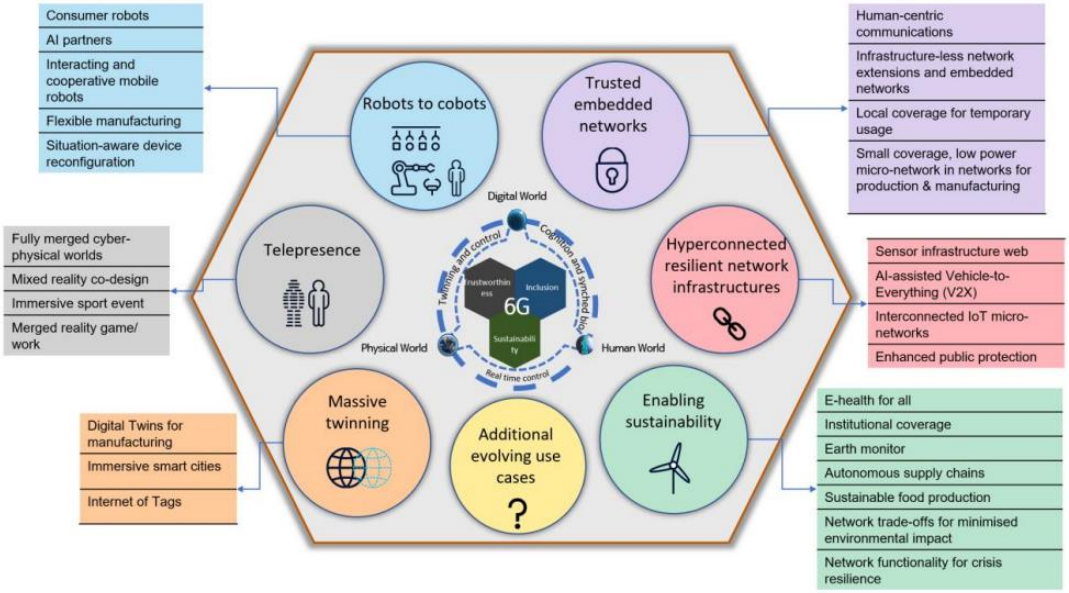

Figure 1. 6g architecture

Chapter 2: Security Challenges with 6G Applications

The future arrival of 6G as a catalyst for network advancements in the 2030s and beyond holds immense potential to revolutionize society, introducing a plethora of innovative applications. However, these applications present significant challenges in terms of both performance and security. Due to their critical nature and the necessity for high levels of trust, it is imperative to implement rigorous security measures. The dynamic interplay between performance expectations and security requirements becomes increasingly intricate with the emergence of skilled and widespread attackers engaging in malicious activities. The possibilities afforded by the capabilities of 6G are vast, offering a multitude of opportunities for groundbreaking applications and use cases. In light of this, we have meticulously identified and extensively explored the most influential 6G applications, with a specific focus on their security considerations. These applications represent early deployment scenarios and are widely recognized within the existing body of research (Saad, et al., 2019).

2.1 UAV based mobility

The rise of 5G technology has sparked a surge in the use of Unmanned Aerial Vehicles (UAVs) across various industries. By integrating 6G and AI-driven services, the potential applications of UAV technologies have expanded even further, encompassing passenger transportation, automated logistics, and military operations (Deebak & Al-Turjman, 2020). However, to meet the resource limitations and low latency requirements of UAVs, it is crucial to implement lightweight security measures. The development of security protocols for UAVs must also consider scalability, device diversity, and high mobility. With 6G supporting AI and Edge-AI functions in UAVs, such as collision avoidance, path planning, route optimization, and swarm control, it becomes essential to deploy effective mechanisms that can mitigate AI-related attacks. Ensuring the integrity of control data is of utmost importance for the safe operation of UAVs, especially considering their unmanned nature. These unmanned vehicles are highly susceptible to physical attacks.

Adversaries have the ability to seize control of unmanned aerial vehicles (UAVs) by either disrupting the control signals or employing specialized equipment, thereby gaining access to the valuable data contained within these aircraft. Furthermore, UAVs possess advanced computational and communication capabilities that surpass those of

other intelligent devices. As a result, a group of drones can be mobilized to carry out synchronized attacks, encompassing a diverse range of offensive actions that range from cyber-attacks to acts of physical terrorism (O'Malley, 2019).

2.2 Holographic Telepresence

The forefront utilization of 6G technology, referred to as holographic telepresence, boasts an extraordinary ability to display lifelike, real-time 3D images of individuals and objects, resulting in an immersive experience that rivals physical presence. This advanced technology encompasses 3D video conferencing and news broadcasting, requiring a significant amount of bandwidth to enable seamless holographic communication. As the number of holographic communication devices continues to rise, the demand for bandwidth also increases. Thus, it is crucial that the security measures implemented for holographic communication do not further strain the already overwhelmed bandwidth. Additionally, when developing these security mechanisms, it is vital to consider factors such as cost-effectiveness and compatibility with various devices. However, the most notable challenge associated with holographic telepresence lies in safeguarding privacy. Specifically, when projecting a holographic image to a remote location, maintaining the necessary level of privacy becomes crucial. Since the remote presenter lacks control over the environmental conditions at the projected location, additional privacy protection measures must be put in place to ensure user privacy.

2.3 Extended reality

The concept of extended reality (XR) encompasses a vast array of virtual and real environments that combine augmented reality (AR), virtual reality (VR), mixed reality (MR), and everything in between (Tariq et al., 2020). The progress of XR will be expedited by 6G, presenting numerous opportunities for its integration in various sectors such as virtual tourism, online gaming, entertainment, online education, healthcare, and robot control. The management of personal data plays a vital role in XR, extending beyond financial information and purchase histories to encompass personal details like emotions, behaviors, judgments, and physical appearance. Consequently, responsible handling of data becomes a crucial requirement for 6G networks, covering aspects such as data collection, storage, protection, and sharing. Furthermore, the utilization of fabricated or falsified data in XR applications would compromise the quality of the user

experience (QoE) in XR. When devising security measures for XR, scalability, minimal overhead, and device diversity must be considered.

The extent of security measures implemented in XR applications can vary significantly based on the specific use case. For instance, military applications necessitate the utmost level of security, encompassing robust multi-factor authentication, data encryption, and user access control. Conversely, entertainment applications may only require a moderate level of security (Siriwardhana, et al., 2021). Additionally, a vital security concern unique to XR is the potential for counterfeit experiences. If counterfeit or manipulated data infiltrates XR applications, it will undermine the overall XR experience. In critical XR environments such as surgery or military operations, the utilization of counterfeit experiences can have life-or-death ramifications.

2.4 Connected Autonomous Vehicles

Nearly 50 prominent automotive and technological companies have shown great interest in and made significant investments towards the development of autonomous vehicle technology. The potential for driverless cars that are completely self-reliant, trustworthy, secure, and economically viable is highly promising. This remarkable progress is being propelled by the emergence of Connected Autonomous Vehicles (CAV) technologies, which will transform transportation services through the introduction of driverless taxis and public transport. However, the intricate nature of the CAV ecosystem also brings about security challenges that can be classified into three main areas: vehicle level, CAV supply chain, and data collection. Attacks targeting the vehicle level can occur through the manipulation of vehicle sensors, V2X communications, and physical control takeover. Although the autonomous nature of these vehicles increases the risk of physical hijacking, they are equipped with advanced features that facilitate the integration of emergency security measures. For instance, in the event of a terrorist attack, the vehicle has the capability to automatically come to a halt. The 6G network can assess the situation and dispatch emergency signals to the vehicles (He, et al., 2020).

Furthermore, within the domain of Connected and Autonomous Vehicles (CAVs), there exists the possibility for the rise of innovative cyber-attacks facilitated by Vehicle-to-Everything (V2X) communications. Cutting-edge CAVs establish a seamless connection with the car manufacturer, facilitating constant surveillance and seamless transmission of software updates to quickly resolve any potential problems wirelessly.

However, if there are weaknesses in the communication channels or if the data from the manufacturer's cloud services is tampered with, it has the capability to jeopardize the safety and security of both the vehicles and their occupants.

In the expansive network that encompasses the CAV ecosystem, various third-party service providers play vital roles. These providers include Communication Service Providers (CSPs), Roadside Equipment (RSE) providers, cloud service providers, and regulators. The main challenge lies in establishing a universally accepted set of security requirements and ensuring smooth interoperability. Privacy concerns may arise when CAVs collect data on travel routes, sensor information, and personal details of owners and passengers. This data becomes an attractive target for malicious attackers. The National Institute of Standards and Technology (NIST) emphasizes the importance of prioritizing device security, data security, and the protection of individuals' privacy within the CAV security framework.

The provision of cutting-edge 6G services, such as XR and holographic telepresence, within the realm of public transportation presents a considerable obstacle in safeguarding personal privacy. Balancing the need for advanced technologies with the protection of sensitive information necessitates a robust security framework for 6G. This framework must effectively address the convergence of physical security and cybersecurity, with a particular emphasis on incorporating the principle of Privacy by Design. This becomes especially crucial in the context of Connected Autonomous Vehicles (CAVs).

2.5 Smart Grid 6.0

With the continuous advancement of smart devices and data analysis techniques, grid networks are undergoing a transformation from Smart Grid 1.0 to Smart Grid 2.0. Smart Grid 2.0 introduces innovative functionalities such as automated analysis of meter data, dynamic pricing based on intelligent algorithms, identification of line losses, automation of distribution grid management, and the ability to provide reliable electricity with self-healing capabilities (Shahinzadeh, et al., 2019). In this new era of grid networks, it is of utmost importance to prioritize network information and cybersecurity to safeguard the confidentiality, integrity, and availability of the energy network. The most prevalent security vulnerabilities encompass a range of attacks, including physical attacks, software-related threats, attacks targeting control elements, network-based attacks, and

attacks associated with AI/ML (Andrea, et al., 2016). These attacks primarily focus on critical components and services such as data access points, control elements (SCADA), the EMS of the cyber-physical system, metering, billing, and information exchange.

