Proceedings of CONF-FMCE 2025 Symposium: Semantic Communication for Media Compression and Transmission
DOI: 10.54254/2755-2721/155/2025.GL23420

Leveraging Quantum Communication for Secure Industrial IoT Networks: A Novel Architecture for 5G Fronthaul Protection

Liyuan Tian

Beijing University of Posts and Telecommunications, Beijing, China
tly050522@qq.com

Abstract: The Industrial Internet of Things (IIoT) is reshaping modern industries by enabling interconnected, intelligent systems that support real-time monitoring, predictive maintenance, and automated control. However, the growing complexity and scale of IIoT networks expose them to increasingly severe cybersecurity threats that traditional methods struggle to address. To meet these challenges, this paper proposes a novel architecture that integrates Quantum Key Distribution (QKD) with passive Wavelength Division Multiplexing (WDM) technology to secure 5G fronthaul communications between Active Antenna Units (AAUs) and Distributed Units (DUs). In this architecture, AAUs and DUs act as quantum communication entities, exchanging secure keys over optical fibers by allocating quantum and classical signals across different wavelengths. This hybrid approach not only enhances bandwidth efficiency but also significantly improves resistance to eavesdropping and tampering, which are critical vulnerabilities in IIoT environments. To evaluate system performance, simulations were conducted by varying key parameters, including attenuation coefficient, detection efficiency, and dark count rate. Simulation results demonstrate that lowering attenuation coefficients and dark count rates substantially improves the secure key generation rate and reduces the quantum bit error rate (QBER), while increased detection efficiency, although beneficial for signal acquisition, introduces trade-offs by potentially raising the QBER under noisy conditions. Figures presented provide clear illustrations of these trends. By merging quantum communication into IIoT frameworks, this study offers a forward-looking, scalable solution that ensures data confidentiality, integrity, and high-speed reliable communication, paving the way for the secure evolution of industrial networks in the era of Industry 4.0.

Keywords: Industrial Internet of Things (IIoT), Quantum Key Distribution (QKD), Quantum Communication, Passive Wavelength Division Multiplexing (WDM), 5G Fronthaul Security

1. Introduction

The rapid advancement of the Internet of Things (IoT) has led to transformative developments across various industries, fostering the emergence of highly interconnected and intelligent systems. The Industrial Internet of Things (IIoT) represents the application of IoT technologies within the industrial sector, often referred to as “Industry 4.0” [1,2]. By facilitating the seamless integration of industrial components, IIoT enhances the flexibility of manufacturing processes, optimizes production efficiency, reduces operational costs, and enables the development of novel service models. These

DOI: 10.54254/2755-2721/155/2025.GL23420

innovations have fundamentally reshaped industrial operations by enabling real-time monitoring, predictive maintenance, and automated decision-making [3,4]. However, despite these advantages, the expansion of IIoT has also introduced substantial security challenges that must be addressed to ensure the reliability, confidentiality, and integrity of industrial networks. Traditional security strategies that have been effective in consumer-grade IoT applications are often inadequate in industrial settings due to the distinct security demands posed by large-scale, interconnected industrial ecosystems. Consequently, developing robust security frameworks tailored to IIoT is essential for mitigating cyber threats and ensuring operational stability [5].

Security in IIoT involves several critical objectives: ensuring the availability of devices and systems, preserving the accuracy and reliability of transmitted data, protecting the confidentiality of information, verifying the identities of devices and users to prevent unauthorized access, and enforcing access control to limit system privileges [6]. However, securing IIoT systems remains a highly complex task due to numerous challenges, such as the prolonged operational lifespans of industrial devices, the large-scale management of connected devices, extensive interconnectivity among system components, the necessity to safeguard critical industrial processes, and persistent concerns over data confidentiality and privacy [3,7]. Furthermore, human-related factors—such as insider threats and inadvertent security breaches—add another layer of difficulty to IIoT security management [6,8].

The architecture of IIoT typically comprises multiple interconnected components, including sensors, controllers, communication networks, and cloud-based platforms, each introducing distinct security vulnerabilities [9]. These vulnerabilities span various layers of the IIoT framework—hardware, software, communication, and data management—creating a broad attack surface that cyber adversaries can exploit. Security threats targeting IIoT systems can be classified according to the layer in which they occur [6].

