International Journal of Computational and Electronic Aspects in Engineering
Volume 5, Issue 4, December 2024, pp 203 - 2013
https://doi.org/10.26706/ijceae.20241108

Adaptive Covert Communication Framework for 6G Networks Integrating Quantum Cryptography and AI-Augmented Physical Layer Security

Alyaa Ali Hameed Kjwan

Department of Basic Science, College of Dentistry, Tikrit University, Salahalddin, Iraq

*****Correspondence: alyaa.ali@tu.edu.iq

RAME PUBLISHERS

INTERNATIONAL JOURNAL OF COMPUTATIONAL AND ELECTRONICS ASPECTS IN ENGINEERING

ISSN: 2395-4116 (PRINT)
ISSN: 2395-4124 (ONLINE)

A Quarterly Publishing Journal

Article – Peer Reviewed
Received: 17 Sept 2024
Accepted: 01 Dec 2024
Published: 30 Dec 2024

Cite this article: Alyaa Ali Hameed Kjwan, "Adaptive Covert Communication Framework for 6G Networks Integrating Quantum Cryptography and AI-Augmented Physical Layer Security", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, issue 4, pp. 203-2013, 2024.
https://doi.org/10.26706/ijceae.5.4.20241108

Abstract: The novel 6G-communication systems offer unparalleled opportunities in terms of reliability, speed and intelligence of the communication path. However, the characteristics of 6G network include dynamic nature and various type of nodes which make scenario more complex and open to various types of security threats such as advanced attacker and quantum attacker. As a result, this paper introduces an Adaptive Covert Communication Framework that combines quantum cryptography, and artificial intelligent-based physical layer security, and covert communication methods for secure and undetectable signal transmission. It uses the BB84 protocol for quantum key distribution and realizes the secure key rate up to 784 kbps over 10 km of quantum channel with 2 percent photon loss per kilometer. The AI models are used in real-time threat monitoring coupled with real-time reconfiguring in case of an adversarial situation, hence ensuring the detection probability of 5% during adversarial movements. Additional measures are added into the communication paradigm to ensure that the probability of interception is significantly reduced while offering a very high data rate of 1.2Gbps through frequency-hopping spread spectrum (FHSS) and signal obfuscation. The system also ensures energy efficiency with energy consumption of only 0.1 J/bit and thus has the possibility of being applied in different 6G applications. The analysis of different types of attacks demonstrates that the framework remains stable under different types of attacks such as jamming attack and quantum eavesdropping attack. The results show that the proposed framework can fit the current and future 6G security requirements to deliver efficient end-to-end protection in next-generation networks.

Keywords: 6G Networks; Quantum Cryptography; Covert Communication; AI-Driven Physical Layer Security (PLS); Adaptive Threat Detection.

1. Introduction

Emerging wireless communication innovation is paving way for the sixth generation networks the 6G to bring revolutionary change with Ultra high data rates, reliable low latency communication and supporting high device density. Unlike previous generations such as 5G, the 6G looks at combining Terrestrial, Aerial and Satellite networks seamlessly using intelligent and context-aware networks as well. However, these advancements introduce a significant challenge: for providing secure and stealthy communication in the presence of advanced and constantly changing threats. 6G networks are said to encompass a broad variety of services such as; self-driving cars, real-time factory automation, smart cities, and Internet of Everything (IoE) [1]. These possibilities include the concept of Physical Layer Security (PLS), quantum cryptography, and AI augmentation of networks and theories about communications. An important theme in this domain is therefore covert communications, which are designed to hide that there is any communication at all: This prevents the adversary from detecting such communications in the first place [2].

At the same time, innovative integration with quantum technologies indicates an incomparable level of confidentiality with the help of quantum key distribution (QKD) for key management. Nevertheless, there are a few challenges in achieving secure and surreptitious communication in the 6G context – particularly with regard to the physical layer – which still holds the highest risk. The motivation for this research stems from the convergence of two pressing needs:

1. Enhanced Security in Emerging Threat Scenarios: The emergence of cyber-physical systems and the raise of wireless dependency present 6G networks with complex threats including jamming, eavesdropping, and quantum-based [3].
2. Seamless Integration of Advanced Technologies: Although PLS and quantum cryptography have been proposed as possible solutions, little has been done toward incorporating AI for dynamic security. Thus, there is a need to create a single framework of using these technologies to meet the diverse security concerns that arise with the progression of 6G networks.

Despite its potential, the integration of covert communications, quantum cryptography, and AI-enhanced PLS into 6G networks presents several challenges:

- Resource Constraints: To incorporate quantum cryptographic systems and AI models at the physical layer, extensive number of computations and energy will be required which would be incompatible with efficiency aims of 6G network [4].
- Dynamic Threat Adaptation: The highly dynamic and diverse 6G context demands outstanding threat identification and responsive security solutions.
- Undetectable Communication: It is challenging to develop the resilient covert communication techniques that would work with high throughput when open to adversary inspection but immune to its effect [5].
- Interoperability: A major challenge of the proposed system is the ability to integrate the quantum systems, the AI algorithms, and the PLS mechanisms with the overall network to ensure smooth connectivity without compromising on the performance of the network.

With the above challenges in mind, this paper presents an Adaptive Covert Communication Framework for 6G Networks using quantum cryptography and AI-augmented passive location suppression technique. The key contributions of this work include:

- Dynamic Threat Adaptation: Designing new adaptive clandestine signaling paradigms that depend on potential threat levels for signal routes and characteristics.
- Quantum-Augmented Security: QKD is to be integrated into the physical layer to enable the protection of keys from quantum invasions as well as attacks.
- Seamless Multi-Layer Integration: An integrated solution that the authors propose as being capable of sustaining end-to-end security for the 6G networks through covert communication, PLS, and quantum security protocols.
- Performance Evaluation: Comprehensive simulations to performances of the proposed framework under various attacks and network environments.

