# Quantum-Secure Signalling Model for L1/L2 Next-Gen Interconnect and Roaming Networks Over IPX for NB-IoT Traffic: A Review

**Themba Ngobeni and Boniface Kabaso**
Cape Peninsula University of Technology, Cape Town, South Africa

216187133@mycput.ac.za
kabasob@cput.ac.za

**Abstract:** Signalling security is critical for next-generation mobile (NGN) networks to ensure integrity, privacy, and confidentiality of communication protocols. However, recent research on existing 5G standards has uncovered vulnerabilities that could be exploited by emerging surveillance threats such as HiddenArt and Harvest Now Decrypt Later (HNDTL), as well as the prospect of quantum computing threatening to break classical cryptographic techniques. This systematic literature review (SLR) investigates quantum-based signalling solutions to mitigate these threats in interconnect and roaming 5G networks (IRN) over IP eXchange for Narrowband Internet of Things (NB-IoT) traffic. A database search was conducted, studies were selected and compared based on methods, approaches, techniques, and limitations. The SLR found that quantum key distribution (QKD) combined with quantum teleportation (QT) can protect and mitigate threats and attacks on signalling networks when protocols interact and interoperate in carrier networks. QKD techniques can be used for L1 protocols, while secure direct quantum communication can be used for L2 protocols. This study concludes that further studies are needed to integrate different techniques and protocols for L1/L2 signalling networks to create a robust quantum-secure signalling model for global interconnect and roaming NGN.

**Keywords:** Quantum teleportation, Quantum cryptography, Interconnect and roaming, NB-IoT, L1/L2 Signalling, Next-generation networks

## 1. Introduction

Signalling security is critical for the NGN to ensure integrity, privacy, and confidentiality of communication protocols (ITU-T, 2021). Signalling, the mechanism used to control network communications and network management, serves as a crucial attack surface for misuse and unauthorized access in wireless and mobile telecommunications (ITU-T, 2021). It also serves as the primary source of network intelligence, analytics, and user behaviour monitoring (Baraković Husić et al., 2012). Exploiting mobile signalling infrastructure can turn the network into a tool for cyber warfare when used by malicious actors (COTS Staff, 2023). Additionally, emerging threats like HNDTL often goes undetected in current L1 signalling networks (Garcia Cid et al., 2022; Cho, 2019). ENEA (COTS Staff, 2023) describes signalling security in mobile communications as a systematic blind spot, emphasising the need for improvements in IRN Signalling security. Roaming enables Mobile Network Operator (MNO) to access services remotely through Visited Public Mobile Networks (VPMN) from their Home Public Mobile Network (HPMN) (GSM Association, 2021). To use VPMN services, a roaming agreement between HPMN and VPMN is essential, with standardized commercial procedures (GSMA, 2020; Lutu, Perino, et al., 2021). Signalling security in the context of IPX pertains to vulnerabilities in telecommunication protocols used for roaming interworking (ENISA, 2018). With the increasing deployment of commercial and industrial Internet of Things (IoT) devices, the need for permanent roaming connectivity is growing (Lutu, Trevisan, et al., 2021).

The advent of 5G represents the NGN, featuring enhanced usecases such as higher bandwidths, lower latencies, and higher communications (C. Yu et al., 2021; ITU-R, 2015; Manzalini, 2020). The adoption of IoT over 5G, specifically 5G NB-IoT, offers cost-effective, low-rate data connectivity (Tan et al., 2022). Additionally, outlines that a significant portion of IoT applications are expected to run on NB-IoT deployment mode by the end of 2025. However, enhanced usecases introduce security challenges that traditional cryptographic solutions cannot effectively address due to stringent latency requirements (Djordjevic, 2022; Dutta, 2022). The abuse of telecommunications infrastructure by surveillance spyware further exacerbates the challenges faced by IRN signalling traffic (Holtrup et al., 2021). The United Nations recognizes the importance of security in connectivity and communication as a human right (United Nations, 2016). To address these critical issues, the International Telecommunication Union (ITU) organized a workshop aimed at improving signalling protocol security (ITU-T, 2021). MNOs have also underscored the importance of secure interconnection protocols, such as Security Edge Protection Proxy (SEPP) for 5G roaming (Intelligence & IBASIS, 2020). The challenges facing NGN's IRN underscore the necessity of secure communication protocols to address threats such as quantum computing, HNDTL, eavesdropping, interception, and key exchange difficulties in control plane signalling and user data traffic. Quantum communication (QC) offers a solution to these challenges as it is immune to tampering, eavesdropping, and interception communication (Pirandola et al., 2015; Asfaw et al., 2022). Implementing unconventional protocols in the IRN can improve signalling security for the NGN over IPX, providing enhanced

