

Quantum-Encrypted 6G Fronthaul Network: Enhancing Security and Efficiency in Next-Generation Wireless Communication

Mengxu Zheng^{1,a}, Yubo Xuan^{1,b,*}

¹*College of Communication Engineering, Jilin University, Room 5372, South Lake Road, Chaoyang District, Changchun City, Jilin, China*

a. 15643117341@163.com, b. xuanyb@jlu.edu.cn

**corresponding author*

Abstract: The transition from 5G to 6G networks introduces significant advancements in speed, latency, and connectivity, but also raises critical security concerns. The increasing number of devices that need to be plugged into the network makes the demand for enhanced security and efficiency paramount. This paper proposes a novel Quantum-Encrypted 6G Fronthaul Network Architecture, integrating quantum communication with passive wavelength division multiplexing technology to address the security challenges in next-generation networks. The architecture ensures theoretically unbreakable encryption by utilizing quantum key distribution techniques on top of the current passive WDM fronthaul network architecture. It reduces the difficulty and cost of network upgrades while maintaining high bandwidth utilization and scalability. By deploying quantum communication devices in Active Antenna Units and Distributed Units, the proposed system enhances the security of the fronthaul link, protecting against eavesdropping and cyber attacks. The results obtained through simulation demonstrate that the system is highly resistant to dark counts, detection efficiency, and photon pulse variations, ensuring reliable key distribution over long distances. This architecture not only provides a cost-effective upgrade path for existing 5G networks but also paves the way for secure, high-capacity communication in future 6G applications, such as autonomous systems, smart cities, and critical infrastructure.

Keywords: 6G, security, Quantum Key Distribution, network architecture.

1. Introduction

As the fifth generation of mobile networks, 5G offers groundbreaking advancements in terms of speed, capacity, and connectivity. Unlike its predecessors, 5G enables ultra-fast data transmission rates, with theoretical speeds reaching up to 100 Gbps, approximately 100 times faster than 4G. This leap in speed supports a vast range of applications, from high-definition video streaming and augmented reality (AR) to Internet of Things (IoT) devices and autonomous vehicles. [1] The expanded bandwidth of 5G also facilitates ultra-reliable low-latency communication (URLLC), which is essential for applications such as remote surgery, autonomous driving, and industrial automation. [2] Furthermore, 5G introduces the concept of network slicing, allowing the creation of virtual networks tailored to specific use cases, which enhances efficiency and user experience.

However, there are still many shortcomings in 5G, such as the need for improvement in transmission rates and the higher latency requirements of an increasing number of devices. At the same time, the demand for more smart devices and the growing need for the Internet of Everything pose significant challenges to the carrying capacity of 5G networks and the security of user data. These issues must still be addressed in the development of 6G networks. [3] 6G is poised to take mobile networks to the next level, surpassing the capabilities of 5G in several key aspects. While 5G has already begun to revolutionize connectivity, 6G will build on this foundation by offering even faster data transmission, lower latency, and higher reliability. 6G aims to provide data speeds exceeding 1 Tbps, which will support an even wider range of applications, from immersive holographic communication to real-time AI-driven systems. This exponential increase in bandwidth will allow for the seamless integration of advanced technologies like artificial intelligence (AI), machine learning (ML), and quantum computing into everyday life. [4]

The most significant difference between 5G and 6G lies in their approaches to connectivity. While 5G primarily focuses on enhancing mobile broadband and low-latency communication, 6G will incorporate a more intelligent, autonomous, and adaptive network framework. 6G networks will integrate advanced AI and machine learning techniques to dynamically optimize network management, reduce congestion, and improve overall efficiency. With enhanced capabilities in data transfer, AI integration, and automation, 6G will enable new applications that extend beyond current technological limitations. [5]

6G will support not only a much larger volume of devices but also a wider variety of use cases, including autonomous systems, smart cities, and critical infrastructure. This increases the attack surface for malicious actors and the potential impact of security breaches. Therefore, securing 6G networks will require a more robust, multi-layered approach to protect against a range of threats, from cyber attacks to privacy violations. Given the complexity of 6G systems, which will involve a diverse set of technologies like AI, quantum computing, and edge computing, traditional security models may no longer be sufficient. Advanced encryption methods, such as AI-driven threat detection and response systems, will be required. These systems will continuously monitor network traffic and user behavior, using machine learning to detect and mitigate potential threats in real-time. Additionally, with the increased use of edge computing in 6G, security measures will need to be deployed not only at central data centers but also at the edge of the network, where data is processed closer to the source. This decentralized approach will provide more localized security, but it will also require new strategies for managing and securing edge devices and nodes. [6] Moreover, network slicing in 6G introduces new challenges for security, as each virtual network may have different security policies and requirements. There is a need to ensure that each slice remains isolated and protected. [7]