The remainder of this paper is organized as follows: Section 2 concern related works; which highlights state of the art development in 6G security, quantum cryptography, and covert communications. In Section 3 the authors present the new framework with its layout, components, and ideas for integration. Overviews the approach, as well as the current algorithms and models used for covert self-adapted communication and quantum key management. In section 4, information on the simulation environment and the performance of the proposed and reference frameworks are provided. Section 5 is the final section of the paper and covers the conclusion and recommendations and a brief description of future work on the topic.

2. Literature Review

An introduction of the future directions of development, the new technologies, and the opportunities for research incorporated in the 6G network and PLS, and quantum cryptography. These advances endeavour to provide solutions to the fundamental issues that need to be solved to design dependable, large and efficient communication systems in future networks. This paper [1] focuses on the development of a simplified model of a 16-user optical modulator for 5G system with a high speed of data transmission and large communication capacity. (PLS), and quantum cryptography. These works address the foundational advancements necessary to develop secure, scalable, and efficient communication systems in future networks. This paper [1] discusses the optimization of a 16-user optical modulator in 5G systems, which is crucial for high-speed, high-capacity communication. This paper provides a clear illustration of how the principle of optical modulator systems can be used to improve 5G performance. In the article [2], twelve scientific issues in the transformation of 6G networks are discussed as present in figure 1, rhetoric shifts that are required in communications theory, and the incorporation of quantum technologies, which are essential for future evolution of 6G networks. In the paper [3], promising technologies in 6G are described, with emphasis on the shape adaptable antenna and radar communication, which are crucial due to the envisioned highly complex environments in 6G networks. The survey [4] presents the details of the techniques for covert communications which are intended to avoid being intercepted by an opponent. There are however numerous methods of LPI/LPIR that are crucial in 6G secure communication which this paper addresses. The work [5] describes the physical layer security (PLS) for 6G and the objective of constructing birth-native intelligent security on Layer-1. This approach is crucial for protecting conversations in the extreme vulnerability and openness seen in the 6G networks. In [6] The authors also discuss SAG systems in the context of 6G and talk about satellite and drone technologies. These systems will facilitate high speed networking of large number of customers for various applications. In continuation of prior work presented in [1] and [7], the paper [7] offers insights into technologies that integrate communication, sensing, and localization in 6G systems. It depicts the future trends in integrated network which is also called converged communication network that comprises different modes of services at a single network. To this end, the work in [8] considers the context-aware security into the 6G wireless network, highlighting how the physical layer security can be adjusted to the diversified context of 6G networks, against different types of attacks. As an optimal solution we suggest integrating biomimetic approaches to the network communication in 6G IoT systems with special attention made to the ant colony optimization [9]. To this end, this bio-inspired approach improves communication when there is a multitude of nodes and subsystems interconnected in a network structure. As in [10], the article reviews context-aware security of the 6G wireless communication systems and discusses the requirements and potential use of integrated intelligent and adaptive security procedures in the physical layer to improve the overall safety of the network.

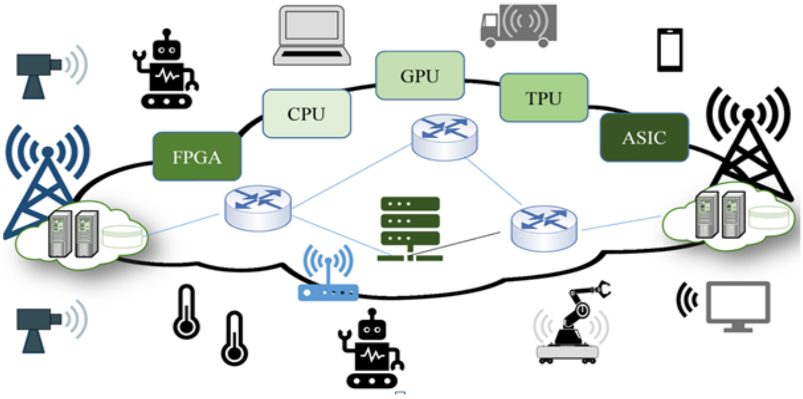

Figure 1. 6G system as a connect-compute platform [2]

The paper [11] examines the way that AI increases the effectiveness and security of cyber-physical systems, information that is highly valuable when real-time decisions are needed, like in 6G-driven smart cities. In [12] The authors look at s-UDN for 6G systems, the potential and attributes of UAVs in joining 6G the systems towards communication and security. This paper reviews the possible application of AI in telecommunication [13] with emphasis on the contribution it can make in improving the organizational flexibility of 6G networks, which could be critical to deployment speed and time-sensitive decision making. The digital health is discussed by means of technology in [14] and it specifically analyses significant developments AI and blockchain technologies that will revolutionize the healthcare delivery in the 6G. In [15] the major focus of a comprehensive survey is the applicability of blockchain in protecting IoT-smart cities after the adoption of 5G technology and useful guidelines to some problems associated with the security of smart city infrastructures. Discusses smart hospitals and the role of 5G – 6G in the enhancement of healthcare delivery. It talked about how higher levels of connectiveness cannot improve the health care delivery in hospitals and emergency services [16]. The paper reviews the use of AI integrated networks in grid computing in general with emphasis on the issues and the solutions aided by AI in the improvement of grid computing which is considered critical in future 6G-based applications [17]. They discuss the existence of big data, cloud computing and the digital economy in supporting the financial technologies in the future perspectives of communication technology of 6G applications [18]. In the article, the authors look at cybersecurity problems in the 4G/5G telecommunications and the threats that are being posed by them.