security for roaming subscribers. In this study, we explore the pressing need for improved signalling security in NGN, the challenges faced, and promising solutions, including the use of QC to enhance the security of roaming subscribers in NGN over IPX for NB-IoT traffic.

## 2. Related Work

The literature reveals critical concerns within the realm of mobile network security and highlights the inadequacies in addressing these issues. Notably, it is emphasized that MNOs have not given sufficient attention to security within the IRN signalling interfaces (Køien, 2021; Tezergil & Onur, 2021). In addition, the transition to IP-based transport networks is deemed unreliable and lacking Quality of Service (QoS) guarantees (Baraković Husić et al., 2012). The absence of end-to-end security, integrity protection, and encryption in signalling further exacerbates security vulnerabilities (Tan et al., 2022; You et al., 2021). As 5G technology evolves, it faces challenges related to ensuring high computing and communication requirements, ultimately impacting QoS (You et al., 2021; Køien, 2021). Consequently, there is a pressing need to address these security issues to safeguard both subscribers and the networks (Abdel Hakeem et al., 2022). Furthermore, the literature underscores the necessity for continuous development and improvement in security measures for mobile networks, as advocated by 3GPP, including enhancing the security of both control and user plane signalling messages (Abdel Hakeem et al., 2022; Garzon et al., 2022; Køien, 2021).

The emerging 5G technology poses unique vulnerabilities that require novel approaches and technologies for mitigating security risks (Kim, 2020; Chih-Lin et al., 2016). In light of these concerns, the integration of quantum-based technologies, particularly Quantum Communication (QC) and Quantum Cryptography (QCrypt), is presented as a promising avenue for addressing these security challenges (Wang et al., 2020). QC offers unconditional security, as eavesdropping attempts are detectable, making it a valuable asset in safeguarding data transmission (Ngobeni et al., 2020; Djordjevic, 2022). However, as quantum-assisted crypto analysers pose a new threat, the security community must focus on devising post-quantum techniques and standardized security protocols (Suomalainen et al., 2018). While the literature covers various aspects of quantum-based technologies, it underscores the lack of quantum-based signalling models for interconnect and roaming networks over IPX, emphasizing the significance of developing a comprehensive quantum-based signalling model for NB-IoT traffic over IRN. In summary, the literature highlights the pressing security challenges faced by NGN, particularly in the context of 5G technology. The inadequacies in addressing these issues have spurred the exploration of quantum-based solutions to enhance the security of signalling interfaces and roaming networks over IPX, aiming to create robust signalling L1/L2 models against evolving threats.

## 3. Research Aim and Objectives

This research aims to find existing quantum-based security solutions for protecting L1/L2 signalling traffic in the IRN over IPX and compare them in terms of approach, method, technique, and constraints. The main objectives are:

- To review existing body of knowledge on quantum-based security solutions to protect interconnect and roaming signals.
- To review how the identified quantum-based signalling solutions compare with each other in terms of technology, technique, approach, methods, and constraints.
- To identify strength of evidence supporting the various quantum-based signalling techniques and how they can be best applied to develop a secure signalling model, and
- To outline the implications of the research to explore new ideas and possibilities.

## 4. Methodology

SLR was adopted with features of the PRISMA statement (Moher et al., 2009) and followed the process outlined by (Okoli, 2015). SLR is a beacon of clarity that provides a rigorous and transparent methodology for synthesising existing research. This study argues that SLR stands out among other research methodologies for its unique ability to provide unbiased, repeatable, comprehensive, and cumulative evidence.