At the perception layer, security risks include physical attacks such as sensor tampering, unauthorized data extraction, and hardware manipulation. Impersonation threats—such as identity spoofing and Sybil attacks—also compromise system integrity by enabling malicious actors to masquerade as legitimate devices or users [9].

At the network layer, IIoT systems are susceptible to a range of cyberattacks, including man-in-the-middle (MitM) attacks, routing attacks, denial-of-service (DoS) attacks, and black hole attacks (BHA). Among these, BHA poses a particularly severe threat, as it involves a malicious node intercepting and discarding data packets, resulting in major communication disruptions that can destabilize industrial operations. These attacks may lead to significant delays, data loss, and service outages, ultimately reducing the overall efficiency of industrial systems [1,8].

The application layer of IIoT is also vulnerable to various security threats, including malicious code injection and data breaches. Cyber adversaries often exploit software vulnerabilities to introduce malware, such as botnets, which can compromise the functionality of industrial devices and systems. Data breaches represent another significant concern, as unauthorized access to sensitive industrial information can result in financial losses, intellectual property theft, and reputational harm. Given the critical nature of industrial operations, addressing these security challenges is essential to maintaining the resilience and reliability of IIoT infrastructures [5,10].

In response to these security concerns, quantum communication has emerged as a promising solution for strengthening the security of IIoT networks. Quantum communication leverages the principles of quantum mechanics to enable secure information transmission, offering unparalleled protection capabilities [11]. Its key attributes include unconditional security, resistance to eavesdropping, the impossibility of cloning quantum states, advanced encryption techniques, and the elimination of the need for trusted intermediaries. These unique features make quantum

DOI: 10.54254/2755-2721/155/2025.GL23420

communication particularly well-suited to mitigating IIoT security risks by providing strong safeguards against interception, tampering, and unauthorized access [12,13].

As IIoT continues to expand and integrate into critical industrial sectors, ensuring the security of its networks and data becomes increasingly urgent. Conventional security approaches that have proven effective in consumer IoT applications are inadequate for addressing the sophisticated threats and challenges inherent in industrial contexts [1,14]. Quantum communication, with its inherent security features, offers a transformative solution for mitigating these risks, preserving the integrity and confidentiality of industrial data, and protecting IIoT networks from evolving cyber threats [11,12].

This paper explores the intersection of IIoT and quantum communication, with a particular emphasis on the security challenges stemming from the highly interconnected nature of industrial systems. Additionally, it examines the potential of quantum technologies to address these vulnerabilities and strengthen the resilience of IIoT infrastructures. By integrating quantum communication into IIoT security frameworks, industrial systems can achieve enhanced levels of protection—ultimately supporting the development of more secure, efficient, and reliable networks in the era of Industry 4.0.

2. Related works

The reviewed literature highlights significant innovations in the application and security of the Internet of Things (IoT) across various industrial sectors. The paper [15] discusses key technologies such as RFID, Wireless Sensor Networks (WSNs), and cloud computing, emphasizing their diverse applications in logistics, healthcare, and manufacturing. This work provides a comprehensive summary of the current state of IoT, emerging research trends, and the challenges faced in its widespread implementation. In paper [16], a novel solution for long-distance, low-data-rate upstream IoT communication is proposed, utilizing Fiber Bragg Gratings (FBG) and Acousto-Optic Modulators (AOM) to enable secure data transmission over a 30 km range at a rate of 300 bps. This passive optical approach offers superior transmission distance and security compared to traditional wireless technologies like LoRa and Sigfox, making it particularly advantageous in regions with poor wireless signal propagation. Paper [17] examines the benefits of 5G networks in Demand Response (DR) for smart grids. It highlights 5G's low-latency, high-reliability communication capabilities and massive device connectivity, demonstrating how these features can enhance the effectiveness of DR in industrial IoT applications. The paper [18] addresses critical security vulnerabilities in Industrial IoT (IIoT), emphasizing risks such as unauthorized access, data breaches, and denial-of-service attacks. It underscores the importance of integrating secure protocols, encryption, and authentication systems to mitigate these threats and improve the reliability of IIoT networks. Furthermore, the paper discusses the role of emerging technologies, such as Blockchain, in addressing these challenges and fostering greater transparency and trust in IIoT systems. Finally, paper [8] introduces a security framework for networked manufacturing systems (NBMS) in the context of Industry 4.0. By integrating IoT technologies and employing NTRUEncrypt encryption with AODV routing, this framework safeguards against black hole attacks (BHA), ensuring secure communication, protecting sensitive data, and enhancing operational efficiency and customization capabilities within manufacturing ecosystems.