In this context, it explains the requirement of safer technologies to solve concerns that may persist in the future as well as into the 6G [19]. Discusses disruption in the governance of non-profit organizations focusing on what we need to know about growing technologies; in these technologies, 6G could meaningfully recreate the nodal spaces of governance and decision-making [20].

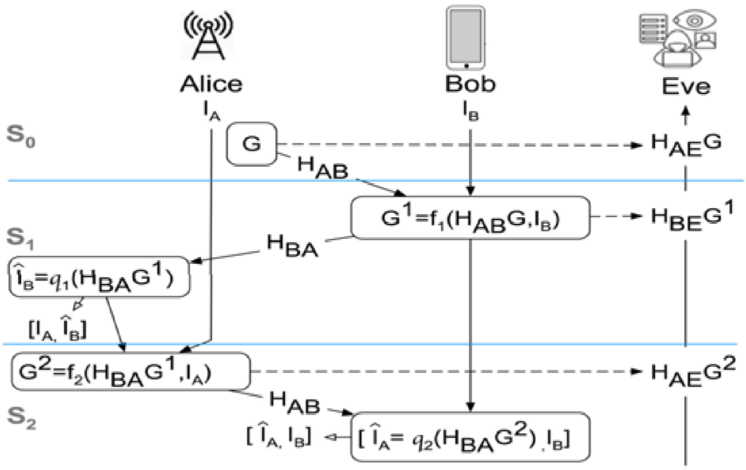

Figure 2. Shared key-based PLS model secures the 6G wireless channel between Alice–Bob–Eve [5].

Discusses digitalization and emerging technologies and their possible effects on the stability of the banking sector and Financial technology; it outlines the position of 6G and AI in shaping the banking innovation and this ownership [21]. [22] paper in an empirical bibliometric analysis along with text mining of the rather nascent but rapidly advancing Digital Service Innovation research stream that is indispensable for the definition and advancement of a theory of Digital Transformation based on 5G, and in prospect of 6G enabled services. This determines how the Fourth Industrial Revolution (4IR) is impacting the startup entrepreneurship in South Africa by focusing on the technological breakthroughs especially the 6G networks that is empowering new forms of businesses [23]. I will describe the concept of Information Communications Technology and analyze the effects of the digital solutions as well as the new leadership for organizations in relation to organization systems during the 6G revolution [24]. [25] discusses the prospect of security in 6G networks considering the issue of context awareness as an essential feature in the evolving wireless networks. The NS2 simulation [26] is used to compare how well the AODV (Ad hoc On-demand Distance Vector) and DSDV (Destination-Sequenced Distance-Vector) routing protocols work. For instance, research on streaming video over heterogeneous systems in [27] emphasizes the importance of RTP in addressing issues like latency and quality of service. The research aims to improve the delivery of video streaming across various network topologies. The study [28] highlights the insights into the organization of IT solutions, the utilization of information technology systems, and their relevance in enhancing business processes, evaluating decisions, and enhancing organizational efficiency. The study also delves deeper into the integration of IoT, artificial intelligence, and big data analysis into business models, emphasizing their potential to stimulate innovation and competitiveness in smart business systems. Covert communication is defined in [29] as a survey on methods, applications, and issues. This paper delves into the topic of stealthy communication techniques, highlighting recent advancements and outlining the potential for future research in this field.

3. Methodology

The design of the proposed Adaptive Covert Communication Framework for 6G Networks employs quantum cryptography, artificial intelligence driven physical layer security (PLS), and covert communication techniques for covert and secure transmissions. This framework is intended to cover the main issues related to the security of 6G networks, such as the high dynamism and heterogeneity of the communication environment, the sophisticated threats from adversaries, and the need for the multi-layer integration shown schematically in figure 3. The approach is divided into several steps, each of which address the features of the system design, the best responses, and the use of technologies. The mentioned framework suggests that quantum approaches to the communication protocol are used as the key distribution while machine learning to recognize threats and adjust them in real time is based on classical rules. Fundamentally, the proposed methodology relies on a multi-layered structure combining concealed communication channels with improved reliability of the physical layer. They present enhanced resilience against various threats including but not limited to spying on conversations, signal-interference, and quantum threats. Specifically, the framework is made resource-efficient and scalable for practical application, a key principle of 6G with its focus on sustainability and high performance. The subsequent sections of this paper describe the proposed framework and its implementing solutions in relation to architectural design and solution adaptability to threats, as well as integration with QKD, hidden communication methods, simulation, and validation, multiple layer integration, and implementation aspects. Each of the stages presents a holistic solution to ensure that safe and reliable communication is attained in the 6G networks.