### 4.1 Review Protocol

The research questions (RQs) posed for this review are: *RQ1*: What existing quantum-based security solutions have been developed for NGN-enabled NB-IoT traffic?, *RQ2*: How do the various quantum-based signalling solutions found in answer to RQ1 differ in terms of technology, technique, approach, method, and limitations?, *RQ3*: How strong is the evidence in support of the different quantum-based signalling security solutions? and

*RQ4*: What are the potential implications of these findings of the research when developing a new quantum-based signalling security solution for NGN-enabled IoT over IPX?

### 4.2 Search Query

For comprehensive and relevant SLR, we were in favour of curated databases such as IEEE Xplore, arXiv, ScienceDirect, ProQuest and ACM Digital Library. They offer precise searching, trustworthy research and seamless analysis tools to drive research forward. Search terms applied: quantum* AND (communication OR teleportation OR entanglement OR QKD) AND (roaming OR interconnect OR security OR "physical layer" OR "data link Layer" OR "L1/L2" OR L1 OR L2) AND (mobile OR wireless OR IoT OR IPX). All searches conducted from the period of 2018 to 2023.

### 4.3 Study Selection

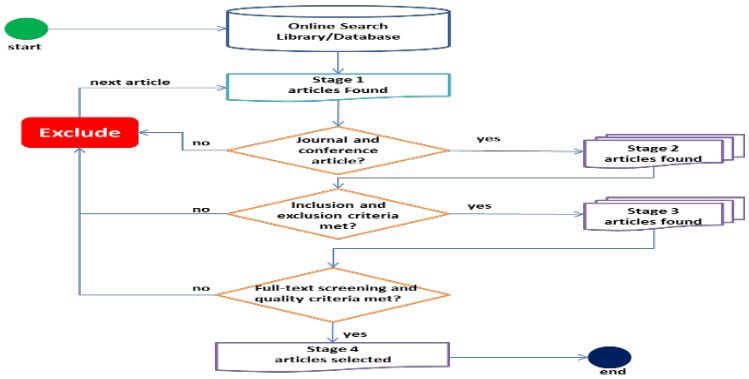


**Figure 1: Execution process**

Figure 1 outlines the primary study protocol, which includes four main stages: the initial search, the identification of relevant literature, the application of inclusion and exclusion criteria, and a quality assessment. The review aims to identify the current state of knowledge in the field of quantum-based signalling security, which includes disciplines such as quantum communication, quantum mechanics, computer science, and information and communication technology (ICT).

*Inclusion criteria*:

- Peer-reviewed empirical studies obtained online and open access.
- Empirical studies with advances in quantum security for NGN's IRN.
- Studies that evaluate the security, effectiveness, or scalability of quantum communication.

*Exclusion criteria:*

- Articles not related to quantum communication and not addressing L1/L2 WAN protocols.
- Studies not written in English, and studies before 2018.

### 4.4 Quality Assessment (Qa) Criteria

We followed a peer-reviewed journal articles and conference proceedings. Each paper has been carefully assessed to ensure quality. The study's abstract, methodology and conclusion were reviewed for applicability and quality. The quality score indicated by 1 for agree, 0.5 partial and 0 disagree, any score less than 6 out of 10 is rejected. Table 1, shows the questions used for the QA.

**Table 1: Quality Assessment Questions**

| Qua# | Quality Assurance Questions |
|---|---|
| **Q0** | Is the aim of this research study clearly stated? |
| **Q1** | Is the quantum security method and approach clearly defined? |
| **Q2** | Is the transmission technique and algorithm used clearly defined? |
| **Q3** | Does the protocol support L1/L2 WAN infrastructure? |
| **Q4** | Does the study address interconnect and roaming or IPX? |
| **Q5** | Is the data collection procedure relevant for L1/L2 security? |

| Qua# | Quality Assurance Questions |
|---|---|
| **Q6** | Does the results and findings contribute to signalling security? |
| **Q7** | Are the limitations specified? |
| **Q8** | Is it a repeatable research methodology? |
| **Q9** | Does study contribute to the telecommunications? |