Another critical aspect of 6G security will be the integration of quantum-safe cryptography, which will be essential to safeguarding data against future quantum-based attacks. Quantum communication is a technology that utilizes the principles of quantum mechanics to achieve information transfer. Its core idea is to use quantum bits instead of traditional bits in classical communication, which can better protect the security and privacy of the communication content. One of the most famous applications of quantum communication is Quantum Key Distribution (QKD), which uses quantum mechanics principles to generate and distribute encryption keys, ensuring that encrypted information cannot be deciphered, even if a third party tries to eavesdrop or interfere with the communication. The greatest advantage of quantum communication is its inherent security. Through the basic principles of quantum mechanics, once someone tries to eavesdrop, both sides of the communication can immediately detect it. In contrast to traditional methods of communication, the security of quantum communication does not rely on mathematical algorithms but on the laws of physics. Traditional encryption techniques rely on computational difficulty to ensure cryptographic security, but as computing power increases, these encryption methods can be broken. The security of quantum

key distribution, on the other hand, is based on the no-cloning theorem of quantum mechanics, which allows any eavesdropping during the transmission of information to be detected in real time. In addition, in theory, quantum communication can enable encrypted communication over ultra-long distances. With the development of quantum computing technology, the quantum Internet will provide a more secure and efficient guarantee for global information communication. Overall, securing 6G will require a shift toward intelligent, adaptive, and resilient security frameworks capable of addressing the unique challenges of future networks.

2. Related Works

With the emergence of new communication technologies and application requirements, there has also been an increase in security risks within the network. The need for network security is growing. According to recent research, 6G networks are expected to offer terabit-level transmission rates, sub-millisecond latency, centimeter-level positioning accuracy, and provide connectivity for trillions of devices. With a thousand-fold increase in network capacity and further reductions in energy consumption, 6G will pave the way for a universally interconnected and intelligent network, aiming to create a society where everything is intelligently interconnected through the integration of digital twins and the Internet of Everything. [8] Research has highlighted the emergence of new threats, such as those targeting the novel technologies of 6G, including terahertz communication and Reflective Intelligent Surfaces (RIS). The integration of these technologies introduces additional layers of complexity in securing the network. One key area of focus is Physical Layer Security (PLS), which plays a critical role in protecting the network. PLS relies on intelligent adjustments to signal amplitude and phase to enhance security, making it a vital component of 6G networks. Furthermore, the integration of terrestrial, airborne, satellite, and maritime networks in 6G systems has been identified as a major challenge, leading to more complex and multifaceted security concerns. [9]

Recent research has explored several promising approaches to safeguard 6G networks through security solutions and technologies. Artificial Intelligence (AI) and Machine Learning (ML) are recognized as key enablers for enhancing the security of these networks, particularly in intelligent threat detection and response. [10] Quantum Secure Communications have been identified as essential technologies for countering attacks from quantum computers, with Quantum Key Distribution (QKD) and post-quantum cryptography offering the necessary protection. Additionally, blockchain and distributed ledger technologies are being explored to enhance trustworthiness and data integrity in 6G systems. Another important security enhancement is Physical Layer Security, which can be strengthened using techniques such as Reflective Intelligent Surfaces (RIS) to improve wireless propagation environments and ensure signal confidentiality. [11] Future research directions in 6G network security are diverse and evolving. One significant area of focus is AI-enabled privacy protection, particularly in large-scale data collection and processing scenarios. [12] Research is also investigating the integration of sensing and communication systems to enhance security through technologies like RIS. Furthermore, quantum communication technologies, including QKD and quantum security protocols, are being actively explored for their potential application in next-generation 6G networks. These areas of research are crucial to the development of secure, reliable, and efficient 6G systems that will meet the evolving demands of future connectivity.