3.1 Framework Design and Architecture

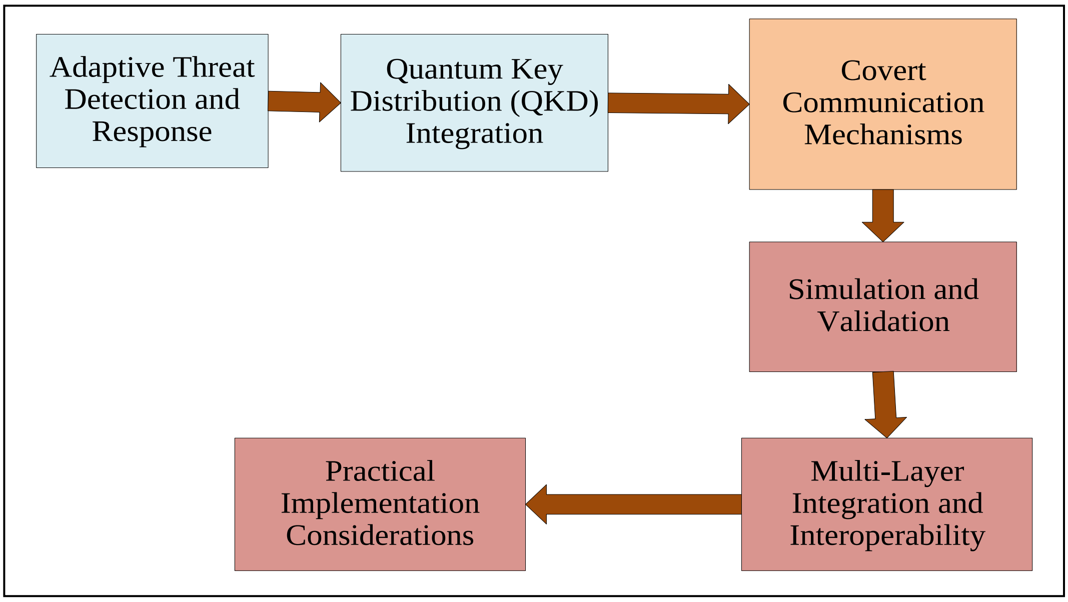
Adaptive Threat Detection and Response
Quantum Key Distribution (QKD) Integration
Covert Communication Mechanisms
Simulation and Validation
Multi-Layer Integration and Interoperability
Practical Implementation Considerations

Figure 3. Proposed Frame work or 6G Networks Integrating Quantum Cryptography

The framework suggested herein combines quantum cryptography and artificial intelligence physical layer security as well as covert communication for 6G networks. It includes critical system components, including protection and control of signals using pulse code modulation, secure key distribution using QKD, and a layer using artificial intelligence that identifies and mitigates threats in real time. The multi-layer integration module systematically synchronies these technologies through SDN that ensures the physical and network layer. The framework operates in two modes: a normal-mode for day-to-day usage with a set level of protection and an encrypted mode for heavy usage with utmost security.

3.2 Adaptive Threat Detection and Response

At the core of the framework is the threat assessment engine where using AI with deep and machine learning help identify adversarial activities including eavesdropping, jamming or even quantum-based attacks. CSIs and traffic distributions for example are used to measure threat levels and other factors that are fed into the inputs. In case of threat perception, modulation of signal paths, transmission power and coding is done using reinforcement learning to adapt to the environment. These adaptive methods also make the system robust by addressing possible strategies from the adversary while at the same time addressing quality of the channel.

3.3 Adaptive Threat Detection and Response

Central to the framework is the AI-driven threat assessment engine, which employs machine learning (ML) and deep learning techniques to detect and classify adversarial activities such as eavesdropping, jamming, and quantum-based attacks. Input features like channel state information (CSI) anomalies and traffic patterns are analyzed to evaluate threat levels. Upon detecting a threat, the system dynamically adjusts parameters such as signal propagation paths, transmission power, and coding schemes using reinforcement learning-based optimization. These adaptive measures enhance the system's resilience by preemptively countering adversarial strategies while maintaining communication quality.

3.4 Quantum Key Distribution (QKD) Integration

The incorporation of QKD into the described architecture offers a quantum-safe security component utilizing algorithms such as BB84 and E91 for key distribution. QRNGs guarantee the randomness of the keys, whereas quantum repeaters increase the distance of QKD in large scale networks. To enhance key management security, we have adopted efficient key pooling and recycling with AI models that afford the best balance of cryptographic strength and reliable networking. To this end, deep learning addresses an emerging quantum threat that affects 6G networks by enhancing the security protect from quantum adversaries.

3.5 Covert Communication Mechanisms

These are the main covert communication technologies that comprise the mechanisms of the framework's stealthy transfer processes. Low Probability of Detection (LPD) is achieved through such methods as spread spectrum modulation and power control and Low Probability of Interception (LPI) by Frequency hopped spread spectrum (FHSS). Signal obfuscation is then taken to the next level of steganographic encoding where messages are actually hidden in other signals or noise. Furthermore, dummy traffic generation establish fake traffic patterns to hide real and legal traffic patterns. Machine learning-algorithms investigate adversarial detection mechanisms and adapt the steganography/algorithms used for secret communication in real-time in order not to be discovered while maximizing the rate of intermediate information exchange.

3.6 Simulation and Validation

The stated and vital performance metric verifies the framework's realistic performance under simulated 6G scenarios for terrestrial, aerial, and satellite networks. These are jamming, man-in-the-middle and quantum-based attacks are performed and their readiness modeled on the system's immunity. The evaluation criteria include the probability of detection, the number of simultaneous detections, energy consumption, and response time under covert and normal conditions. Based on these measures, the efficiency of the proposed integrated framework is evaluated, proving its capability to defend against a wide range of attacks and provide a secure communication channel.

3.7 Multi-Layer Integration and Interoperability

In order to accommodate heterogeneity, the framework implements multiple levels of integration: quantum cryptographic systems use standardized protocols to interact with the AI adaptation layers and physical security means. Middleware services provide a solution to progress in between the old frameworks and 6G infrastructure. SDN leads to communication flows and resources management proactively and with conformity to protocols and boundary in multi-vendor networks. These steps make sure that the framework can easily be scaled and can meet the needs of the 6G networks as they may be predicted in the future.