The reviewed studies provide valuable insights into the diverse applications and security considerations of IoT across various industries. From advancements in long-distance, low-data-rate communication technologies and 5G applications in smart grids to the development of unique security frameworks for IIoT and networked manufacturing systems, each paper contributes essential knowledge to the evolution of IoT. These works emphasize the importance of addressing industry-specific challenges, such as ensuring secure communication, managing large-scale networks, and

DOI: 10.54254/2755-2721/155/2025.GL23420

integrating emerging technologies like 5G and optical communication. The proposed frameworks and solutions lay the foundation for more secure, efficient, and scalable IoT deployments, which are critical for unlocking the potential of IoT in industrial applications, particularly within Industry 4.0. Future research should continue to explore these areas, focusing on refining security protocols, enhancing system scalability, and tackling new challenges arising from the rapid growth of IoT in industrial environments.

3. Quantum encryption-based passive wavelength division multiplexing communication architecture

In 5G networks, fronthaul refers to the connection between the DU and the active AAU, as well as the signal transmission between base stations. The efficiency of fronthaul directly impacts the overall performance of the 5G network, especially under the demand for high bandwidth and low latency. The AAU, as a key access point for wireless communication, is responsible for interacting with user equipment (such as smartphones, wireless terminals, etc.). The DU is primarily responsible for signal processing and computational tasks at the base station. It receives and processes signals from the AAU, performs analysis and scheduling, and then transmits the processed signals to the core network for further processing. As 5G networks continue to evolve, traditional fronthaul technologies are facing challenges in bandwidth and security. Accordingly, a new architecture is proposed that combines passive Wavelength Division Multiplexing (WDM) technology with quantum communication, utilizing Quantum Key Distribution (QKD) to enhance the security of the fronthaul system. Furthermore, quantum communication between the AAU and DU further strengthens data encryption protection.