3. Quantum-Encrypted 6G Fronthaul Network Architecture

Currently, conventional communication networks are not capable of addressing communication security challenges, especially in areas with high security requirements, such as finance, government, and military. To address these challenges, we propose a new network architecture called “Quantum-encrypted 6G fronthaul network architecture,” which combines passive wavelength division

multiplexing (WDM) technology with quantum communication. This combination not only improves the bandwidth utilization but also significantly enhances the network's security. The quantum communication devices are deployed separately in the Active Antenna Unit (AAU) and the Distributed Unit (DU), ensuring that the link between the AAU site and the DU site is protected by the information security provided by quantum communication. Quantum key distribution devices are deployed in each AAU, enabling independent quantum key distribution. The Distributed Unit, as the receiving end, deploys a single quantum communication device to receive quantum keys from different Active Antenna Units, enabling the two ends of the fronthaul network to quickly generate key sequences.

The user's information is initially sent to the AAU site as a wireless signal. The AAU site acts as the sender, distributing the quantum key to the DU site. Photons with different polarization states travel to the DU site via fibre-optic cable, allowing the DU site to quickly establish the quantum key from the information carried by the optical signals. In this system, the AAU and the transmitter (referred to as "Alice") together act as the 'transmitter' of the signal chain, responsible for sending both classical and quantum signals to the transmission medium. The AAU integrates a quantum signal transmission module, enabling the joint transmission of classical and quantum signals. The DU and Bob serve as the receivers in the signal chain, responsible for processing the received signals. The DU integrates a quantum signal receiving module, which captures the quantum signals and passes them to Bob for decoding quantum states and extracting the key.

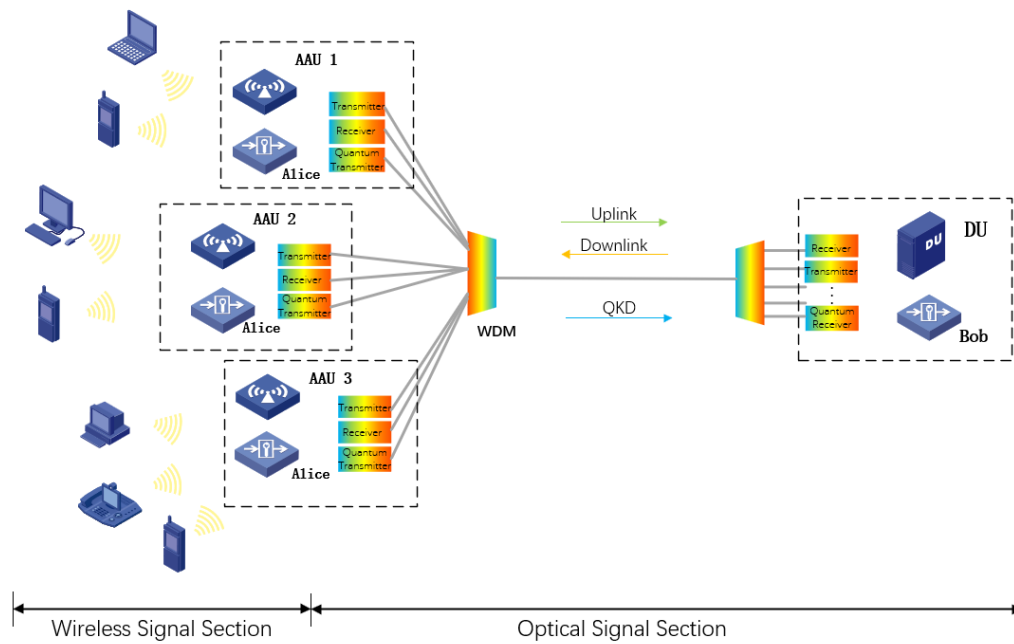


Figure 1: Quantum-Encrypted 6G Fronthaul Network Architecture

The green and yellow arrows in the Figure 1 represent the uplink and downlink of classical signals, respectively. Classical signals are transmitted in both directions in the signal chain, meaning that the sender and receiver can communicate with each other. The blue arrows in the Figure 1 represent the direction of communication for quantum signals. Quantum signals differ from classical signals in that they are transmitted in one direction in this system. AAU assigns independent wavelengths to quantum signals to achieve isolation from classical signals. The quantum signal is sent from Alice to Bob, and the process cannot be reversed.