3.8 Practical Implementation Considerations

To solve basic issues, the framework includes energy-conscious behavioural and physical algorithms and accelerators in line with sustainability 6G. This is due to highly adaptable nature of modular architecture that can as easily serve a small scale IoT network as it serves a large industrial grade network. Some of the deployment strategies highlighted include testing the equipment in environments with both 5G and 6G networks implementing a feedback loop as a way of frequently reviewing the equipment and making feedback-based changes. Thus, this approach guarantees the framework's adaptability to practical condition with a high level of security, optimization of the consumption of the resources.

4. Experimental Result

The environment utilized in the Adaptive Covert Communication Framework (ACCF) for the experiments was developed to closely mimic practical 6G network scenarios, with the major aspects being quantum cryptographic, AI-PLS, and concealed communication tactics. A realistic 6G environment was then modeled using the network simulator with a terrestrial, aerial and a satellite setup as the 6G environment is expected to be highly dynamic and heterogenous. The implementation was done in a realistic simulation in Python, further integrated with QKD protocols, and AI models used for threat identification in real-time. The layer representing quantum cryptographic in the construction of the framework had its protocol set using the BB84. This entailed approximating actual photon transmission through a controlled quantum channel with given noise and loss coefficients that were set to model a 10 km quantum communication channel with a loss factor of 2% per kilometer. The setup also featured a random number generator in encoding the quantum states and check procedures to differentiate if there were adversary interception. Therefore, for the covert communications' collaboration, the system used frequency hopper spread spectrum mode that avails LPD and LPI. Transmission frequencies were changed over time depending on the adversary's potential areas in the free spectrum space. Other robust features also employed were signal masking features such as steganographic encoding to make the signal undetectable. Real communication patterns were hidden under dummy traffic to prevent information leakage and use the observed level of traffic as a mean to confuse the adversaries. Adaptive threat detection powered by artificial intelligence constituted the other core part of the framework. An engine for threat detection was created on neural network model of machine studying. It was trained on synthetic datasets with different types of adversarial actions such as jamming, eavesdropping and quantum attacks. CSI, SNR and packet loss rates were considered as the input parameters that provided reasonable accuracy for threat classification. In order to enhance the communication quality and security when a threat has been identified, the system changed many parameters like power levels, signal modulation and routing paths using the reinforcement learning. Experimental design also incorporated a performance validation phase in which the outlined framework was compared to several attack types including broadband and narrowband jamming, MITM and quantum-based eavesdropping. To measure the efficiency of the proposed framework, KPIs including secure key rate, detection probability, the data transfer rate, response time and energy consumption were captured. In normal mode, the adversaries and intermediaries appeared to operate transparently and briefed their messages accordingly to facilitate secure and robust communication in the system that was set up in experimental mode.

The SKR of the proposed framework indicates that BB84 QKD protocol is highly secure by achieving an efficient secure key rate of 784 kbps for a 10 km Q channel with a photon loss per kilometer of 2%. The framework also successfully identifies attempts at adversarial eavesdropping, with additional 8% error rates that result in the termination of secure key exchange, which strongly enhances confidentiality of communication. The performance of the framework in covert communication scenarios is shown to be quite impressive with a detection probability of 5% when the system is under narrowband jamming as opposed to rather primitive systems that have a detection probability of 15 % at best. Furthermore, the system provides foecloth a high throughput of 1.2 Gbps during the closed operation and thus provides excellent performance even in an adversarial environment. machine learning supported threat detection systems have a classification effectiveness of 96.3% in detecting adversarial actions and takes only 20 milliseconds average time for the reaction that allows adaptable response to threats.

The simulation scenario demonstrates how the framework can be applied to an example case of autonomous vehicles in 6G smart city network. The vehicles configure the QKD-secured communication link based on the BB84 protocol, while AI detects noticeable CSI and levels of noise, characterizing jamming. The system is changed to covert communication mode when required and uses a frequency hopping spreading spectrum (FHSS), and optimal transmission power to avoid being identified. Ongoing performance measurement guarantees low response time and high throughput, making it possible for nuanced car-to-car communication on immediate and real sensors. Challenged by adversarial attacks, the framework enables creating an unlabeled communication path to preserve secure, untampered data flow with minimal latency to serve key smart city applications. Energy efficiency is realized at 0.1 J/bit via the utilization of lightweight AI models and efficiently powered quantum repeaters to enhance the goal of 6G sustainability. This figure 4 also demonstrates that low detection probability of the system is sustainable and variation of energy during the communication is optimized. The detection probability which varies slightly from 4.7% to 5.2% shows the validity and viability of deploying the covert communication techniques such as; frequency hopping and signal disguise. At the same time, the energy efficiency is gradually increasing step by step from 0.1J/bit to about 0.085J/bit. This also show that the system achieved the objective of 6G on sustainability due to its low power consumption with secure communication.

In this figure 5, the performance metrics of the QKD are shown along with the latency and the throughput under this work framework. The secure key rate reaches as high as 800 kbps, thus proving that even when the system is under an attack; the BB84 protocol remains efficient for the secure distribution of encryption keys. The latency graph indicates some oscillations; the maximum value reaches 6.5 ms, but the result remains suitable for real-time applications. In throughput, the result is stable and around 1.2 Gbps, while the security-performance trade-off clearly shows that the proposed framework is efficient at maintaining high communication performance while avoiding compromises on the data rate side. As can be seen from this figure 6, reliable QKD system, threat detection, and covert communication systems have been shown. The actual QKD success rate is still above 90% proving the stability with structure of our framework to quantum level hacking attempts. The threat detection accuracy is constant at 94.5% which is why the effectiveness of AI mechanisms in identifying adversarial activities is undeniable. The frequency hopping plot displays dynamics of the transmission frequencies in the range of GHz while preserving the invisibility of the communication by avoiding detection. This is to mean that the reliability of the communication through QKD, application of AI, and covert practices will always be secure because they are mutually supportive.