The development of smart grid 2.0 places significant emphasis on the importance of trust management, particularly in facilitating peer-to-peer (P2P) energy trading among unfamiliar parties. This type of trading has gained popularity with the increase in small-scale solar PV energy production and electric vehicles. It involves transactions between prosumers or between prosumers and consumers. To handle the large number of transactions involved, it is crucial to establish trust without relying heavily on intermediaries. Furthermore, the shift from a centralized to a distributed mode of smart grid management has created a need for trust between buyers and sellers, a role traditionally fulfilled by third-party intermediaries like Distribution System Operators in a vertical grid structure.

2.6 Industry 5.0

Industry 5.0, the upcoming phase of the industrial revolution, involves a harmonious collaboration between humans, robots, and intelligent machines to infuse a personal touch into the efficiency and automation of Industry 4.0 (Nahavandi, 2019). To facilitate progress in automated industrial environments, the role of 6G technology is paramount. Similar to other applications empowered by 6G, Industry 5.0 will confront significant security risks and must address core security requirements such as authenticity, availability, integrity, and audit aspects. When devising security mechanisms for Industry 5.0, it is crucial to consider factors like cost reduction, device diversity, and scalability. In the era of 6G, safeguarding data security and preserving integrity will be of utmost importance as control commands and monitoring data traverse 6G networks (Xu, 2012). Consequently, the 6G era must also offer highly scalable and automated access control mechanisms and audit systems to restrict access to sensitive resources, including intellectual properties associated with Industry 5.0.

2.7 Intelligent Healthcare

The world of digital healthcare, commonly referred to as e-healthcare, is currently undergoing a significant transformation. In the near future, we can expect to witness the rise of intelligent healthcare driven by AI, incorporating cutting-edge approaches like Quality of Life (QoL), Intelligent Wearable Devices (IWD), Intelligent Internet of

Medical Things (IIoMT), Hospital-to-Home (H2H) services, and innovative business models (Mucchi, et al., 2020). The importance of e-healthcare will be further emphasized by the aging population, making it more crucial than ever before. The integration of Body Area Networks (BANs) and intelligent health systems is pushing us towards personalized health monitoring and management. These personalized BANs have the ability to gather health data from various sensors, interact with the environment, and connect with networking services, including social networks (Isravel, et al., 2020).

Playing a crucial role in connecting intelligent healthcare services, the upcoming era of 6G will serve as the main communication platform. Security challenges in this era will center around guaranteeing secure communication, authenticating devices, and controlling access for the multitude of IoMT and wearable devices. The preservation of user privacy and adherence to ethical standards regarding electronic health records and user data will be of utmost importance in the healthcare system of the future. It is important to note that the management of IoMT devices and health-related information necessitates the utilization of AI. However, current AI models prioritize performance optimization at the expense of ethical considerations. To tackle this issue, AI models must strictly follow ethical guidelines when collecting data and utilizing user data for training purposes. Additionally, these AI models must comply with privacy regulations set forth by regulatory bodies. As the primary communication infrastructure for future healthcare systems, 6G networks must prioritize the safeguarding of patient information and records, ensuring their privacy and integrity.

2.8 Digital Twin

Within the field of industrial control and automation systems, there exists a groundbreaking technology called the digital twin, which has become an essential component of 6G technology. The digital twin essentially functions as a virtual duplicate of a physical object, asset, or product (Grieves & Vickers, 2017). By establishing a connection between Internet of Things (IoT) devices and the physical system, the digital twin acts as a crucial bridge between the virtual and physical realms, enabling the real-time collection of data. This data is then stored in either locally decentralized servers or centralized cloud servers. Following this, the collected data is analyzed and evaluated within the virtual representation of the assets. The insights gained from these simulations are subsequently applied to the actual systems. The integration of data from both the physical and virtual domains plays a vital role in optimizing the performance of physical

assets. Furthermore, the digital twin holds great potential for application in various other fields, including Industry 5.0, automation, healthcare, utility management, and construction.

Ensuring the security of digital twin systems entails addressing various aspects, primarily focusing on securing the communication between the physical and digital realms. Intercepting, manipulating, or replaying communication messages poses significant risks that must be mitigated. As the future unfolds and digital twin systems gain wider adoption, it becomes imperative to integrate highly scalable and secure communication channels to advance 6G technology. Another challenge arises from the unauthorized tampering and modification of IoT data by malicious individuals, which directly threatens privacy. To tackle this issue, it is crucial to prioritize the implementation of mechanisms that guarantee the integrity and protection of IoT data while harnessing the power of 6G for digital twin systems. One potential solution that holds promise in this regard is the utilization of blockchain technology, which presents itself as an ideal candidate for enabling these functionalities within 6G networks (Grieves, 2019).

Chapter 3: Security Impact on New 6G Technologies

This section will explore the security concerns and possible solutions related to specific 6G technologies that have attracted considerable attention, taking into account the security requirements and unique attributes of these networks, as discussed earlier. Although there are several other promising technologies for 6G, their potential security risks and privacy implications have not been extensively studied in current research. On the other hand, certain topics like network softwarization and cloudification have already been investigated in terms of the security of 5G networks.

3.1 Distributed Ledger Technology

Blockchain technology has emerged as the leading distributed ledger technology (DLT) in the telecommunications industry. Its numerous advantages, such as disintermediation, immutability, non-repudiation, proof of provenance, integrity, and pseudonymity, hold immense value in establishing secure and reliable services for 6G networks (Hewa, et al., 2020). However, it is crucial to acknowledge that while AI brings its own benefits to 6G, it also introduces potential vulnerabilities through the use of AI/ML and other data analytic technologies, which can be exploited as new attack vectors in the 6G landscape. Extensive research has demonstrated the susceptibility of ML techniques to various attacks during both the training phase (e.g., poisoning attacks) and the testing phase (e.g., evasion attacks) (Barreno, et al., 2006). Considering that data is the lifeblood of AI algorithms, ensuring the integrity and provenance of this data from trusted sources becomes of utmost importance.

By leveraging DLT, stakeholders can establish a network of trust and ensure the veracity of AI data with the help of unchangeable records. This innovative approach effectively tackles concerns related to trust, instilling a sense of confidence in AI-driven systems operating in a multi-tenant/multi-domain setting.

The utilization of DLT/blockchain technology has the potential to play a vital role in propelling the service models of 5G forward and adapting them to meet the requirements of 6G. These extensive models can encompass a wide array of services, including the management of secure VNFs, brokering secure slices, the automation of Security SLA management, the management of scalable IoT PKI, the handling of secure roaming and offloading, and the protection of user privacy, all in accordance with the needs of 6G (Hewa, et al., 2020). It is imperative to recognize that the convergence of DLT and 6G

also raises concerns regarding the potential security vulnerabilities of blockchain and smart contracts, which could indirectly impact 6G networks. These vulnerabilities typically arise from errors in software programming, limitations within programming languages, and security loopholes in network connectivity (Hewa, et al., 2021). It is crucial to emphasize that these security issues can have an impact on both public and private blockchain platforms, resulting in complications such as compromised accuracy, financial losses in terms of cryptocurrency, and decreased system availability. In the event that malicious individuals gain control of 51% or more of the nodes within the blockchain, they could seize complete control of the entire system.

The prevalence of majority attacks poses a significant threat to the integrity of blockchain systems that depend on consensus through majority voting. According to Dey (2018), there is a concern regarding the manipulation of transaction records by malicious actors, which can impede the verification of valid transactions. Although cryptographic tokens are typically prioritized in most blockchain platforms, there exists a potential vulnerability where users may try to spend a single token multiple times, taking advantage of the intangible nature of digital currency. These fraudulent actions, commonly known as double-spending attacks, underscore the necessity of implementing robust security measures within blockchain systems.

When one smart contract repeatedly calls upon another, a vulnerability known as re-entrancy emerges. It is crucial to acknowledge that the secondary smart contract being invoked may harbor malicious intentions. An infamous instance of this kind of attack took place in 2016, targeting the Decentralized Autonomous Organization (DAO) and resulting in the theft of $50 million worth of Ether by an unidentified hacker (Mehar, et al., 2019). The objective of the attacker or group of attackers in this specific case was to gain control over the blockchain peer network by fabricating fake identities. Blockchain systems that have simplified procedures for adding members are particularly susceptible to Sybil attacks (Cai & Zhu, 2016).

The security of blockchains and smart contracts can be compromised due to various privacy concerns. These concerns encompass the potential compromise of transaction data privacy, smart contract logic privacy, user privacy, and privacy during the execution of smart contracts (Bunz, et al., 2020). Within the blockchain network, certain nodes might inadvertently breach privacy regulations and exhibit an excessive level of

transparency, leading to the unintended revelation of sensitive information such as proprietary knowledge and pricing details. Additionally, when an organization integrates its business logic into the blockchain, it may unknowingly expose confidential data, such as commission rates and bonuses, to competitors (Bunz, et al., 2020).

Alongside concerns regarding privacy, blockchains and smart contracts encounter a range of security risks that demand attention. These risks encompass the annihilation of contracts, disturbances in exceptional cases, weaknesses in call stacks, unpredictable randomness, errors associated with underflow/overflow, vulnerabilities in authentication and access control, security misconfigurations, and computationally demanding operations lacking appropriate restrictions (Li, et al., 2020). It is imperative to tackle these security vulnerabilities to uphold the trustworthiness and dependability of blockchains and smart contracts.

3.2 Possible Solutions

When incorporating DLT/blockchain solutions into 6G networks, it is crucial to follow security protocols that can effectively combat potential attacks. However, the implementation of these security measures may have a more significant impact on public blockchains compared to private blockchains. This difference arises from the complex process of debugging or fixing smart contracts, which are universally adopted by all nodes in a blockchain network (Zhang, et al., 2020). Smart contracts play a vital role in DLT/blockchain systems by enabling automation, highlighting the need to ensure their accuracy. Therefore, it is essential to verify the flawless functionality of smart contracts before deploying them across multiple blockchain nodes. This can be achieved by identifying semantic flaws, using security check tools, and performing formal verification (Atzei, et al., 2017).

To effectively counteract malicious bots and AI agent-based blockchain nodes, it is imperative to implement access control and authentication mechanisms with precision. These fundamental safeguards are pivotal in safeguarding against majority and Sybil attacks. To bolster security even further, it is strongly advised to incorporate privacy preservation measures like privacy by design and TEE into 6G services based on blockchain (Schaar, 2010).