Constructing the network in this way can significantly reduce the cost of network upgrades. The adoption of uplinks allows the fronthaul network to minimize costs while improving security, without adding too many unnecessary quantum communication devices. This cost-effectiveness gives this combination great potential for practical applications. The main front-end network architecture used in current 5G networks is passive WDM, and quantum communication is compatible with existing passive WDM architectures without the need for large-scale modifications to existing infrastructure. This means that quantum communication technology can be introduced gradually without disrupting existing services, resulting in a smooth transition to a more secure network environment. This compatibility greatly reduces the difficulty of network upgrades and the impact on users, increasing the feasibility of practical deployment. In addition, quantum key distribution provides theoretically unbreakable security. Combining quantum communication with passive WDM can achieve highly secure data transmission in existing optical fiber networks, especially for areas with very high security requirements. Additionally, this architecture has high bandwidth utilization and better scalability. Passive WDM technology supports multi-wavelength transmission, which can easily expand the capacity and coverage of quantum communications. As communication demand increases, quantum communication can expand the network capacity by increasing the number of wavelengths, and one or more of them can be used for data transmission, thus making full use of the bandwidth resources of optical fiber without affecting existing communication. This scalability allows the Quantum-Encrypted 6G Fronthaul Network Architecture to cope with a wider range of more complex communication scenarios.

4. Performance analysis of QKD system

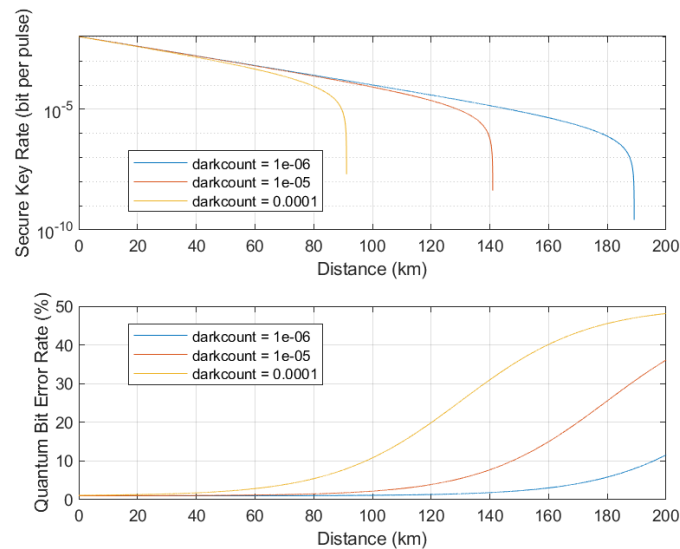


Figure 2: Effects of Dark Counting on the System

The dark count is one of the main sources of background noise in the detector. From the simulation results in Figure 2, it can be observed that the secure key rate is highest when the dark count is $1e-6$. Additionally, the signal propagates up to 180 km, where a high secure key rate still exists, and the system performance approaches the ideal case for normal key distribution. However, as the number of dark counts increases, the background noise grows, causing the useful signal to be overwhelmed. This not only reduces the percentage of the useful signal but also increases the complexity of the error correction and privacy amplification processes, which in turn reduces the key rate. When the dark

count reaches $1e-5$, the signal propagates to approximately 140 km, where the key rate has decayed to nearly zero.

The dark count is a random event, independent of the signal sent by Alice. When Bob receives a dark count, he mistakenly interprets it as a valid signal, introducing a false code. The higher the dark count rate, the more spurious events occur, leading to an increase in the quantum bit error rate (QBER). At lower dark counts ($1e-6$), there are fewer spurious events, and the QBER is mainly influenced by channel noise and eavesdropping behavior. However, at higher dark counts (0.0001), the QBER increases significantly. The bit error rate (BER) exceeds 10 percent at 100 km, which does not meet the system's requirements.