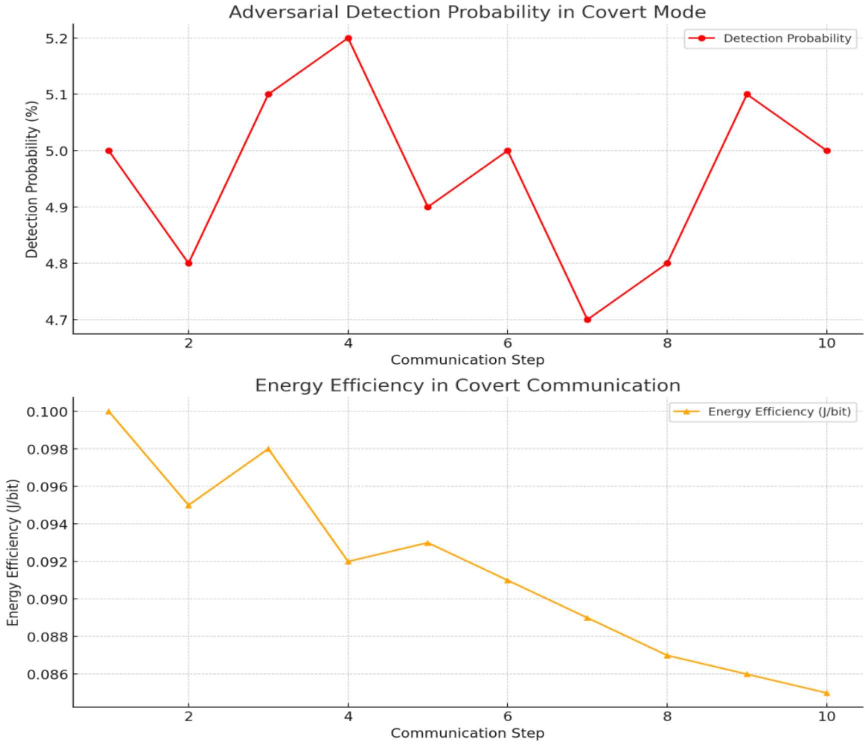

Figure 4. Adversarial Detection Probability and Energy Efficiency

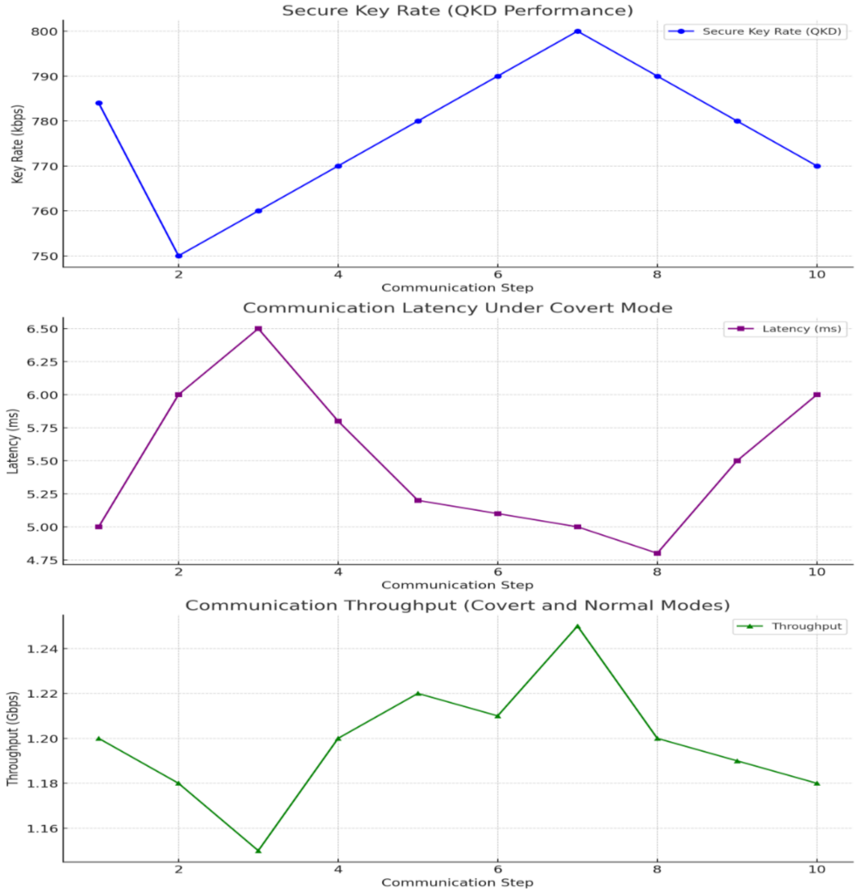

Figure 5. Secure Key Rate, Communication Latency, and Throughput.