Different types of blockchain/DLT technology, such as public, private, consortium, and hybrid blockchains, offer diverse architectural options. It is important to consider that

the impact of security attacks mentioned previously can differ based on the chosen architecture. For example, 51% attacks pose a significant threat to public blockchains. In cases where specific 6G services, like spectrum management and roaming, involve a smaller number of miners, consortium or private blockchains may be a more appropriate choice (Weerasinghe, et al., 2021).

Hence, it is of utmost importance to meticulously choose the suitable blockchain/DLT type that aligns with the particular 6G application and services in order to effectively minimize the consequences of targeted attacks.

3.3 Quantum Computing

The imminent future will bear witness to the introduction of quantum computing into the commercial market, a development that poses a substantial threat to existing cryptographic systems. Pioneering research indicates that quantum computing will play a crucial role in 6G communication networks by facilitating the identification, mitigation, and prevention of security vulnerabilities. A captivating and emerging field known as quantum computing-assisted communication explores the prospect of substituting quantum channels with flawless classical communication channels to attain unparalleled reliability in 6G networks. Moreover, as quantum computing continues to progress, security experts foresee the necessity for quantum-safe cryptography in a post-quantum era. The advancement of quantum algorithms holds the potential to solve the discrete logarithmic problem, which forms the foundation of current asymmetric cryptography, in polynomial time (Roetteler, et al., 2017).

The introduction of quantum computing into 6G networks offers a remarkable chance to augment both the security of communication links and the quality of transmission. By utilizing the inherent randomness and security of quantum information, quantum computing holds the potential to provide unmatched levels of security while simultaneously enhancing overall transmission quality. To ensure the utmost level of security in 6G networks, it is advisable to combine post-quantum cryptography schemes with physical layer security schemes, as proposed by Bernstein and Lange (2017). Furthermore, the integration of machine learning (ML)-based cybersecurity and quantum encryption in communication links has the potential to unlock new possibilities in this field. Quantum ML algorithms have the capability to significantly improve security and privacy in communication networks, particularly through advancements in

unsupervised and supervised learning for tasks such as classification and clustering. It is worth noting that there are numerous promising applications for 6G networks that can reap the benefits of quantum security mechanisms.

Various forms of communication, such as ocean communication, satellite communication, terrestrial wireless networks, and TeraHertz communication systems, have the potential to utilize quantum communication protocols like quantum key distribution (QKD), as noted by Tarantino et al. (2020). QKD offers a quantum-powered method for establishing confidential keys among authorized entities, making it a viable option for traditional key distribution methods.

It is crucial to recognize that our adversaries have the capability to utilize quantum technology when it comes to quantum-based threats. While quantum computers have not yet reached their full potential, it is vital to proactively evaluate the potential risks they may present to IoT devices. As cryptography plays a critical role in safeguarding IoT networks and devices, the integration of lightweight cryptographic solutions becomes essential. However, the implementation of post-quantum cryptographic solutions that can effectively withstand quantum-based attacks remains an ongoing challenge in the realm of IoT devices. Consequently, the pursuit of device-independent quantum cryptography becomes a formidable undertaking in the post-quantum era of the 6G paradigm.

When it comes to classical information sharing, there is a method known as oblivious transfer (OT) that allows the sender to transmit a single piece of information to the receiver without disclosing which option was sent. However, this feature cannot be maintained in the realm of quantum information, as even the smallest amount of leakage could have significant consequences for the entire communication between the two parties.

In the realm of quantum computers, the fundamental principle that governs their operation renders the preservation of an identical quantum state an unattainable feat. The concept of rewinding or reverting back to a previous state is simply not feasible within this domain. Quantum cloning attacks, on the other hand, involve the audacious endeavor of duplicating a random quantum state without altering the original information. While the creation of flawless replicas of quantum states is strictly prohibited, extensive research has shown that optimal cloning methods can achieve the

utmost precision (Bouchard, et al., 2017). These attacks pose a significant threat to the security of quantum channels, as they can infiltrate even high-dimensional Quantum Key Distribution (QKD) schemes. Furthermore, collision attacks can occur in the quantum domain when two distinct inputs of a hash function produce the same output.

In preparation for the future era of 6G, scientists are actively exploring hardware and encryption solutions that can effectively combat potential threats posed by quantum computing. They have identified several types of post-quantum cryptographic primitives, such as lattice-based, code-based, hash-based, and multivariate-based cryptography. Among these options, lattice computational problems have emerged as a particularly promising choice for IoT devices due to their ability to utilize shorter key lengths, which align with the limitations of 32-bit architecture. It is worth noting, however, that these categories are still undergoing development and are specifically recommended for IoT devices based on their performance, memory constraints, and communication capabilities. As the classical random oracle model is phased out, it may become necessary to verify security in the quantum-accessible random oracle model for post-quantum cryptography. In this model, adversaries have the capability to query the random oracle using quantum states.

3.5 Distributed and Scalable AI/ML

The forthcoming era of 6G technology envisions networks that possess the capacity to execute a multitude of functions, such as self-monitoring, self-configuration, self-optimization, and self-healing, all without any human intervention. This pivotal concept, known as Self-X, plays a vital role in the progression of 6G technology (Zhang & Zhu, 2020). To attain such a remarkable level of automation, the ongoing development of the ZSM architecture incorporates intent-based interfaces, closed-loop operation, and the utilization of AI/ML techniques. These advancements aim to facilitate the complete automation of network management operations, including security, thus bringing us closer to the ultimate objective of autonomous networks. As AI/ML technologies continue to expand into distributed and large-scale systems, their application in network management will necessitate the efficient and expeditious control and analysis of the extensive volume of data generated within these networks.

The forthcoming evolution of wireless technology, known as 6G, presents a remarkable opportunity to enhance security measures in cybersecurity through the integration of

Distributed AI/ML. This integration holds great potential in bolstering security protocols across various domains. By incorporating AI/ML technology into the field of cybersecurity, we can expect numerous advantages, including heightened autonomy, enhanced precision, and cutting-edge predictive capabilities for analyzing security threats.

AI and ML technologies are expected to play a crucial role in the upcoming 6G network. However, this reliance also brings about the possibility of AI/ML-related attacks on the management system of the 6G intelligence network. These attacks can occur in both the training and test phases. During the training phase, known as poisoning attacks, attackers can manipulate the training data by introducing carefully crafted malicious samples. This manipulation can have a significant impact on the learning process, leading to inaccurate predictions and misclassification of services provided by intelligence services supporting end-to-end (E2E) services. In the test phase, evasion attacks aim to bypass the learned model by introducing disturbances to the test data. Additionally, there are model inversion attacks, which seek to derive the training data by utilizing the outputs of the targeted ML model, and model extraction attacks, which involve stealing model parameters to create nearly identical models. These AI/ML-related assaults pose potential threats to the integrity and security of the 6G network. (Khurana, et al., 2019)

Through direct acts of aggression on communication and computational infrastructure, individuals purposefully manipulate these systems to induce disturbances in the flow of information. These disturbances can lead to communication failures and impairments, ultimately posing significant challenges to decision-making processes and data analysis. It is worth noting that these disruptions possess the capability to render AI systems entirely inoperable, as highlighted in the research conducted by Xiao et al. (2015).

The AI middleware layer harbors a significant vulnerability that can be manipulated by compromising the various elements of AI frameworks, such as software, firmware, and hardware. Furthermore, individuals with malicious intent possess the ability to launch attacks that focus on APIs, specifically by querying and targeting the API of a machine learning model to obtain predictions on input feature vectors. This form of attack has the potential to lead to model inversion, where the training data is retrieved, model extraction, which compromises the confidentiality of the model's structure, and

membership inference attacks, which exploit the model's output to predict both the training data and the machine learning model itself.

To mitigate the potential dangers associated with AI/ML, there are several approaches that can be employed. One effective method is adversarial training, which involves incorporating manipulated examples into the training data to simulate attacks and enhance resilience (Kurakin, et al., 2018). Another defensive technique called defensive distillation involves transferring knowledge between neural networks using soft labels, obtained from a previously trained network, which indicate the probability of different classes (Soll, et al., 2019). During training, these soft labels replace rigid labels, allowing for a more flexible classification approach. Both adversarial training and defensive distillation have demonstrated their effectiveness in countering adversarial attacks and evasion attempts.

Ensuring the authenticity and integrity of data during the training phase is crucial in protecting against poisoning attacks. Blockchain technology provides a secure and transparent framework for sharing data, offering a distributed perspective (Li, et al., 2020). To effectively combat adversarial attacks, various techniques, such as input validation and moving target defense, are implemented. Controlling the information received by ML algorithms from APIs proves to be an effective defense strategy against model inversion attacks, effectively preventing these attacks. Additionally, introducing noise to ML predictions, particularly at the execution time of the ML model, serves as a countermeasure against model extraction attacks (Sengupta, et al., 2019).

3.6 Physical Layer Security

By harnessing the unique attributes of erratic and chaotic wireless channels, physical layer security (PLS) techniques have the ability to greatly enhance privacy and streamline authentication and key exchange processes. These techniques hold tremendous promise, especially in resource-constrained scenarios, and when integrated with the groundbreaking advancements of 6G technologies, they unveil a multitude of thrilling possibilities for the future of PLS in the era of 6G.

The imminent arrival of the 6G generation is poised to revolutionize the world of wireless technology. This upcoming generation seeks to push the boundaries of what is currently achievable by harnessing carrier frequencies in the terahertz range, specifically spanning from 1 GHz to 10 THz. The primary goal of this advancement is to optimize

the efficiency and capacity of future wireless networks, guaranteeing widespread access to high-speed Internet. By operating within these frequencies, the transmitted signals become highly concentrated, resulting in a challenging propagation environment. Consequently, interception of these signals is predominantly limited to unauthorized individuals who happen to stumble upon the narrow beam designated for authorized users.

Despite the implementation of concentrated beams, unauthorized individuals still possess the capability to intercept signals in line-of-sight (LoS) transmissions, leaving THz communications susceptible to data exposure, eavesdropping, and access control attacks. Ma et al. (2018) conducted a study that showcased how an illicit user can strategically position an object in the transmission path to redirect radiation towards themselves, thus enabling the interception of signals. The authors propose the examination of channel backscatter as a method for identifying certain eavesdroppers, although its effectiveness may vary. Petrov et al. (2019) suggest utilizing the multipath nature of THz propagation links to enhance information-theoretic security. By dispersing data transmission across multiple paths, the authors were able to significantly decrease the likelihood of message eavesdropping, even in scenarios where multiple eavesdroppers were collaborating. While this approach may slightly impact link capacity, it offers a potential solution for securely transmitting sensitive data or facilitating secure key exchange in THz networks.