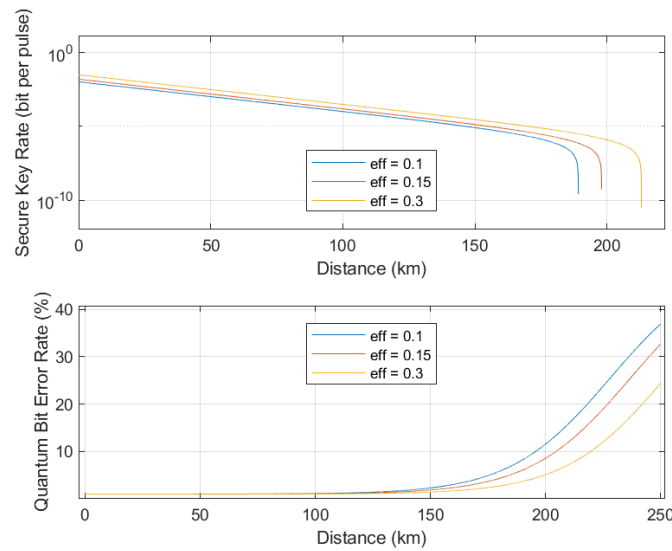


Figure 3: Effect of Detection Efficiency on the System

Figure 3 illustrates the effect of detection efficiency on the secure key rate and quantum bit error rate (QBER). Detection efficiency directly impacts the signal state gain, which is the ratio of the signal detected by Bob to the signal sent by Alice. The higher the detection efficiency, the greater the probability that Bob successfully detects the photons sent by Alice, increasing the number of valid signals. More valid data can be used for error correction and privacy amplification, thereby increasing the key rate. Additionally, a higher detection efficiency results in a larger percentage of valid signals in the total count and a relatively lower percentage of background noise. Since background noise is a primary source of QBER, improving detection efficiency effectively reduces the QBER. In the experimental simulation, detection efficiencies of 0.1, 0.15, and 0.3 were tested. At 150 km, the differences in secure key rate and QBER for the three detection efficiencies were minimal. However, after 170 km, the difference became more pronounced; the higher the detection efficiency, the higher the key rate and the lower the QBER. At 250 km, the system is no longer safe and reliable.

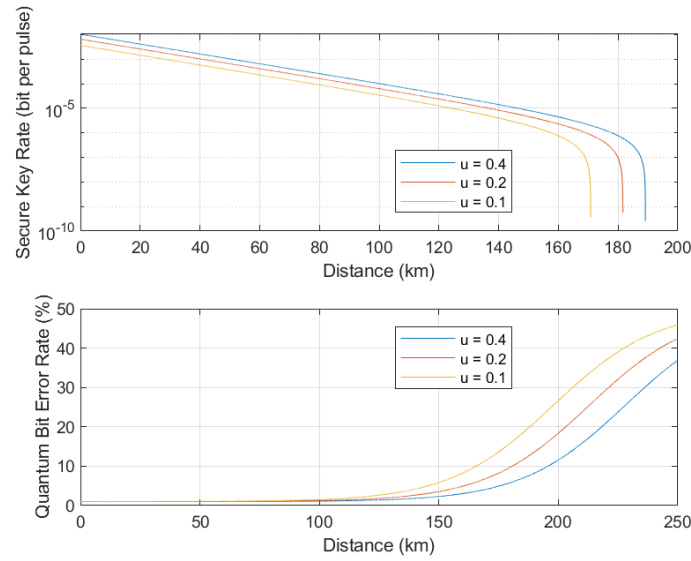


Figure 4: Effect of Number of Photons per Pulse on the System

The average number of photons in each optical pulse sent by Alice influences the signal state gain as significantly as detection efficiency. The higher the number of photons per pulse, the greater the signal state gain. An increased number of photons per pulse also results in a larger proportion of multiphoton pulses, which can be exploited by an attacker to reduce system security, causing an increase in QBER. In Figure 4, the photon per pulse value is chosen within the range of 0.1 to 0.4 to balance the secure key rate and system security. When the number of photons per pulse is 0.1, the secure key rate is low. As the number of photons per pulse increases to 0.2 and finally to 0.4, the secure key rate of the system gradually increases. Beyond 160 km, the difference between the secure key rates for the three parameters becomes more pronounced, and each key rate decreases sharply.

A higher number of photons per pulse also increases the number of valid signals. The number of photons per pulse influences the QBER by affecting the count rate of the signal light and, thus, the percentage of background noise. The percentage of background noise at 0.1 photons per pulse is higher than at 0.2 and 0.4 photons per pulse, leading to a decrease in QBER as the number of photons per pulse increases. When the signal propagates up to 200 km, the QBER exceeds 10% for all three parameters, significantly reducing system reliability.