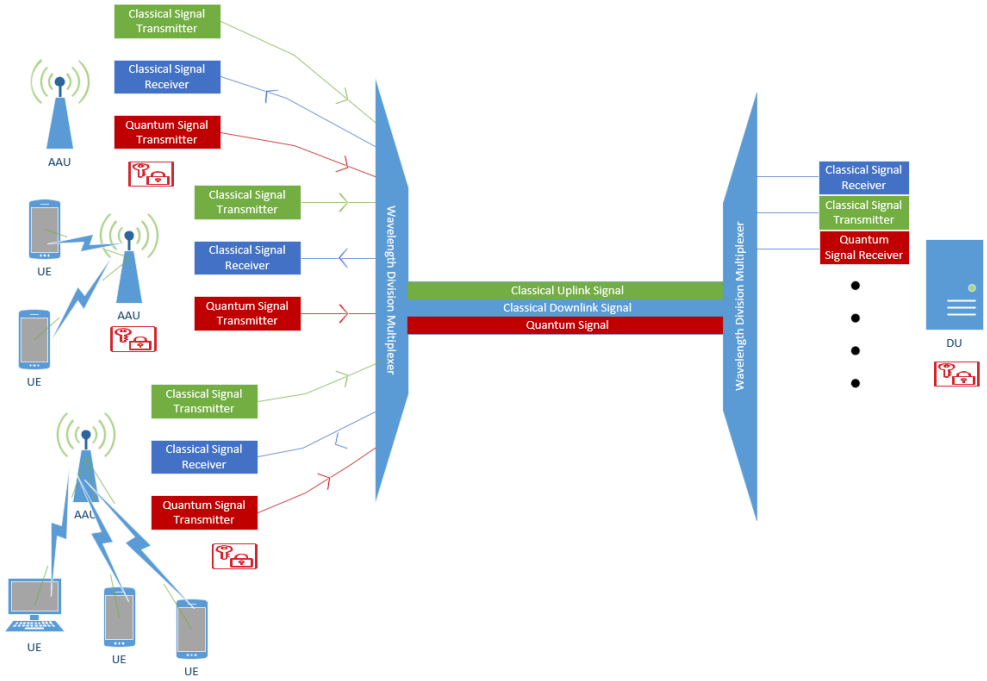

Figure 1: Quantum encryption-based passive wavelength division multiplexing communication architecture

In this architecture, the AAU serves as the Alice node in quantum communication, receiving information transmitted wirelessly from mobile phones and computers. It is responsible for initiating the QKD process, generating, and transmitting quantum keys. The AAU handles different types of

DOI: 10.54254/2755-2721/155/2025.GL23420

signals, including classical uplink signals, classical downlink signals, and quantum signal transmission. Using passive WDM technology, the AAU multiplexes multiple wavelengths onto a single optical fiber, with some wavelengths dedicated to QKD and others to classical data transmission. As the Bob node in quantum communication, the DU receives quantum bits (qubits) from the AAU via the passive WDM link and uses the received qubits to generate a shared key. Additionally, the DU exchanges basis selection information with the AAU via a classical channel and publicly announces part of the key data to ensure mutual agreement on the key. According to the QKD protocol, the DU measures and compares the received quantum bits. If any interference or eavesdropping behavior is detected (e.g., a significant increase in the error rate), the DU will notify the AAU to regenerate and transmit a new key, ensuring the confidentiality of the communication.

This architecture integrates the benefits of quantum communication and passive WDM technology, offering a secure and efficient communication link for the IIoT. Quantum communication provides ultra-high security, preventing eavesdropping and interference, while passive WDM enhances bandwidth utilization through wavelength multiplexing and reduces network costs. Furthermore, the high security afforded by quantum encryption ensures that sensor data and control commands are adequately protected during transmission, significantly enhancing the overall data security and network stability of IIoT systems. This architecture not only meets the demand for high bandwidth and low latency but also effectively supports the efficient and secure operation of 5G and future communication networks.

4. Simulation analysis

To systematically investigate the impact of various parameters on the secure key generation rate and Quantum Bit Error Rate (QBER), three key system parameters were adjusted: attenuation coefficient, detection efficiency and dark count per pulse. The results of these adjustments are summarized as follows.

The relationship between the secure key generation rate and QBER with respect to transmission distance was analyzed in this study. The general trends observed indicate that, in the quantum communication system designed within our architecture, increasing transmission distance leads to greater signal attenuation, which negatively impacts the secure key generation rate. At the same time, the QBER increases as transmission distance extends, largely due to cumulative noise effects.

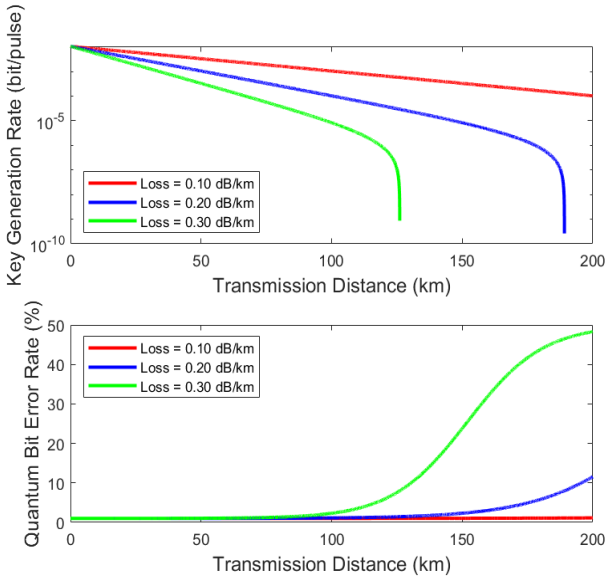

Figure 2: Effect of loss coefficient on secure key rate and QBER in quantum communication