### 4.5 Data Extraction Form

**Table 1: Data Extraction Form**

| Variables | Purpose |
|---|---|
| **SID** | to uniquely identify the study for the article |
| **Authors** | to represent the article authors |
| **Title** | to capture the title/topic of the research article/journal |
| **Year** | to capture publication year |
| **OSI layer** | to indicate which OSI layer used L1/L2 |
| **Quantum Approach** | Quantum communication Approach applied |
| **Quantum Technology** | Physical implementation used |
| **Quantum Technique** | Quantum method/technique applied |
| **Method/Protocol** | to indicate the protocol used |
| **WAN infrastructure** | WAN infrastructure supported (Optical, Freespace, Satellite, etc.) |
| **Quality of Evaluation** | Evaluation score (out of 10) |
| **Strengths** | to capture article strength |
| **Weaknesses** | to capture articles weakness |
| **Gap** | To identify a gap or gaps in the study |

### 4.6 Data Synthesis

The data collected was not statistically analysed. However, the selected study in this report presents key facts using a narrative and tabular format. Combining narrative and tabular formats is an effective strategy to achieve a comprehensive and impactful presentation. Our choice is guided by the research objectives, QA criteria and target audience. Since clarity, accessibility and engagement are paramount, narrative and tabular formats offer valuable advantages over purely statistical formats.

## 5. Findings and Discussion

RQ1: What existing quantum-based signalling security solutions have been developed for NGN-enabled NB-IoT traffic?

**Table 2: Process Results [2018-2023]**

| Stage | Description | Studies# | Excluded |
|---|---|---|---|
| **0th** | Online library/database search | 2708 | - |
| **1st** | Filter by Journal or article | 134 | 2574 |
| **2nd** | Filter by Inclusion, exclusion criteria | 92 | 42 |
| **3rd** | Full text gathered | 59 | 33 |
| **4th** | Selected study | 13 | 46 |

To answer the research questions, the studies were briefly summarised using a yearly breakdown, see Fig. 2.

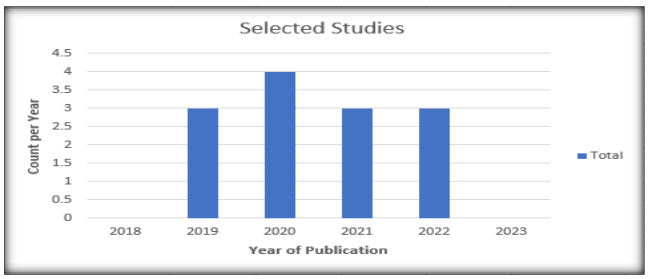


**Figure 2: Publication on quantum-based security solutions**

In this review, 13 key studies were selected. Several quantum-based communication solutions in the literature were examined, which encompasses aspects of the development and application of quantum communication technologies. The selected studies have been given an identifier (SID) followed by citation e.g S#[<ref>] as follows: S1(Kozlowski et al., 2020), S2(Abulkasim et al., 2019), S3(Chen et al., 2020), S4(Khawasik et al., 2022), S5(Li et al., 2019), S6(Li et al., 2022), S7(Lou et al., 2019), S8(Ntanos et al., 2021), S9(Pan et al., 2020), S10(N. Yu et al., 2021), S11(Zimmer et al., 2021), S12(Tanizawa & Futami, 2020), S13(Tanizawa & Futami, 2022). Four categories were identified and divided into quantum cryptography, quantum teleportation, quantum networks and other areas of quantum communication. All these studies contribute to the advancement of quantum communication and provides new insights into the challenges and opportunities. The studies have various level of application in terms of open system interconnection (OSI) physical layer (L1) and datalink layer (L2) categorised in terms of techniques and protocols on how they lead to signalling security enhancements for L1 and L2 as:

*OSI L1*:

- Quantum cryptography (Qcrypt) uses quantum mechanics principles to secure communication, considered more secure as it's impossible to eavesdrop without being detected. It can authenticate devices, encrypt signalling traffic and create secure key exchange: *S4, S8, S9, S12, S13.*
- Quantum teleportation (QT) uses quantum entanglement to transfer the quantum state to other locations. This can be used to protect signalling messages by ensuring that it cannot be intercepted or modified in transit: *S3.*
- Quantum networks (QN) uses quantum technologies to transmit and process information. This can be used to protect signalling messages by providing a secure and reliable communication channel: *S1, S3, S6, S10, S11.* Other quantum communication protocols *S2, S5 and S11.*

*OSI L2*:

- Quantum secure direct communication (QSDC) allows two parties to communicate directly without need for a shared key using QT. This can be used to protect signalling on OSI L2 by ensuring signalling messages cannot be intercepted or eavesdropped: *S5* and *S9*.
- QN's security of signalling using packet level quantum network intercommunication: *S10.*
- Quantum signature allows two parties to sign messages in a secure manner, this can be used to protect the authenticity and integrity of signalling messages using Qcrypt: *S7* and *S13*.
- Quantum arbitration allows two parties to reach an agreement on a value in a secure manner, this can be used to protect the fairness of signalling messages using QT: *S13*. Studies have been classified based on approach and exact area in which the study was conducted, table III.

**Table 3: Selected Studies and Classifications**

| Studies (SID) | Approach |
|---|---|
| S4, S5, S8, S12, S13 | Quantum Cryptography |
| S3, S7, S9 | Quantum Teleportation |
| S1, S6, S10 | Quantum Networks |
| S2, S11 | Other areas Quantum Communication |

*RQ2: How do the various quantum-based signalling solutions found in answer to RQ1 differ in terms of technology, technique, approach, method, and limitations?*

This question aimed to explore, identify and compare the commonly used quantum technology, techniques, methods, and protocols for secure signalling in OSI L1/L2. The analysis revealed that the application of quantum communication approaches, techniques, methods, and protocols has the potential to significantly enhance signalling security in these layers. However, a notable gap exists in terms of interoperability and standardization, hindering seamless interaction of these protocols within carrier networks. Many methods and protocols are still in the experimental stage and have not been field-tested, primarily due to their complexity, high cost, and hardware compatibility issues, limiting their adoption in current telecommunications. Some interesting findings include the discovery of quantum arbitration and quantum secure signature studies that contribute to QC. While most studies rely on QKD through Qcrypt, others combine aspects of QKD and QT. However, a lack of standardization for interoperability and interconnectivity poses challenges for IRN over IPX. Security concerns related to distance, technical challenges, attenuation, and the no-cloning theorem for quantum repeaters and communication networks were identified. Despite the promise of QT, it still faces challenges such as freespace losses and decoherence. One practical quantum technology suitable for wide area network (WAN) infrastructure is Photonic qubits, which spans various classifications, followed by optical modes. Additionally, a noteworthy development is the "Quantum noise-assisted coherent radio-over-fiber cipher system" that employs quantum noise to encrypt radio signals, providing protection for signalling messages transmitted over radio waves. Summary is outlined in table 5 below:

**Table 4: Quantum-based signalling comparisons**

| Quantum Technology | Quantum Technique | SID# | Quantum Method/Protocol | Limitations |
|---|---|---|---|---|
| Photonic Qubits | Quantum Cryptography | S4, S5 S8, S12, S13<br>Related studies (S1, S2, S10, and S11) | Continuous-variable QKD, Discrete-variable QKD, Hybrid QKD (entanglement-based), CV-DV QKD which can be based on BB84, Ekert91, BM92, DQKD protocol. | *Security:* limited distance, technical challenges, and atmospheric attenuation. *Interoperability: L1/L2* different standards, and integration complexity.<br>*Implementation:* High complexity, costs, environmental sensitivity, and low-key exchange |
| Photonic Qubits,<br>Optical Modes, Trapped Ions, Superconducting Circuits | Quantum Teleportation | S3, S7, S9 | QSDC protocol based on Hyper-entangled states,<br>Two-step QDC scheme,<br>DL04 protocol,<br>CV-AQS,<br>DQSDC,<br>Q2BC | *Security:* Entropy, eavesdropping risk, losses: Free-Space, attenuation, decoherence. *Interoperability: L2* Standards mismatch, relies on complex quantum channel. *Implementation:* Detector efficiency for small photons, quantum channel noise, distance limits, regulations, distance limits, deployment costs. |
| Photonic qubits,<br>Optical Modes | Quantum Networks | S1, S6, S10<br>Related studies (S2, S9, S11, and S12) | Quantum repeaters, Quantum Key Networks, Quantum internet, PQNI<br>Entangled pairs, Hybrid CV-DV QCN, Hybrid QCN, Hybrid QKD (entanglement-based), QNP using Connection-Oriented entanglement distribution protocol. | *Security:* attack risk during node repeater decryption, distance limits, and technical issues, atmospheric attenuation, No-cloning theorem, quantum noise and distance.<br>*Interoperability: L1/L2*<br>Standardisation, compatibility for multiple protocols and hardware. *Implementation:* Lab development challenges, high costs, scalability issues, entanglement fragility, incomplete quantum repeater development. |
| Photonic qubits,<br>Optical Modes | Other QC's | S2, S11 | Quantum arbitration,<br>Quantum signature | *Security:* technical challenges<br>*Interoperability: L2*<br>Standardisation, compatibility for multiple protocols<br>*Implementation:* Complexity |

In table 5 a greater attempt to identify most used quantum technology, quantum techniques, Method and protocol for secure signalling approaches also taking into an account the constraints while analysing the details

of preselected papers was undertaken. Our extensive analysis of the studies demonstrates that application of QC approaches with their various techniques, methods and protocols can significantly improve signalling security on L1/L2. However, there seems to be gap within interoperability and intercommunication for the protocols, there exists multiple approaches which have not been standardized for interoperability when protocols interact in carrier networks. Further investigation of the literature as categorised in RQ1 found that extensive research demonstrate that multiple methods and protocols are still being developed and tested in the laboratory with no deployment. We also found that the physical implementation for these approaches and techniques in the field are complex, costly, and not compatible with multiple hardware. This will make them not to be a best candidate for adoption in the current telecommunications domain. Interesting aspects of quantum arbitration and quantum secure signature were discovered in studies (Abulkasim et al., 2019) and (Li et al., 2019). These studies do not actually form part of Qcrypt nor QT however they are part of QC. Most studies rely on Qcrypt through QKD, while others mainly focused on QN combining both aspects of QKD and QT. These studies have one common factor lack of standardization for interoperability and interconnectivity which further widens the gap for IRN over IPX. Another aspect of security which was identified is the various levels of attack that may arise due to distance, technical challenges, attenuation and the no-cloning theorem for quantum repeaters and communication networks. QT though looks promising it still suffers from freespace losses and decoherence. The most practical quantum technology identified across wide area network (WAN) infrastructure has been Photonic qubits, that managed to cut across the four classifications followed by optical modes. The last interesting aspect of quantum signalling is the "Quantum noise-assisted coherent radio-over-fiber cipher system" which uses quantum noise to encrypt radio signals. This can be used to protect signalling messages that are transmitted over radio waves *S12, S13.*

*RQ3: How strong is the evidence in support of the different quantum-based signalling security solutions?*