In their study, Rahman et al. (2017) examined the concept of authentication within in vivo nano networks that operate at THz frequencies. The researchers investigated the use of distance-dependent path loss as a means of authentication, showcasing its potential as a distinctive identifier in a THz time-domain spectroscopy configuration. By incorporating inventive countermeasures into transceiver designs, it is possible to enhance the effectiveness of physical layer authentication in THz wireless systems by capitalizing on the unique electromagnetic properties of THz frequencies.

VLC, an optical wireless technology, has attracted significant attention due to its multitude of advantages when compared to radio frequency (RF) systems. These advantages encompass rapid data transmission, a diverse array of spectrum choices, immunity to interference, and cost-efficient implementation. Moreover, VLC has the

capability to augment RF systems by harnessing the combined strengths of both networks (Saud et al., 2017).

VLC systems possess inherent security advantages over RF systems due to the inability of light to penetrate walls. However, similar to RF systems, VLC systems are vulnerable to eavesdropping attacks in public spaces or areas with extensive windows, which may compromise the confidentiality of communication (Arfaoui et al., 2020). When designing PLS mechanisms for VLC systems, it is essential to consider the unique characteristics of these systems, such as quasi-static and real-valued channels, as well as the peak-power constraint that restricts unbounded inputs like Gaussian inputs. Consequently, it becomes imperative to reevaluate these operational limitations in order to assess and optimize PLS strategies in VLC systems. Furthermore, research conducted by Chen and Shu (2020) highlights the specific susceptibility of VLC systems in environments characterized by strong reflections.

Arfaoui et al. (2020) delve into the realm of multiple-input multiple-output (MIMO) visible light communication (VLC) systems, specifically examining the potential for improving secrecy performance. Their focus lies in enhancing the achievable secrecy rate while adhering to the constraint of peak power for the transmitted signal. To accomplish this, the researchers exclusively utilize discrete input signaling methods. Similarly, Soderi (2020) delves into the investigation of a blind physical layer security (PLS) scheme for VLC systems. This particular scheme incorporates red, green, and blue LEDs, as well as three color-tuned photodiodes. The ultimate goal is to bolster the system's security by combining a jamming receiver with the spread spectrum watermarking technique.

The advent of reconfigurable intelligent surfaces (RIS) has presented a fresh approach to tackle the obstacles encountered by intelligent environments in terms of security, energy efficiency, and spectral efficiency. RIS employs an array of economical and passive reflecting elements, referred to as metasurfaces, which can be flexibly manipulated to alter the reflective coefficients instantaneously. This dynamic manipulation of the amplitude and phase shift of reflected signals significantly amplifies the wireless propagation performance. The fusion of metamaterials and micro electro-mechanical systems has paved the path for the effective implementation of RIS.

The traditional approaches to guaranteeing Physical Layer Security (PLS), such as using active relays or friendly jammers with artificial noise (AN), often come with high costs and energy consumption. Furthermore, even with the inclusion of AN, achieving satisfactory levels of secrecy performance in intricate wireless propagation environments is a difficult task. Therefore, it is imperative to dynamically control the properties of wireless channels to establish secure communication, a task that cannot be achieved through conventional communication methods.

The potential of reconfigurable intelligent surfaces (RIS) lies in their ability to intelligently manipulate phase shifts, resulting in two distinct outcomes that hold immense promise for the advancement of secure and cost-effective 6G networks. This groundbreaking technology, known as RIS-assisted physical layer security (PLS), offers significant advantages. Firstly, it enables the coherent addition of reflected signals at the desired receiver, leading to a notable enhancement in signal quality. Conversely, it also allows for the destructive addition of reflected signals at an undesired receiver, thereby strengthening security measures. A comprehensive survey conducted by Cui et al. (2019) emphasizes the importance of RIS technology in enhancing security, even when the eavesdropping link performs better than the legitimate link. Furthermore, extensive research has been dedicated to the generation of secret keys for RIS-assisted wireless networks, leveraging the individual scatter properties of each element in the RIS to amplify the capacity for secret key generation.

Bio-nanomachines engage in molecular communication within a liquid environment, utilizing chemical signals or molecules for interaction purposes (Nakano et al., 2019). This revolutionary technology offers immense potential for healthcare advancements in the era of 6G, resulting in tangible progress and real-world implementations. Nevertheless, it is crucial to recognize that the security and privacy obstacles linked to this technology pose significant challenges, especially in areas such as communication, authentication, and encryption protocols when handling extremely sensitive data.

Ensuring the security of MC technology is paramount for fully harnessing its potential benefits. From the very beginning stages of development, prioritizing security is crucial. In this regard, PLS mechanisms play a vital role. The concept of biochemical cryptography, introduced by Dressler and Kargl (2012), is a notable contribution to this field. It leverages the unique composition and structure of biological macromolecules to

safeguard the integrity of information. Furthermore, Mucchi et al. (2019) conducted an extensive survey that comprehensively explores the advantages and limitations of PLS in diffusion-based channels. This survey also calculates the secrecy capacity, providing valuable insights into the maximum number of secure symbols that can be transmitted through such channels.

By harnessing the unique attributes of erratic and chaotic wireless channels, physical layer security (PLS) techniques have the ability to greatly enhance privacy and streamline authentication and key exchange processes. These techniques hold tremendous promise, especially in resource-constrained scenarios, and when integrated with the groundbreaking advancements of 6G technologies, they unveil a multitude of thrilling possibilities for the future of PLS in the era of 6G.

The imminent arrival of the 6G generation is poised to revolutionize the world of wireless technology. This upcoming generation seeks to push the boundaries of what is currently achievable by harnessing carrier frequencies in the terahertz range, specifically spanning from 1 GHz to 10 THz. The primary goal of this advancement is to optimize the efficiency and capacity of future wireless networks, guaranteeing widespread access to high-speed Internet. By operating within these frequencies, the transmitted signals become highly concentrated, resulting in a challenging propagation environment. Consequently, interception of these signals is predominantly limited to unauthorized individuals who happen to stumble upon the narrow beam designated for authorized users.

Despite the implementation of concentrated beams, unauthorized individuals still possess the capability to intercept signals in line-of-sight (LoS) transmissions, leaving THz communications susceptible to data exposure, eavesdropping, and access control attacks. Ma et al. (2018) conducted a study that showcased how an illicit user can strategically position an object in the transmission path to redirect radiation towards themselves, thus enabling the interception of signals. The authors propose the examination of channel backscatter as a method for identifying certain eavesdroppers, although its effectiveness may vary. Petrov et al. (2019) suggest utilizing the multipath nature of THz propagation links to enhance information-theoretic security. By dispersing data transmission across multiple paths, the authors were able to significantly decrease the likelihood of message eavesdropping, even in scenarios where multiple

eavesdroppers were collaborating. While this approach may slightly impact link capacity, it offers a potential solution for securely transmitting sensitive data or facilitating secure key exchange in THz networks.

In their study, Rahman et al. (2017) examined the concept of authentication within in vivo nano networks that operate at THz frequencies. The researchers investigated the use of distance-dependent path loss as a means of authentication, showcasing its potential as a distinctive identifier in a THz time-domain spectroscopy configuration. By incorporating inventive countermeasures into transceiver designs, it is possible to enhance the effectiveness of physical layer authentication in THz wireless systems by capitalizing on the unique electromagnetic properties of THz frequencies.

VLC, an optical wireless technology, has attracted significant attention due to its multitude of advantages when compared to radio frequency (RF) systems. These advantages encompass rapid data transmission, a diverse array of spectrum choices, immunity to interference, and cost-efficient implementation. Moreover, VLC has the capability to augment RF systems by harnessing the combined strengths of both networks (Saud et al., 2017).

VLC systems possess inherent security advantages over RF systems due to the inability of light to penetrate walls. However, similar to RF systems, VLC systems are vulnerable to eavesdropping attacks in public spaces or areas with extensive windows, which may compromise the confidentiality of communication (Arfaoui et al., 2020). When designing PLS mechanisms for VLC systems, it is essential to consider the unique characteristics of these systems, such as quasi-static and real-valued channels, as well as the peak-power constraint that restricts unbounded inputs like Gaussian inputs. Consequently, it becomes imperative to reevaluate these operational limitations in order to assess and optimize PLS strategies in VLC systems. Furthermore, research conducted by Chen and Shu (2020) highlights the specific susceptibility of VLC systems in environments characterized by strong reflections.

Arfaoui et al. (2020) delve into the realm of multiple-input multiple-output (MIMO) visible light communication (VLC) systems, specifically examining the potential for improving secrecy performance. Their focus lies in enhancing the achievable secrecy rate while adhering to the constraint of peak power for the transmitted signal. To accomplish this, the researchers exclusively utilize discrete input signaling methods.

Similarly, Soderi (2020) delves into the investigation of a blind physical layer security (PLS) scheme for VLC systems. This particular scheme incorporates red, green, and blue LEDs, as well as three color-tuned photodiodes. The ultimate goal is to bolster the system's security by combining a jamming receiver with the spread spectrum watermarking technique.

The advent of reconfigurable intelligent surfaces (RIS) has presented a fresh approach to tackle the obstacles encountered by intelligent environments in terms of security, energy efficiency, and spectral efficiency. RIS employs an array of economical and passive reflecting elements, referred to as metasurfaces, which can be flexibly manipulated to alter the reflective coefficients instantaneously. This dynamic manipulation of the amplitude and phase shift of reflected signals significantly amplifies the wireless propagation performance. The fusion of metamaterials and micro electro-mechanical systems has paved the path for the effective implementation of RIS.

The traditional approaches to guaranteeing Physical Layer Security (PLS), such as using active relays or friendly jammers with artificial noise (AN), often come with high costs and energy consumption. Furthermore, even with the inclusion of AN, achieving satisfactory levels of secrecy performance in intricate wireless propagation environments is a difficult task. Therefore, it is imperative to dynamically control the properties of wireless channels to establish secure communication, a task that cannot be achieved through conventional communication methods.