DOI: 10.54254/2755-2721/155/2025.GL23420

The attenuation coefficient (Loss) is a critical factor that impacts the loss of light signals during transmission. In our study, when the attenuation coefficient was low (e.g., Loss = 0.1 dB/km), the key generation rate remained high, especially over longer transmission distances, with little decrease in key generation capability. Additionally, a lower attenuation coefficient helped mitigate the increase in the QBER, indicating that the system was better at suppressing noise, thereby maintaining communication quality. In contrast, with a higher attenuation coefficient (e.g., Loss = 0.2 dB/km), both the key generation rate and QBER exhibited poorer performance. As the transmission distance increased, the key generation rate sharply decreased, and the QBER escalated, demonstrating that a higher attenuation coefficient caused greater signal loss, exacerbating system noise interference and reducing system effectiveness.

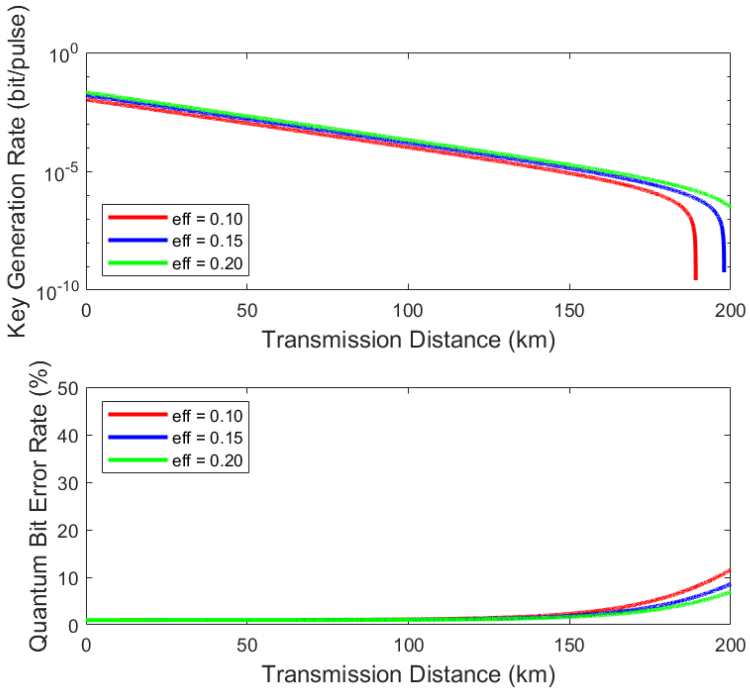

Figure 3: Effect of detection efficiency on secure key rate and QBER in quantum communication

Detection efficiency (Eff) plays a crucial role in the overall performance of the system. As the detection efficiency increases (e.g., Eff = 0.20), the secure key generation rate improves significantly. Higher detection efficiency enhances the system's ability to detect quantum signals, thereby increasing the likelihood of successful key generation. However, this improvement also comes with a trade-off—QBER tends to rise as detection efficiency increases, particularly over longer transmission distances. This suggests that while greater detection efficiency facilitates key generation, it may also amplify error rates in noisy environments. Therefore, optimizing detection efficiency is essential to balance key generation performance and system stability. As shown in Fig. 3, higher detection efficiency consistently results in a higher secure key rate across the entire transmission range but also leads to a steeper increase in QBER beyond approximately 140 km. This visual evidence highlights the importance of striking a balance between detection capability and noise tolerance when designing robust quantum communication systems.