5. Conclusions

This paper proposes a quantum-encrypted 6G front-end network architecture to address key security challenges in next-generation wireless networks. By combining quantum key distribution with passive wavelength division multiplexing (WDM) technology, the architecture achieves theoretically unbreakable encryption while maintaining high bandwidth utilization and scalability. Deploying quantum communication devices in active antenna units and distributed units ensures secure key distribution in the front-end network, effectively preventing eavesdropping and network attacks. Simulation results show that the system performs stably under various conditions, such as dark count, detection efficiency, and photon pulse rate, while maintaining a high secure key rate over distances of up to 180 km with appropriate parameters. Additionally, the architecture is compatible with existing 5G passive WDM infrastructure, enabling cost-effective upgrades, minimizing deployment complexity, and facilitating a smooth transition to 6G. The practical applications of this technology span several high-security areas: in finance, it protects sensitive transactions from data leakage; in government and military communications, it safeguards classified information from interception; in

smart cities, it secures critical infrastructure such as smart grids and transport systems; in autonomous driving, it ensures that real-time communications from vehicles to the cloud remain untampered with; and in healthcare, it supports ultra-reliable, low-latency, and secure connectivity for remote surgeries and medical data transfers. These applications highlight the architecture's versatility in addressing diverse security needs. Looking ahead, integrating quantum encryption into 6G networks lays the foundation for a quantum Internet that will enable secure global communications. As 6G deployments accelerate, this technology could become a standard security protocol, particularly in areas requiring unparalleled data protection. Future research should focus on standardization and cost reduction to drive commercialization, while exploring synergies with artificial intelligence and blockchain to enhance threat detection and data integrity. Furthermore, extending the architecture's use cases to logistics and manufacturing will unlock its full potential across industries. By combining quantum resilience with the transformative capabilities of 6G, this work paves the way for a secure, smart, and connected future.

References

- [1] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems, " in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.
- [2] Dangi, R.; Lalwani, P.; Choudhary, G.; You, I.; Pau, G. Study and Investigation on 5G Technology: A Systematic Review. *Sensors* 2022, 22, 26. <https://doi.org/10.3390/s22010026>
- [3] C. -X. Wang et al., "On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds, " in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905-974, Second quarter 2023, doi: 10.1109/COMST.2023.3249835.
- [4] A. Dogra, R. K. Jha and S. Jain, "A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies, " in *IEEE Access*, vol. 9, pp. 67512-67547, 2021, doi: 10.1109/ACCESS.2020.3031234.
- [5] W. Tong and G. Y. Li, "Nine Challenges in Artificial Intelligence and Wireless Communications for 6G, " in *IEEE Wireless Communications*, vol. 29, no. 4, pp. 140-145, August 2022, doi: 10.1109/MWC.006.2100543.
- [6] B. Mao, J. Liu, Y. Wu and N. Kato, "Security and Privacy on 6G Network Edge: A Survey, " in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1095-1127, Second quarter 2023, doi: 10.1109/COMST.2023.3244674. keywords: {Security; Privacy; 6G mobile communication; Servers; Edge computing; Artificial intelligence; Image edge detection; Surveys; Security; privacy; edge intelligence; edge computing; edge caching; 6G},
- [7] V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges, " in *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384-2428, Fourth quarter 2021, doi: 10.1109/COMST.2021.3108618.
- [8] Wang, Z., Du, Y., Wei, K. et al. Vision, application scenarios, and key technology trends for 6G mobile communications. *Sci. China Inf. Sci.* 65, 151301 (2022).
- [9] M. Alsabah et al., "6G Wireless Communications Networks: A Comprehensive Survey, " in *IEEE Access*, vol. 9, pp. 148191-148243, 2021, doi: 10.1109/ACCESS.2021.3124812.
- [10] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi and A. Rezaki, "Security and Trust in the 6G Era, " in *IEEE Access*, vol. 9, pp. 142314-142327, 2021, doi: 10.1109/ACCESS.2021.3120143.
- [11] F. Naeem, M. Ali, G. Kaddoum, C. Huang and C. Yuen, "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges, " in *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1196-1217, 2023, doi: 10.1109/OJCOMS.2023.3273507.
- [12] Ahmad, I.; Rodriguez, F.; Huusko, J.; Seppänen, K. On the Dependability of 6G Networks. *Electronics* 2023, 12, 1472. <https://doi.org/10.3390/electronics12061472>