The potential of reconfigurable intelligent surfaces (RIS) lies in their ability to intelligently manipulate phase shifts, resulting in two distinct outcomes that hold immense promise for the advancement of secure and cost-effective 6G networks. This groundbreaking technology, known as RIS-assisted physical layer security (PLS), offers significant advantages. Firstly, it enables the coherent addition of reflected signals at the desired receiver, leading to a notable enhancement in signal quality. Conversely, it also allows for the destructive addition of reflected signals at an undesired receiver, thereby strengthening security measures. A comprehensive survey conducted by Cui et al. (2019) emphasizes the importance of RIS technology in enhancing security, even when the eavesdropping link performs better than the legitimate link. Furthermore, extensive research has been dedicated to the generation of secret keys for RIS-assisted wireless

networks, leveraging the individual scatter properties of each element in the RIS to amplify the capacity for secret key generation.

Bio-nanomachines engage in molecular communication within a liquid environment, utilizing chemical signals or molecules for interaction purposes (Nakano et al., 2019). This revolutionary technology offers immense potential for healthcare advancements in the era of 6G, resulting in tangible progress and real-world implementations. Nevertheless, it is crucial to recognize that the security and privacy obstacles linked to this technology pose significant challenges, especially in areas such as communication, authentication, and encryption protocols when handling extremely sensitive data.

Ensuring the security of MC technology is paramount for fully harnessing its potential benefits. From the very beginning stages of development, prioritizing security is crucial. In this regard, PLS mechanisms play a vital role. The concept of biochemical cryptography, introduced by Dressler and Kargl (2012), is a notable contribution to this field. It leverages the unique composition and structure of biological macromolecules to safeguard the integrity of information. Furthermore, Mucchi et al. (2019) conducted an extensive survey that comprehensively explores the advantages and limitations of PLS in diffusion-based channels. This survey also calculates the secrecy capacity, providing valuable insights into the maximum number of secure symbols that can be transmitted through such channels.By harnessing the unique attributes of erratic and chaotic wireless channels, physical layer security (PLS) techniques have the ability to greatly enhance privacy and streamline authentication and key exchange processes. These techniques hold tremendous promise, especially in resource-constrained scenarios, and when integrated with the groundbreaking advancements of 6G technologies, they unveil a multitude of thrilling possibilities for the future of PLS in the era of 6G.

The imminent arrival of the 6G generation is poised to revolutionize the world of wireless technology. This upcoming generation seeks to push the boundaries of what is currently achievable by harnessing carrier frequencies in the terahertz range, specifically spanning from 1 GHz to 10 THz. The primary goal of this advancement is to optimize the efficiency and capacity of future wireless networks, guaranteeing widespread access to high-speed Internet. By operating within these frequencies, the transmitted signals become highly concentrated, resulting in a challenging propagation environment. Consequently, interception of these signals is predominantly limited to unauthorized

individuals who happen to stumble upon the narrow beam designated for authorized users.

Despite the implementation of concentrated beams, unauthorized individuals still possess the capability to intercept signals in line-of-sight (LoS) transmissions, leaving THz communications susceptible to data exposure, eavesdropping, and access control attacks. Ma et al. (2018) conducted a study that showcased how an illicit user can strategically position an object in the transmission path to redirect radiation towards themselves, thus enabling the interception of signals. The authors propose the examination of channel backscatter as a method for identifying certain eavesdroppers, although its effectiveness may vary. Petrov et al. (2019) suggest utilizing the multipath nature of THz propagation links to enhance information-theoretic security. By dispersing data transmission across multiple paths, the authors were able to significantly decrease the likelihood of message eavesdropping, even in scenarios where multiple eavesdroppers were collaborating. While this approach may slightly impact link capacity, it offers a potential solution for securely transmitting sensitive data or facilitating secure key exchange in THz networks.

In their study, Rahman et al. (2017) examined the concept of authentication within in vivo nano networks that operate at THz frequencies. The researchers investigated the use of distance-dependent path loss as a means of authentication, showcasing its potential as a distinctive identifier in a THz time-domain spectroscopy configuration. By incorporating inventive countermeasures into transceiver designs, it is possible to enhance the effectiveness of physical layer authentication in THz wireless systems by capitalizing on the unique electromagnetic properties of THz frequencies.

VLC, an optical wireless technology, has attracted significant attention due to its multitude of advantages when compared to radio frequency (RF) systems. These advantages encompass rapid data transmission, a diverse array of spectrum choices, immunity to interference, and cost-efficient implementation. Moreover, VLC has the capability to augment RF systems by harnessing the combined strengths of both networks (Saud et al., 2017).

VLC systems possess inherent security advantages over RF systems due to the inability of light to penetrate walls. However, similar to RF systems, VLC systems are vulnerable to eavesdropping attacks in public spaces or areas with extensive windows, which may

compromise the confidentiality of communication (Arfaoui et al., 2020). When designing PLS mechanisms for VLC systems, it is essential to consider the unique characteristics of these systems, such as quasi-static and real-valued channels, as well as the peak-power constraint that restricts unbounded inputs like Gaussian inputs. Consequently, it becomes imperative to reevaluate these operational limitations in order to assess and optimize PLS strategies in VLC systems. Furthermore, research conducted by Chen and Shu (2020) highlights the specific susceptibility of VLC systems in environments characterized by strong reflections.

Arfaoui et al. (2020) delve into the realm of multiple-input multiple-output (MIMO) visible light communication (VLC) systems, specifically examining the potential for improving secrecy performance. Their focus lies in enhancing the achievable secrecy rate while adhering to the constraint of peak power for the transmitted signal. To accomplish this, the researchers exclusively utilize discrete input signaling methods. Similarly, Soderi (2020) delves into the investigation of a blind physical layer security (PLS) scheme for VLC systems. This particular scheme incorporates red, green, and blue LEDs, as well as three color-tuned photodiodes. The ultimate goal is to bolster the system's security by combining a jamming receiver with the spread spectrum watermarking technique.

The advent of reconfigurable intelligent surfaces (RIS) has presented a fresh approach to tackle the obstacles encountered by intelligent environments in terms of security, energy efficiency, and spectral efficiency. RIS employs an array of economical and passive reflecting elements, referred to as metasurfaces, which can be flexibly manipulated to alter the reflective coefficients instantaneously. This dynamic manipulation of the amplitude and phase shift of reflected signals significantly amplifies the wireless propagation performance. The fusion of metamaterials and micro electro-mechanical systems has paved the path for the effective implementation of RIS.

The traditional approaches to guaranteeing Physical Layer Security (PLS), such as using active relays or friendly jammers with artificial noise (AN), often come with high costs and energy consumption. Furthermore, even with the inclusion of AN, achieving satisfactory levels of secrecy performance in intricate wireless propagation environments is a difficult task. Therefore, it is imperative to dynamically control the

properties of wireless channels to establish secure communication, a task that cannot be achieved through conventional communication methods.

The potential of reconfigurable intelligent surfaces (RIS) lies in their ability to intelligently manipulate phase shifts, resulting in two distinct outcomes that hold immense promise for the advancement of secure and cost-effective 6G networks. This groundbreaking technology, known as RIS-assisted physical layer security (PLS), offers significant advantages. Firstly, it enables the coherent addition of reflected signals at the desired receiver, leading to a notable enhancement in signal quality. Conversely, it also allows for the destructive addition of reflected signals at an undesired receiver, thereby strengthening security measures. A comprehensive survey conducted by Cui et al. (2019) emphasizes the importance of RIS technology in enhancing security, even when the eavesdropping link performs better than the legitimate link. Furthermore, extensive research has been dedicated to the generation of secret keys for RIS-assisted wireless networks, leveraging the individual scatter properties of each element in the RIS to amplify the capacity for secret key generation.

Bio-nanomachines engage in molecular communication within a liquid environment, utilizing chemical signals or molecules for interaction purposes (Nakano et al., 2019). This revolutionary technology offers immense potential for healthcare advancements in the era of 6G, resulting in tangible progress and real-world implementations. Nevertheless, it is crucial to recognize that the security and privacy obstacles linked to this technology pose significant challenges, especially in areas such as communication, authentication, and encryption protocols when handling extremely sensitive data.

Ensuring the security of MC technology is paramount for fully harnessing its potential benefits. From the very beginning stages of development, prioritizing security is crucial. In this regard, PLS mechanisms play a vital role. The concept of biochemical cryptography, introduced by Dressler and Kargl (2012), is a notable contribution to this field. It leverages the unique composition and structure of biological macromolecules to safeguard the integrity of information. Furthermore, Mucchi et al. (2019) conducted an extensive survey that comprehensively explores the advantages and limitations of PLS in diffusion-based channels. This survey also calculates the secrecy capacity, providing valuable insights into the maximum number of secure symbols that can be transmitted through such channels.

Chapter 4: 6G Privacy

4.1 Privacy

In the age of digitalization, technology progresses swiftly, giving rise to substantial apprehensions over digital privacy.

- The purpose of data gathering is to improve the quality of service, but it also presents privacy hazards because of the potential for exposure.
- It is imperative to incorporate privacy-preserving methodologies while simultaneously upholding a harmonious equilibrium between privacy and functionality.
- The processing of local data across devices and centralized bodies presents several challenges, hence requiring the implementation of privacy protection systems.
- The emergence of 6G technologies, anticipated to surpass 5G in speed by a factor of 1000, highlights the imperative of safeguarding privacy as a fundamental necessity.
- At now, privacy protection is not given the necessary level of attention and importance in the process of collecting and analyzing data.
- Conducting research is crucial in order to achieve a harmonious equilibrium between improving data privacy and minimizing computational requirements, particularly in the context of 6G.
- The European Union's General Data Protection Regulation (GDPR) should be reevaluated to guarantee its alignment with the changing requirements of 6G technology.
- The advent of 6G necessitates the essential task of surmounting obstacles in privacy protection for both governmental and commercial sectors.
- The widespread use of sophisticated mobile applications heightens susceptibility to assaults, thus requiring the implementation of lightweight privacy techniques.
- Differential Privacy (DP) has emerged as a crucial mechanism for safeguarding privacy in the fields of statistical analysis and machine learning, providing strong and reliable protection.
- The incorporation of blockchain technology in 6G has the potential to improve privacy, but it also presents hazards due to its inherent transparency.