DOI: 10.54254/2755-2721/155/2025.GL23420

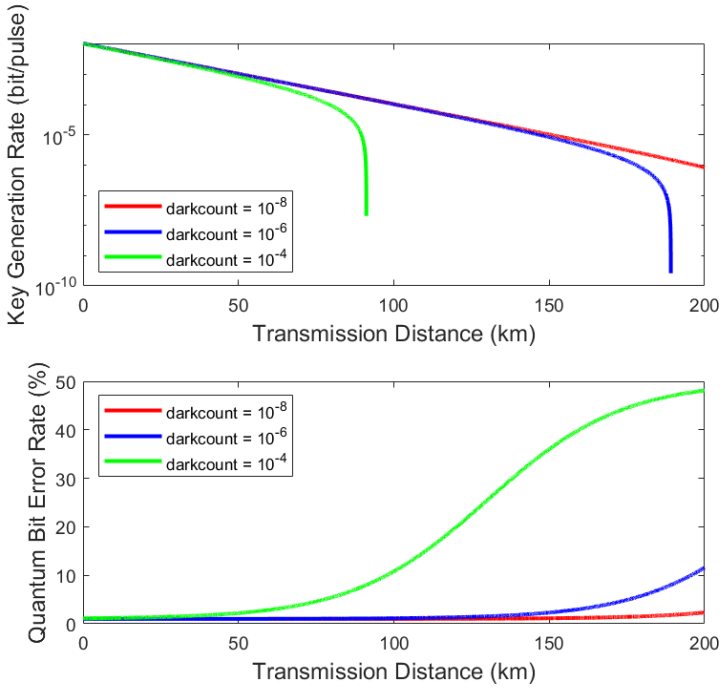

Figure 4: Effect of varying dark count values on QKD performance across transmission distances

Dark count (darkcount) is another critical parameter that affects the quality of quantum signal detection. As illustrated in Fig. 4, a lower dark count value (e.g., darkcount = 10^{-8}) significantly improves system performance by reducing background noise. This enables the system to maintain a higher key generation rate and slows the increase in QBER. However, when the dark count increases (e.g., darkcount = 10-4), the key generation rate declines more sharply, and the QBER rises rapidly. This suggests that higher dark count values introduce more noise into the quantum signal detection process, leading to rapid degradation in system performance. Therefore, minimizing the dark count is essential for enhancing the overall reliability and efficiency of quantum communication systems.

5. Conclusions

This paper presents a comprehensive investigation into the application of quantum encryption in the Industrial Internet of Things (IIoT), with a focus on integrating passive wavelength division multiplexing (WDM) and quantum key distribution (QKD) to secure 5G fronthaul communications. The proposed architecture introduces a novel model for high-efficiency, multi-channel transmission and redefines the practical deployment of quantum communication in real-world industrial environments. Simulation results confirm the effectiveness of the proposed framework, demonstrating how key physical and operational parameters influence transmission performance. Specifically, a lower attenuation coefficient and dark count rate were shown to significantly enhance the secure key generation rate and reduce the quantum bit error rate (QBER). Conversely, while increased detection efficiency improved signal detection, it also introduced trade-offs in noisy environments. These findings offer valuable insights for parameter optimization in future system implementations.

From an application standpoint, the architecture's compatibility with existing fiber infrastructure and its alignment with 5G technologies make it a highly practical solution for industrial deployment. It shows strong potential in scenarios that demand secure data transmission, such as factory automation, real-time diagnostics, and intelligent logistics.Moreover, this architecture only requires

DOI: 10.54254/2755-2721/155/2025.GL23420

the addition of quantum signal channels to the existing infrastructure without necessitating a complete overhaul of current equipment, thereby reducing implementation costs to a certain extent. By integrating quantum communication, the architecture offers a scalable and future-ready solution to IIoT security challenges, representing a strategic advancement toward next-generation industrial networks.

Future research may explore multi-user quantum key distribution, evaluate performance under dynamic network conditions, and investigate the integration of quantum-safe protocols with classical network management systems to further improve scalability, robustness, and practical applicability.