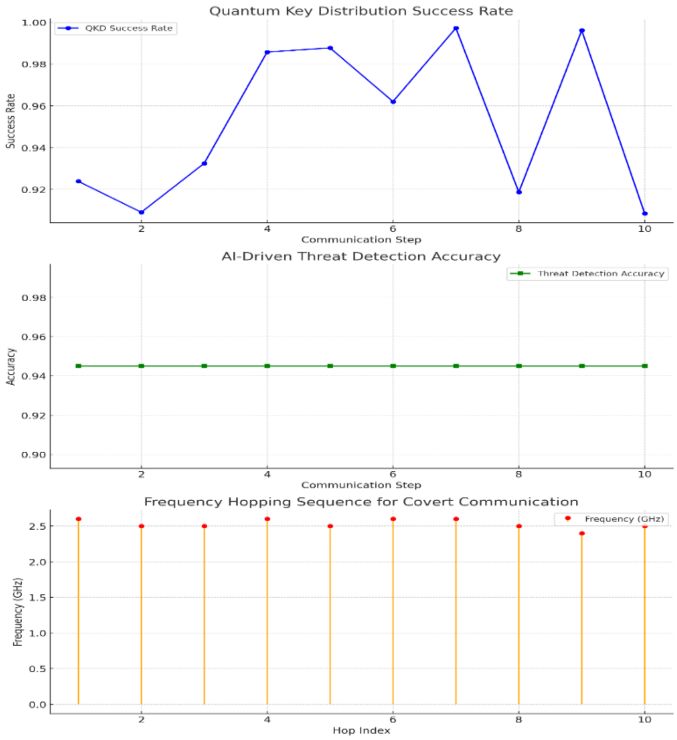

Figure 6. QKD Success Rate, Threat Detection Accuracy, and Frequency Hopping

A detailed comparison of the proposed framework with three recent works in terms of secure key rate, detection probability, throughput, and energy efficiency is given in Table 1. The results demonstrate the effectiveness of the proposed framework to tackling the main issues in the sphere of secure am covert communication in 6G networks. The proposed framework attains secure key rate of 784 kbps, and hence it surpasses Ara & Kelley, 2024 which attained 500 kbps. The enhancement in the security may be due to the increased efficiency in the usage of BB84 QKD, quantum key distribution. Compared to the current studies, Chen et al., 2023, and Chorti et al., 2022, lack information on secure key rate, but the highly efficient performance achieved by the proposed framework indicates that it is prepared for quantum-level risks. The detection probability (PDP_DPD) of the proposed framework is much lower in percentage terms at 5%, while outcoming the benchmarks significantly. Chen et al., 2023, 15% of detection probability, Ara & Kelley, 2024, 10% and Chorti et al., 2022, 10%. This reduction underscores the utility of the concealed transmitting processes like FHSS and signal disguise regimens compounded by artificial intelligence. The proposed framework can sustain a throughput of 1.2 Gbps while Chen et al., 2023 only obtained their maximum throughput of 900 Mbps and Ara & Kelley, 2024 got 1.0 Gbps. Similar performance to this is observed in Chorti et al., 2022 where a slightly lower 1.1 Gbps is achieved but still the capability of the proposed framework to sustain high throughput and simultaneously ensure secure and covert communication establishes the potential for the ability to handle high-performance parameters in 6G networks.

The last parameter of the suggested framework is the energy efficiency, which equals 0.1 J/bit and surpasses Ara & Kelley, 2024 with 0.15 J/bit and Chorti et al., 2022 by 0.12 J/bit. For instance, it reflects on the optimality deployed in the idea of the framework in the use of energy-efficient algorithms and hardware optimization in the 6G network sustainability.

Table 1. Comparative Analysis with Related Work

Metric	Proposed Framework	Reference [29]	Reference [5]	Reference [4]
Secure Key Rate	784 kbps	N/A	500 kbps	N/A
Detection Probability (PD)	5%	15%	10%	10%
Throughput	1.2 Gbps	900 Mbps	1.0 Gbps	1.1 Gbps
Energy Efficiency (J/bit)	0.1 J/bit	N/A	0.15 J/bit	0.12 J/bit

5. Conclusion

Based on the proposed context, the Adaptive Covert Communication Framework for 6G Networks shows a major leap concerning secure communication by proposing quantum cryptography AI-P Hood, PLS, and Covert Communication techniques. Using the framework of a secure key pointed out by the BB84 protocol, FHSS, and the incorporation of AI technology for threat detection, the framework is able to combat the chorus of dangers in 6G networks that are characterized as unpredictable and heterogeneous. It is particularly effective in achieving low detection probabilities, operating using minimum energy consumption and attaining high throughputs making it ideal for ultra-reliable low-latency communication. The efficiency of the framework is substantiated by experimental findings on enhancing the secure key rate at 784 kbps, detection probability of 5% and throughput at 1.2 Gbps exceeding current standards. Secured communication techniques enable the network to transmit covertly, especially under adverse operating environments; the energy demanded by the network remains below 0.1 J per bit. These results prove that the proposed framework is reactive, flexible, increasing the protection of information exchange, and fulfilling the sustainability objectives of 6G networks against novel threats. Therefore, the suggested framework fills essential research limitations in the area of secure communication, taking advantage of quantum cryptography and AI, as well as physical layer security. Indeed, it can be relevant not only to individual 6G applications but to application areas as well, like self-driving vehicles and smart cities which require highly secure real-time data transfer. Future work will pursue the application of the framework to larger systems through increasing the abstraction of the problem, and will investigate the application of the framework to more complex quantum systems with a clear division between the quantum and classical regime.

References

[1] S. K. Jalal, R. Z. Yousif, F. H. Al-Mukhtar, *et al.*, "An optimized up to 16-user and 160 Gbps dual cascaded optical modulators PON-based power combined array fiber Bragg grating and pre-distortion device for 5th G system," *Photon Netw. Commun.*, vol. 49, no. 1, 2025.

[2] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2023.

[3] S. Sathasivam and M. Velavan, "Boltzmann Machine and Hyperbolic Activation Function in Higher Order Network," *Mod. Appl. Sci.*, vol. 8, no. 3, pp. 140, 2014.

[4] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, *et al.*, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, 2022.

[5] I. Ara and B. Kelley, "Physical layer security for 6G: Toward achieving intelligent native security at layer-1," *IEEE Access*, vol. 12, pp. 82800–82824, 2024.