- Advanced artificial intelligence (AI) and machine learning (ML) technologies have a double function: safeguarding privacy and posing possible risks.
- Collaborative robots, also referred to as cobots, underscore the significance of ethical conduct and openness in safeguarding privacy.
- Quantum mechanics present auspicious approaches for safeguarding privacy, particularly considering the capabilities of quantum computers.
- The issue of privacy in 5G/6G technology necessitates the implementation of systems that effectively preserve anonymity and mitigate the risk of information leaking.
- Achieving a harmonious equilibrium between privacy and usability is of utmost importance, as the level of leakage may be deemed acceptable contingent upon the specific application.

4.2 Security Standardization and Projects

ETSI has taken a comprehensive approach to thoroughly analyze the different aspects of 5G technologies by establishing multiple Industry Specification Groups (ISGs). These ISGs cover a wide range of areas such as NFV, AI, and network automation. One of these ISGs, known as NFV-SEC, operates under the ISG NFV and focuses specifically on addressing security concerns related to NFV technology. Since 2014, the NFV SEC WG has actively worked on developing industry specifications for security matters, resulting in the creation of Group Specifications (GS) and Group Reports (GR). The importance of security specifications has been further highlighted in releases 3 and 4 of ETSI NFV as the scope and capabilities of NFV platforms continue to expand.

In 2017, a groundbreaking advancement called ETSI ISG ENI emerged, introducing a comprehensive framework for Cognitive Network Management. This innovative framework utilizes artificial intelligence techniques and context-aware policies to dynamically adapt services based on user needs, environmental factors, and business objectives. The successful implementation of this framework has opened up various possibilities, including enhancing network security. With the ENI system in place, the network has the ability to efficiently detect and identify different types of attacks, leading to swift and appropriate responses. Expanding on this progress, ETSI ISG SAI was established in 2019 with the primary objective of developing technical specifications to address the potential risks associated with deploying AI and the threats

posed by AI systems targeting both other AI systems and traditional attack sources. This dedicated group takes on the crucial responsibility of defining AI threats, presenting relevant use cases, proposing effective measures to mitigate these threats, and providing valuable recommendations for data sharing.

In order to propel the progress of machine learning within upcoming networks, the ITU has established the ITU-T Focus Group on ML for Future Networks (FG-ML5G). The primary aim of this group is to create comprehensive technical specifications that encompass a wide range of elements, including protocols, interfaces, network architectures, algorithms, and data formats (ITU-T Focus Group on ML for Future Networks, 2019). Additionally, the ITU-T FGNET2030 - Focus Group on Technologies for Network 2030 is currently investigating emerging catalysts, requirements, and gaps to propose innovative use cases for applications such as augmented and virtual reality and holograms. These advancements will also have a significant impact on the security aspects of 6G networks.

The integration of AI/ML into the 5G Core Service-Based Architecture (SBA) has been a key focus for 3GPP. This emphasis has led to the development of the Network Data Analytics Function, which plays a vital role in providing analytics and notifications to different network functions. By doing so, it enables a more comprehensive understanding of user behavior and enhances overall network efficiency. Currently, 3GPP SA3 is actively working on a preliminary TR that specifically addresses security concerns, requirements, and potential solutions related to Network Slicing and the utilization of the Network Data Analytics Function in specific use cases (TSG SA, 2020).

In the realm of post-quantum cryptographic algorithms, the National Institute of Standards and Technology (NIST) plays a vital role by setting standards. NIST's dedicated Post-Quantum Cryptography Program aims to identify potential contenders and establish algorithms that can withstand quantum attacks in areas such as digital signatures, public-key encryption, and cryptographic key establishment. The program is currently making steady advancements in Round 3, having successfully completed the second round in July 2020. The algorithms that pass this rigorous process will form the initial set of standards, effectively reducing the risks posed by quantum decryption.

The IETF Security Automation and Continuous Monitoring (SACM) Architecture Request for Comments (RFC) establishes the groundwork for fostering collaboration within the SACM ecosystem. Central to this ecosystem is a collaborative environment that emphasizes the sharing of information among different entities and components. In this framework, specific components serve as consumers of information, while others function as providers. At the core of this architecture lies the orchestrator, which enables automation for essential tasks such as configuration, coordination, and management across various SACM components. Additionally, multiple repositories are accessible, including repositories for policies, vulnerability definitions, and security information.

In order to effectively tackle the various security risks and challenges associated with 5G technology, the 5G PPP has taken proactive measures by establishing the 5G PPP Security Work Group. This collaborative effort provides valuable insights and guidance to address concerns regarding the security of 5G in a comprehensive manner. The work group delves into a wide range of topics, including the architectural aspects of 5G security, its compliance with the 3GPP, access control, privacy, trust, security monitoring and management, as well as standardization efforts in the field of 5G security. While the primary focus remains on 5G networks, the outcomes of this group have broader implications for future networks beyond 5G, encompassing the security of intelligent networks, key performance indicators (KPIs) for security, emerging risks, threats, and countermeasures.

The significance of the NGMN 5G End-to-End Architecture Framework v4.3 (2020) in meeting the security requirements of the dynamic 5G service paradigm is underscored by Porambage et al. (2021). This comprehensive framework not only outlines the fundamental network elements and procedures but also integrates vital security measures to safeguard the wide array of network functionalities and attributes.

The primary objective of the IEEE P1915.1 Standard for SDN/NFV Security is to establish a strong basis for creating and managing secure environments in the realm of SDN/NFV. This standard addresses the diverse needs of various stakeholders, including end users, network operators, and service/content providers. It offers a comprehensive security framework for SDN/NFV, encompassing system models, analytics, and requirements (Porambage, et al., 2021). Similarly, the IEEE P1917.1 Standard for SDN/NFV Reliability focuses on the essential prerequisites for ensuring reliability and

develops a framework that guarantees a trustworthy infrastructure for delivering SDN/NFV services.

At the forefront of quantum communications is the IEEE P1913.1 (Draft) Standard for Software-Defined Quantum Communication (SDQC), playing a vital role in this field. The SDQC protocol, introduced by this standard, allows for the establishment of quantum endpoints within a communication network (Porambage, et al., 2021). Through this protocol, users are empowered with the capability to dynamically create, modify, or remove quantum protocols or applications within a software-defined environment. The key to this flexibility lies in a precisely defined interface to quantum communication devices, which can be reconfigured to support a wide array of protocols and measurements. Operating at the application layer and leveraging TCP/IP, the SDQC protocol also takes into consideration future integration with network softwarization standards.

4.3 Future scientific direction

As the world moves closer to the next frontier in wireless communication, 6G emerges as a beacon of revolutionary potential. It promises to redefine how we connect with one another, engage with technology, and make use of it. 6G is ready to usher in a new era of ultra-fast, secure, and intelligent connection. It will do so by building on the foundations that were introduced by 5G, which brought about speeds and network reliability that had never been seen before. This leap ahead is not merely evolutionary; rather, it marks a paradigm change that will enable a multitude of novel applications, ranging from digital healthcare to smart cities, thereby radically transforming the landscape of technology.

4.3.1 Advancements in Technology Regarding 6G

It is the revolutionary technological improvements that would alter the boundaries of wireless communication that are at the heart of the promise that 6G would provide. The research of the terahertz (THz) frequency range is at the heart of these developments. This band offers data transmission speeds on the order of terabits per second, which is a significant leap that has the potential to render the broadband speeds that are currently available obsolete. Equally as important is the incorporation of technologies that utilize artificial intelligence (AI) and machine learning (ML), which are destined to revolutionize network administration and optimization. These technologies will make it

possible for networks to be not only quicker, but also smarter and more adaptable to the ever-changing requirements of users. In addition, developments in nanotechnology and novel materials are making it possible to create devices that are more compact, more efficient, and capable of supporting the high-frequency operations of 6G networks.

4.3.2 Applications and the Influence of Sixth Generation Wireless

A new era of digital interaction and connectivity is about to start off, and the applications of 6G technology go far beyond the enhancement of internet speeds. The adoption of autonomous cars and drones will be significantly aided by the implementation of 6G in the sphere of URLLC. This will make it possible for these vehicles and drones to communicate with one another and their surroundings with a minimal amount of delay, hence ensuring unprecedented levels of safety and efficiency. The widespread use of Internet of Things devices, which will be powered by 6G, will further enable smart cities to manage resources and services in real time, which will significantly improve the quality of life in urban areas. Furthermore, the immersive experiences given by next-generation virtual reality and augmented reality, which are made feasible by the ultra-low latency of 6G, have the potential to reimagine the entertainment industry, as well as education and professional training.

4.3.3 The Obstacles and Future Directions of Research

The road to 6G is plagued with technological and regulatory obstacles, despite the fact that it has a tremendous amount of potential. The shortage of spectrum presents a considerable obstacle, which calls for the development of novel technologies in order to liberate the enormous bandwidth that is necessary for THz communications. In addition, the energy requirements of these high-frequency networks bring to light the necessity of making significant advancements in energy efficiency practices. Multidisciplinary teams are working diligently to develop solutions that are sustainable and scalable, with the goal of paving the way for the worldwide rollout of 6G networks. The development of these solutions is the focus of continuing international research that is being conducted to address these difficulties.

4.3.4 Concluding Remarks and Prospects for the 6G technology

The introduction of 6G technology offers the potential to bring about a digital future that is defined by seamless connectivity, intelligent networks, and application possibilities

that have never been seen before. Despite the fact that the path leading to this future is difficult and there are numerous obstacles to overcome, the coordinated efforts of the scientific community all over the world are gradually making the vision of 6G into a reality. As research continues to advance and new discoveries are made, the anticipation of a society that is enabled with 6G technology rises. This promises a future in which the full potential of digital technology may be unleashed, bringing us closer to a world in which everything and everyone is connected in ways that we can only begin to conceive.

Conclusion

As we continue to witness progress in 5G technology, it is clear that the journey towards 6G is an extensive one. With each new generation of wireless communication, we experience substantial enhancements compared to the previous iteration. However, the advent of 6G signifies more than just an evolution; it represents a complete paradigm shift, where autonomous networks take center stage. This groundbreaking technology will propel us towards a future defined by sustainability and unwavering dependability.