References

[1] *Sisinni, Emiliano, et al. "Industrial Internet of Things: Challenges, Opportunities, and Directions." IEEE Transactions on Industrial Informatics, vol. 14, no. 11, Nov. 2018, pp. 4724–4734. https://doi.org/10.1109/TII.2018.2852491.*

[2] *Pivoto, Diego G. S., et al. "Cyber-Physical Systems Architectures for Industrial Internet of Things Applications in Industry 4.0: A Literature Review." Journal of Manufacturing Systems, vol. 58, 2021, pp. 176–192. https://doi.org/10.1016/j.jmsy.2020.11.017.*

[3] *Jamwal, Anbesh, et al. "Industry 4.0 Technologies for Manufacturing Sustainability: A Systematic Review and Future Research Directions." Applied Sciences, vol. 11, no. 11, 2021, article 5725. https://doi.org/10.3390/app11115725.*

[4] *H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework," Computers in Industry, vol. 101, pp. 1–12, 2018, doi: 10.1016/j.compind.2018.04.015.*

[5] *Roblek, Vasja, Maja Meško, and Alojz Krapež. "A Complex View of Industry 4.0." SAGE Open, vol. 6, no. 2, 2016, pp. 1–11. DOI: 10.1177/2158244016653987.*

[6] *Raimundo, Ricardo Jorge, and Albérico Travassos Rosário. "Cybersecurity in the Internet of Things in Industrial Management." Applied Sciences, vol. 12, no. 3, 2022, article 1598. https://doi.org/10.3390/app12031598.*

[7] *Abhishek Hazra, Mainak Adhikari, Tarachand Amgoth, and Satish Narayana Srirama. A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions. ACM Computing Surveys, Vol. 55, No. 1, Article 9, November 2021. https://doi.org/10.1145/3485130*

[8] *Hammad, Muhammad, et al. "Security Framework for Network-Based Manufacturing Systems with Personalized Customization: An Industry 4.0 Approach." Sensors, vol. 23, no. 17, 2023, article 7555. https://doi.org/10.3390/s23177555.*

[9] *Serror, Martin, et al. "Challenges and Opportunities in Securing the Industrial Internet of Things." IEEE Transactions on Industrial Informatics, vol. 17, no. 5, May 2021, pp. 2985–2996. https://doi.org/10.1109/TII.2020.3023507.*

[10] *Ahmed, Shams Forruque, et al. "Industrial Internet of Things Enabled Technologies, Challenges, and Future Directions." Computers & Electrical Engineering, vol. 110, Sept. 2023, 108847. https://doi.org/10.1016/j.compeleceng.2023.108847.*

[11] *Zhao, Baokang, et al. "A Tutorial on Quantum Key Distribution." 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015, pp. 174–179. https://doi.org/10.1109/BWCCA.2015.108.*

[12] *Padmavathi, V., et al. "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey." 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016, pp. 139–143. https://doi.org/10.1109/IACC.2016.87.*

[13] *Liu, Yutong. "The Principle and Prospect of Quantum Communication." Journal of Physics: Conference Series, vol. 1634, 2020, 012139. https://doi.org/10.1088/1742-6596/1634/1/012139.*

[14] *Preuveneers, Davy, and Elisabeth Ilie-Zudor. "The Intelligent Industry of the Future: A Survey on Emerging Trends, Research Challenges, and Opportunities in Industry 4.0." Journal of Ambient Intelligence and Smart Environments, vol. 10, no. 3, 2018, pp. 1–12. https://doi.org/10.3233/AIS-170432.*

[15] *Xu, Li Da, and Wu He. "Internet of Things in Industries: A Survey." IEEE Transactions on Industrial Informatics, vol. 10, no. 4, Nov. 2014, pp. 2233–2243. https://doi.org/10.1109/TII.2014.2300753.*

[16] *Díaz, Camilo A. R., et al. "IoToF: A Long-Reach Fully Passive Low-Rate Upstream PHY for IoT over Fiber." Electronics, vol. 8, no. 3, Mar. 2019, article 359. https://doi.org/10.3390/electronics8030359.*

DOI: 10.54254/2755-2721/155/2025.GL23420

[17] *Hui, Hongxun, et al. "5G Network-Based Internet of Things for Demand Response in Smart Grid: A Survey on Application Potential." Applied Energy, vol. 257, 2020, 113972. https://doi.org/10.1016/j.apenergy.2019.113972.*

[18] *Wójcicki, Krzysztof, et al. "Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review." Energies, vol. 15, no. 5, 2022, article 1806. https://doi.org/10.3390/en15051806.*