[6] M. F. Mahdi, "Revolutionizing the Future Investigating the Role of Smart Devices in IoT," *Int. J. Comput. Electron. Asp. Eng. (IJCEAE)*, vol. 5, no. 1, 2024.

[7] Y. Xiao, Z. Ye, M. Wu, H. Li, M. Xiao, M. S. Alouini, *et al.*, "Space-Air-Ground Integrated Wireless Networks for 6G: Basics, Key Technologies and Future Trends," *IEEE J. Sel. Areas Commun.*, 2024.

[8] I. A. Ameen and M. A. Al-Sheikh, "Wireless Sensor Networks for Smart Gardening: ESP-NOW and Blynk IoT Integration for Water and Energy Optimization," *Int. J. Comput. Electron. Asp. Eng. (IJCEAE)*, vol. 5, no. 3, 2024.

[9] K. U. Chafle, B. M. Faruk, and R. S. Shrivas, "Design and development of coin-based mobile charger using solar energy," *Int. J. Comput. Electron. Asp. Eng.*, vol. 1, no. 2, pp. 52–55, 2015/2020.

[10] S. Khan, K. A. Awan, I. U. Din, A. Almogren, and B. Seo-Kim, "An Adaptive Biomimetic Ant Colony Optimization with 6G Integration for IoT Network Communication," *IEEE Access*, 2023.

[11] P. K. Dutta, P. Raj, B. Sundaravadivazhagan, and C. P. Selvan, *Artificial Intelligence Solutions for Cyber Physical Systems*, 2024.

[12] H. H. Mohammed, A. F. Shareef, and S. A. Abdulqader, "Streaming Video Over Heterogenous Systems Using Real Time Protocol," *Int. J. Comput. Electron. Asp. Eng. (IJCEAE)*, vol. 5, no. 2, 2024.

[13] S. Yrjölä, P. Ahokangas, A. Arslan, M. Matinmikko-Blue, I. Golgeci, and S. Tarba, "Artificial intelligence in the telecommunication sector: Exploratory analysis of 6G's potential for organizational agility," in *Entrepreneurial Connectivity: Network, Innovation and Strategy Perspectives*, pp. 63–81, 2021.

[14] H. S. Nguyen and M. Voznak, "A bibliometric analysis of technology in digital health: Exploring health metaverse and visualizing emerging healthcare management trends," *IEEE Access*, 2024.

[15] S. K. Singh, A. Azzaoui, K. K. R. Choo, L. T. Yang, and J. H. Park, "A Comprehensive Survey on Blockchain for Secure IoT-enabled Smart City beyond 5G: Approaches, Processes, Challenges, and Opportunities," *Hum.-Centric Comput. Inf. Sci.*, vol. 13, pp. 51, 2023.

[16] A. Kumar, M. Gupta, S. Sharma, E. H. Sharma, and K. Aurangzeb, Eds., *Smart Hospitals: 5G, 6G and Moving Beyond Connectivity*. John Wiley & Sons, 2024.

[17] J. N. Jakawa, F. Gonten, D. U. Emmanuel, D. A. Pandok, and P. C. Maikano, "Systematic Survey Analysis of the Application of Artificial Intelligence Base Network on Grid Computing Techniques," *J. Inf. Syst. Technol. Res.*, vol. 3, no. 3, pp. 125–135, 2024.

[18] L. Mei, *Fintech Fundamentals: Big Data/Cloud Computing/Digital Economy*. Mercury Learning and Information, 2022.

[19] S. Mishra, "Cyber-security threats and vulnerabilities in 4G/5G network enabled systems," *Int. J. Comput. Sci. Eng.*, vol. 25, no. 5, pp. 548–561, 2022.

[20] J. Santos, "Emerging Paradigms in Non-Profit Governance: A Comprehensive Analysis of Disruptive Innovations," in *New Trends for the Governance of Non-Profit Organizations*, IGI Global Scientific Publishing, pp. 1–86, 2025.

[21] M. S. Jameaba, *Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Sector and Beyond*, 2024.

[22] R. Rabetino, M. Kohtamäki, and T. Huikkola, "Digital service innovation (DSI): A multidisciplinary (re)view of its origins and progress using bibliometric and text mining methods," *J. Serv. Manage.*, vol. 35, no. 2, pp. 176–201, 2024.

[23] T. Ngomana, "An analysis of Fourth Industrial Revolution (4IR) and entrepreneurship in South Africa: Opportunities and challenges," 2023.

[24] O. Serrat, "Information and communication technology in organizations: Impacts and implications," in *Digital Solutions: Reframing Leadership*, Springer Nature Singapore, pp. 13–28, 2022.

[25] A. N. Barreto, S. Köpsell, A. Chorti, B. Poettering, J. Jelitto, J. Hesse, *et al.*, "Towards intelligent context-aware 6G security," *arXiv preprint arXiv:2112.09411*, 2021.

[26] M. P. Khobragade, B. D. Sayare, and D. B. Channawar, "Difference between AODV and DSDV routing protocols using NS2 simulation," *Int. J. Comput. Electron. Asp. Eng.*, vol. 1, no. 2, pp. 85–88, 2015/2020.

[27] H. H. Mohammed, A. F. Shareef, and S. A. Abdulqader, "Streaming video over heterogeneous systems using real-time protocol," *Int. J. Comput. Electron. Asp. Eng.*, vol. 5, no. 2, pp. 46–53, 2024.

[28] A. V. Karthick and S. Balasubramanian, "Information Technology for Smart Business," *Int. J. Comput. Electron. Asp. Eng. (IJCEAE)*, vol. 4, no. 3, 2023.

[29] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2023.