The future and beyond demand connectivity, and 6G networks are poised to fulfill this need. Serving as the backbone of communication infrastructure in our interconnected society, these networks have a vital role to play. To achieve their objective, the advancement of state-of-the-art technologies is crucial. These include intelligent surfaces, energy-efficient Internet of Things (IoT) devices, cutting-edge artificial intelligence (AI) methods, potential quantum computing frameworks, automated devices driven by AI, air interfaces powered by AI, humanoid robots, self-sustaining networks, and the ever-evolving dynamics of digital communities.

Get ready for the upcoming era known as 6G, a time of incredible advancements and endless possibilities. This next phase of connectivity will revolutionize the way we live with groundbreaking innovations such as UAV-based mobility, Connected Autonomous Vehicles (CAV), Smart Grid 2.0, Collaborative Robots, Hyperintelligent Healthcare, Industry 5.0, Digital Twin, and Extended Reality. However, with these remarkable developments come unique challenges and specific requirements. These include the wide availability of small data, an aging population, the merging of communication, sensing, and computing, and the introduction of communication without the need for devices. Ultimately, 6G will not only push the limits of connectivity but also establish the groundwork for transformative applications that will shape the future of various industries and sectors.

In the realm of 6G technology, there are four distinct areas that have been acknowledged as having significant ramifications for security and privacy. One of these areas is blockchain and distributed ledger technology (DLT), which has the potential to establish a secure and accountable network through surveillance and governance mechanisms. By ensuring that every occurrence is documented in a transparent and unchangeable manner, DLT fosters a sense of confidence among unfamiliar participants in the system.

However, the integration of DLTs may pose certain challenges in terms of protecting user and data privacy, as well as introducing additional computational and storage burdens to achieve the desired level of trust.

In the process of developing advanced networks, it is crucial to consider the incorporation of quantum security algorithms and their influence on network protocols and associated security measures. This involves the integration of post-quantum cryptography and quantum key distribution, which must be taken into account to ensure the network's resilience against possible quantum threats.

It is imperative to recognize the immense importance of artificial intelligence and machine learning (AI/ML) in the field of security. These cutting-edge technologies possess the capability to enhance security measures while simultaneously revealing vulnerabilities within the fundamental infrastructure of 6G networks. Therefore, striking a balanced and symbiotic relationship between leveraging AI/ML to fortify security and mitigating the risks presented by potential threats becomes paramount.

The impending arrival of 6G wireless technology is poised to unlock a realm of groundbreaking advancements in the realm of artificial intelligence and machine learning. This groundbreaking technology will bring these state-of-the-art capabilities closer to the source of data, resulting in minimal delays and an overall enhancement in performance. By dispersing machine learning functions throughout the network, models will be refined, facilitating seamless collaboration in decision-making processes. Nevertheless, there will be obstacles to overcome in ensuring the security of AI, particularly given the practical constraints of certain network components like IoT devices. To surmount this challenge, protective mechanisms known as PLS mechanisms will be devised. These mechanisms will leverage the distinctive attributes of wireless channels to establish secure communication, encompassing a wide array of security operations such as authentication, encryption, and key exchange.

When examining the development of 6G applications, it becomes crucial to take into account the different entities involved and their specific network needs, especially when it comes to ensuring security. The current security frameworks created for pre-6G technologies are inadequate for addressing the heightened security requirements of these innovative applications. Moreover, the introduction of these applications might bring about a completely new range of security weaknesses. Therefore, it is absolutely

essential for 6G networks to confront the security obstacles presented by these groundbreaking 6G applications.

References

Abd El-Latif, A. A., Abd-El-Atty, B., Abou-Bassar, E. M. & Venegas-Andraca, S. E., 2020. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Optics & Laser Technology*, Volume 124.

AI HLEG, 2019. *Ethics guidelines for trustworthy ai.*
Available at: ttps://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Andrea, I., Chrysostomou, C. & Hadjichristofi, G., 2016. *Internet of Things: Security Vulnerabilities and Challenges,* IEEE.

Arfaoui, M. A. et al., 2020. Physical layer security for visible light communication systems: A survey. *IEEE Communications Surveys Tutorials*, 22(3), pp. 1887-1908.

Atzei, N., Bartoletti, M. & Cimoli, T., 2017. A Survey of Attacks on Ethereum Smart Contracts (sok). In: *International Conference on Principles of Security and Trust.* Springer, pp. 164-186.

Barreno, M. et al., 2006. *Can machine learning be secure?* ACM.

Benzaid, C. & Taleb, T., 2020. ZSM security: Threat surface and best practices. *IEEE Network*, 34(3), pp. 124-133.

Bernstein, D. J. & Lange, T., 2017. Post-quantum cryptography. *Nature*, pp. 188-194.

Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E., 2017. High-dimensional quantum cloning and applications to quantum hacking. *Science advances*.

Bunz, B., Agrawal, S., Zamani, M. & Boneh, D., 2020. Zether: Towards privacy in a smart contract world. In: *International Conference on Financial Cryptography and Data Security* Springer, pp. 423-443.

C. Insights, 2019. *40+ corporations working on autonomous vehicles.*

Cai, Y. & Zhu, D., 2016. Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, 2(1), p. 20.

Charalambous, M., Farao, A., Kalantzantonakis, G., Kanakakis, P., Salamanos, N., Kotsifakos, E., & Froudakis, E. (2022, August). *Analyzing coverages of cyber insurance policies using ontology*. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-7).

Chen, J. & Shu, T., 2020. Statistical modeling and analysis on the confidentiality of indoor VLC systems. *IEEE Transactions on Wireless Communications*, 19(7), pp. 4744-4757.

Cui, M., Zhang, G. & Zhang, R., 2019. Secure wireless communication via intelligent reflecting surface. *IEEE Wireless Communications Letters*, 8(5), pp. 1410-1414.

Deebak, B. & Al-Turjman, F., 2020. Drone of IoT in 6G wireless communications: Technology, challenges, and future aspects. In: *Unmanned Aerial Vehicles in Smart Cities.* Springer, pp. 153-165.

Dey, S., 2018. *Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work.* IEEE.

Dharminder, D. & Mishra, D., 2020. Lcppa: Lattice-based conditional privacy preserving authentication in vehicular communication. *Transactions on Emerging Telecommunications Technologies*, 31(2).

Diaz, M., Wang, H., Calmon, F. P. & Sankar, L., 2020. On the robustness of information-theoretic privacy measures and mechanisms. *IEEE Transactions on Information Theory*, 66(4), pp. 1949-1978.

Dressler, F. & Kargl, F., 2012. Towards security in nano-communication: Challenges and opportunities. *Nano Communication Networks*, 3(3), pp. 151-160.

Du, Y. et al., 2020. *Quantum noise protects quantum classifiers against adversaries.*

Dwork, C. & Roth, A., 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4), pp. 211-407.

Efanov, D. & Roschin, P., 2018. The all-pervasiveness of the blockchain technology. *Procedia Computer Science*, Volume 123, pp. 116-121.

ENISA, 2020. *Artificial intelligence cybersecurity challenges.* ENISA.

Farao, A., Ntantogian, C., Istrate, C., Suciu, G., & Xenakis, C. (2019, September). SealedGRID: *Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID. In 6th International Symposium for ICS & SCADA Cyber Security Research* 2019. BCS Learning & Development.

Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., ... & Xenakis, C. (2020). SECONDO: *A platform for cybersecurity investments and cyber insurance decisions. In Trust, Privacy and Security in Digital Business*: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17 (pp. 65-74). Springer International Publishing.

Farao, A., Rubio, J. E., Alcaraz, C., Ntantogian, C., Xenakis, C., & Lopez, J. (2020). Sealedgrid: *A secure interconnection of technologies for smart grid applications. In Critical Information Infrastructures Security*: 14th International Conference, CRITIS 2019, Linköping, Sweden, September 23–25, 2019, Revised Selected Papers 14 (pp. 169-175). Springer International Publishing.

Farao, A., Veroni, E., Ntantogian, C., & Xenakis, C. (2021). P4G2Go: *a privacy-preserving scheme for roaming energy consumers of the smart grid-to-go*. Sensors, 21(8), 2686.

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2024). INCHAIN: *a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain*. International Journal of Information Security, 23(1), 347-371.

G. ETSI, 2020. *004, Zero-touch network and service management (ZSM).* Reference Architecture.

Grieves, M. & Vickers, J., 2017. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In: *Transdisciplinary perspectives on complex systems.* Springer, pp. 85-113.

Grieves, M. W., 2019. *Virtually intelligent product systems: digital and physical twins.*

Gui, G. et al., 2020. 6G: Opening new horizons for integration of comfort, security and intelligence. *IEEE Wireless Communications*.

He, J., Yang, K. & Chen, H. H., 2020. 6G cellular networks and connected autonomous vehicles. *IEEE Network*, pp. 1-7.

Hewa, T. et al., 2020. *The role of blockchain in 6G: Challenges, opportunities and research directions.* IEEE.

Hewa, T. M. et al., 2021. Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research. *IEEE Access*, p. 1.

Hewa, T., Ylianttila, M. & Liyanage, M., 2020. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*.

Isravel, D. P., Silas, S. & Rajsingh, E. B., 2020. SDN-based traffic management for personalized ambient assisted living healthcare system. In: *Intelligence in Big Data Technologies—Beyond the Hype.* Springer, pp. 379-388.

ITU-T Focus Group on ML for Future Networks, 2019. *ITU FG ML5G - Unified architecture for machine learning in 5G and future networks.*
Available at: handle.itu.int/11.1002/pub/8128dfee-en

Jameel, F. et al., 2020. Optimizing blockchain networks with artificial intelligence: Towards efficient and reliable iot applications. In: *Convergence of Artificial Intelligence and the Internet of Things.* Springer, pp. 299-321.

Jere, M. S., Harnan, T. & Koushanfar, F., 2020. A taxonomy of attacks on federated learning. *IEEE Security & Privacy*.

Kalaiprasath, R., Elankavi, R. & Udayakumar, R., 2017. Cloud security and compliance-a semantic approach in end to end security. *International Journal on Smart Sensing & Intelligent Systems*, Volume 10.

Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022, August). GTM: *Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. In Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-9).

Karatisoglou, M., Farao, A., Bolgouras, V., & Xenakis, C. (2022, June). BRIDGE: *BRIDGing the gap bEtween CTI production and consumption*. In 2022 14th International Conference on Communications (COMM) (pp. 1-6). IEEE.

Khan, R., Kumar, P., Jayakody, D. N. K. & Liyanage, M., 2019. A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, 22(1), pp. 196-248.

Khurana, N., Mittal, S., Piplai, A. & Joshi, A., 2019. *Preventing poisoning attacks on ai based threat intelligence systems.* IEEE.

Kurakin, A. et al., 2018. *Ensemble adversarial training: Attacks and defenses.* Available at: https://openreview.net/pdf?id=rkZvSe-RZ

Latva-Aho, M. & Leppanen, K., 2019. *Key drivers and research challenges for 6G ubiquitous wireless intelligence.* Oulu, Finland: 6G Flagship.

Lebeck, K., Ruth, K., Kohno, T. & Roesner, F., 2018. *Towards security and privacy for multi-user augmented reality: Foundations with end users.* IEEE.

Letaief, K. B. et al., 2019. The roadmap to 6G: Ai empowered wireless networks. *IEEE Communications Magazine*, 57(8), pp. 84-90.

Li, S. et al., 2021. Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things. *IEEE Internet of Things Journal*.

Li, W. et al., 2020. Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Network*, 34(6), pp. 31-37.

Li, X. et al., 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems*, Volume 107, pp. 841-853.

Liyanage, M. et al., 2018. *A comprehensive guide to 5G security,* Wiley Online Library.

Li, Z. et al., 2018. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(8), pp. 3690-3700.

Lohachab, A. & Jangra, A., 2020. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum iot networks. *Internet of Things*, Volume 9.

Ma, J. et al., 2018. Security and eavesdropping in terahertz wireless links. *Nature*, 563(8), pp. 89-93.

Mehar, M. I. et al., 2019. Understanding a revolutionary and flawed grand experiment in blockchain: The dao attack. *Journal of Cases on Information Technology (JCIT)*, 21(1), pp. 19-32.

Miglani, A., Kumar, N., Chamola, V. & Zeadally, S., 2020. Blockchain for Internet of Energy Management: Review, Solutions, and Challenges. *Computer Communications*, Volume 151, pp. 395-418.

Montville, A. W. & Munyan, B., 2021. *Security Automation and Continuous Monitoring (SACM) Architecture.*
Available at: https://datatracker.ietf.org/doc/html/draft-ietf-sacm-arch-08

Mucchi, L. et al., 2020. *How 6G technology can change the future wireless healthcare.* IEEE.

Mucchi, L. et al., 2019. Secrecy capacity and secure distance for diffusion-based molecular communication systems. *IEEE Access*, Volume 7, pp. 687-697.

Mukherjee, M. et al., 2020. Intelligent edge computing: Security and privacy challenges. *IEEE Communications Magazine*, 58(9), pp. 26-31.

Muñoz, A., Farao, A., Correia, J. R. C., & Xenakis, C. (2021). P2ISE: *preserving project integrity in CI/CD based on secure elements*. Information, 12(9), 357.

Muñoz, A., Farao, A., Correia, J. R. C., & Xenakis, C. (2020). ICITPM: *integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM)*. In Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25 (pp. 147-165). Springer International Publishing.

Nahavandi, S., 2019. Industry 5.0 - a human-centric solution. *Sustainability*, 11(16), p. 4371.

Nakano, T. et al., 2019. Methods and applications of mobile molecular communication. *Proceedings of the IEEE*, 107(7), pp. 1442-1456.

Nayak, S. & Patgiri, R., 2020. *6G communication technology: A vision on intelligent healthcare*.

Nguyen, T. et al., 2020. *Privacy-aware blockchain innovation for 6g: Challenges and opportunities.* IEEE.

NIST, 2020. *NIST Post-Quantum Cryptography Standardization.*
Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

O'Malley, J., 2019. The no drone zone. *Engineering & Technology*, 14(2), pp. 34-38.

Ortiz, J. et al., 2020. *Isnpire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks.* 15th International Conference on Availability, Reliability and Security.

Petrov, I. & Janevski, T., 2020. 5G mobile technologies and early 6G viewpoints. *European Journal of Engineering Research and Science*, 5(10), pp. 1240-1246.

Petrov, V., Moltchanov, D., Jornet, J. M. & Koucheryavy, Y., 2019. *Exploiting multipath terahertz communications for physical layer security in beyond 5g networks.* IEEE.

Plastiras, G., Terzi, M., Kyrkou, C. & Theocharides, T., 2018. *Edge intelligence: Challenges and opportunities of near-sensor machine learning applications.* IEEE.

Porambage, P. et al., 2021. *6G Security Challenges and Potential Solutions.* 2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit.

Porambage, P., Osorio, D. P. M., Gur, G. & Liyanage, M., 2021. *The Roadmap to 6G Security and Privacy.* IEEE.

Qu, Y. et al., 2020. Decentralized privacy using blockchain-enabled federated learning in fog comppiting. *IEEE Internet of Things Journal*, 7(6), pp. 5171-5183.

Rahman, M. M. U. et al., 2017. Physical layer authentication in nano networks at terahertz frequencies for biomedical applications. *IEEE Access*, Volume 5, pp. 7808-7815.

Ranaweera, P., Jurcut, A. D. & Liyanage, M., 2021. Survey on multi-access edge computing security and privacy. *IEEE Communications Surveys & Tutorials*.

Roetteler, M., Naehrig, M., Svore, K. M. & Lauter, K., 2017. Quantum resource estimates for computing elliptic curve discrete logarithms. In: *International Conference on the Theory and Application of Cryptology and Information Security.* Springer, pp. 241-270.

Saad, W., Bennis, M. & Chen, M., 2019. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE network*, 34(3), pp. 134-142.

Saito, T., Xagawa, K. & Yamakawa, T., 2018. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques.* Springer, pp. 520-551.

Saud, M. S., Chowdhury, H. & Katz, M., 2017. *Heterogeneous software-defined networks: Implementation of a hybrid radio-optical wireless network.* IEEE.

Schaar, P., 2010. Privacy by design. *Identity in the Information Society*, 3(2), pp. 267-274.

Schneier, B., 2018. Artificial intelligence and the attack/defense balance. *IEEE security & privacy*, 16(2), p. 96.

Sengupta, S., Chakraborti, T. & Kambhampati, S., 2019. Mtdeep: boosting the security of deep neural nets against adversarial attacks with moving target defense. In: *International Conference on Decision and Game Theory for Security.* Springer, pp. 479-491.

Shahinzadeh, H. et al., 2019. *Internet of Energy (IoE) in smart power systems.* IEEE.

Siriwardhana, Y., Porambage, P., Liyanage, M. & Ylinattila, M., 2021. A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications and Technical Aspects. *IEEE Communications Surveys Tutorials*, p. 1.

Soderi, S., 2020. *Enhancing security in 6g visible light communications.* 6G SUMMIT.

Soll, M., Hinz, T., Magg, S. & Wermter, S., 2019. Evaluating defensive distillation for defending text processing neural networks against adversarial examples. In: I. V. Tetko, V. Kurkova, P. Karpov & F. Theis, eds. *Artificial Neural Networks and Machine Learning – ICANN 2019: Image Processing.* Cham: Springer International Publishing, pp. 685-696.

Suciu, G., Farao, A., Bernardinetti, G., Palamà, I., Sachian, M. A., Vulpe, A., ... & Xenakis, C. (2022). SAMGRID: *security authorization and monitoring module based on SealedGRID platform*. Sensors, 22(17), 6527.

Sun, Y. et al., 2020. When machine learning meets privacy in 6G: A survey. *IEEE Communications Surveys & Tutorials*, 22(4), pp. 2694-2724.

Tarantino, S., Da Lio, B., Cozzolino, D. & Bacco, D., 2020. Feasibility of quantum communications in aquatic scenarios, Optik.

Tariq, F. et al., 2020. A speculative study on 6G. *IEEE Wireless Communications*, 27(4), pp. 118-125.

TSG SA, 2020. *3GPP SA3 - Security.*
Available at: https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

Viswanathan, H. & Mogensen, P. E., 2020. Communications in the 6G era. *IEEE Access*, Volume 8, pp. 63-74.

Wang, M. et al., 2020. Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks*, 6(3), pp. 281-291.

Weerasinghe, N. et al., 2021. A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators. *IEEE Open Journal of the Communications Society*, Volume 2, pp. 575-601.

Wijethilaka, S. & Liyanage, M., 2021. Survey on network slicing for internet of things realization in 5g networks. *IEEE Communications Surveys & Tutorials*.

Xiao, H. et al., 2015. *Is feature selection secure against training data poisoning?*. ICML.

Xu, S., Qian, Y. & Hu, R. Q., 2020. Edge intelligence assisted gateway defense in cyber security. *IEEE Network*, 34(4), pp. 14-19.

Xu, X., 2012. From cloud computing to cloud manufacturing. *Robotics and computer-integrated manufacturing*, 28(1), pp. 75-86.

Yao, M., Sohul, M., Marojevic, V. & Reed, J. H., 2019. Artificial intelligence defined 5g radio access networks. *IEEE Communications Magazine*, 57(3), pp. 14-20.

Yasmin, R., Petajajarvi, J., Mikhaylov, K. & Pouttu, A., 2017. *On the integration of lorawan with the 5g test network.* IEEE.

Ylianttila, M. et al., 2020. *6G white paper: Research challenges for trust, security and privacy.* :arXiv preprint arXiv:2004.11665.

You, X. et al., 2021. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. *Science China Information Sciences*, 64(1), pp. 1-74.

Zhang, S. & Zhu, D., 2020. Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. *Computer Networks*, Volume 183, p. 107556.

Zhang, Y. et al., 2020. *SMARTSHIELD: Automatic smart contract protection made easy.* IEEE.

Zhang, Z. et al., 2019. 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Vehicular Technology Magazine*, 14(3), pp. 28-41.

Ziegler, V. et al., 2020. 6G architecture to connect the worlds. *IEEE Access*, Volume 8, pp. 508-520.

Ziegler, V. & Yrjola, S., 2020. *6g indicators of value and performance.* IEEE.