**Table 5: Strength of evidence**

| Method/ Protocol | Strengths | Constraints/Limitations |
|---|---|---|
| **CV-QKD** | High key rates, Compatible with existing telecom infrastructure, robust to noise and scalable. | Comple data processing,<br>Less mature technology,<br>Susceptible to certain attacks e.g., Photon splitting attack, requires high-quality components. |
| **DV-QKD & DQKD** | Proven security, tolerance to noise, efficient key generation, well-established technology. Efficient modulation scheme, less susceptible to noise and interference. | Single-photon detectors, less compatible with existing technology infrastructure, splitting attacks vulnerability, complex modulation schemes. |
| **Hybrid CV-DV QKD** | Larger number of entangled states, tolerant to noise, more secure and versatile. Serve as backbone for quantum Internet. | Less mature technology, more complex difficult to implement and deploy, high-quality components, less efficient to DV-QKD. |
| **QSDC** | Uses hyper entangled states, Bell states for secure transmission, secure information without key generation or sharing, present-day linear optics measurement, realized for practical applications, facilitate interconnection of QCN | Noisy quantum channels vulnerable,<br>Relies on quantum memory, less mature technology, more complex, expensive equipment |
| **DQSDC** | Deterministic, unconditionally secure, high key rates and simple to implement | Less efficient than QSDC and BB84, complex, requires entanglement, vulnerable to noise |
| **CV-AQS** | Uses arbitrator and verifier, Signature cannot be denied or forged. Use dense coding and teleportation. Can be used on lossy and lossless channel, security by two-mode squeezed vacuum state teleportation. Scalable, compatible with existing telecommunication infrastructure. | Complex data processing, less mature technology, susceptible to photon number splitting attack, high-quality components |
| **DL04** | Discrete-variable (DV) Proven security, efficient and robust to noise, simple implement. Continuous-variable (CV) does not require entanglement, robust to noise, efficient and scalable | Requires entanglement, collective attack, difficult to scale. Not provably secure, gaussian attack, not fully implemented |
| **Q2BC** | BB84 protocol with proven security, robust to noise and simple to implement. | Requires entanglement, collective attack, difficult to scale. Not provably secure, gaussian attack, not fully implemented |

| Method/ Protocol | Strengths | Constraints/Limitations |
|---|---|---|
| **PQNI** | Supports quantum packet communication, robust to noise, scalable and secure against eavesdropping | Requires entanglement, complex and expensive, not yet fully developed, denial of service attacks |
| **Quantum repeaters** | data plane network using virtual circuits on link layer protocol. Scalability and flexibility, resilient to noise and extends distance of QC | limited implementation for control plane protocol.<br>Requires entanglement, denial of service attacks, not fully developed, complex and expensive. |

In Table 6, an important consideration is the choice of QC method/protocol. Which method is most appropriate depends on several factors, including the required key rates, the distance between nodes and the level of security required. Promising methods/protocols include CV-QKD, Hybrid CV-DV QKD, CV-AQS, QSDC and quantum repeaters. Another important consideration is the interoperability of the chosen method/protocol with the existing telecommunications infrastructure. This is particularly important in the context of IRN, which often involves multiple operators and a variety of systems and networks. The chosen method/protocol must also be able to operate at both L1/L2 (i.e. the physical and data link layers) to send and receive raw data over the physical network infrastructure.

*RQ4: What are the potential implications of these findings of the research when developing a new quantum-based signalling security solution for NGN-enabled IoT over IPX?*

This question focused on the potential implications of QC methods and protocols for the development of a new quantum-based signalling security solution for IRN over IPX. The choice of method/protocol for this application depends on key factors such as required key rates, node distance, and security levels. Strengths to consider include compatibility with existing infrastructure, interference robustness, scalability, and security. Limitations involve complexity, cost, and technology maturity. The table analysis suggests several suitable methods/protocols. CV-QKD is compatible with existing infrastructure and robust but less mature. Hybrid CV-DV QKD offers enhanced security but is complex and less mature. QSDC is highly secure but costly and complex. CV-AQS is scalable and compatible but less mature. Quantum repeaters could extend range but are in early development stages. The choice depends on specific network requirements, making a careful evaluation of strengths and limitations is essential. Given the complexity and multiple operators in IRN networks, interoperability across systems in OSI L1/L2 is crucial. The selected method/protocol should operate on both layers to handle raw data over the physical network. Developing a quantum-based signaling security model for IRN over IPX at OSI L1/L2 is challenging but provides unprecedented level of security. In summary the study contributes following insights:

- Quantum-based signalling security approaches, techniques, methods/protocols studied, compared, and presented.
- The advantages of quantum-based signalling techniques are highlighted.
- The quantum-based technology strengths and limitations are highlighted.
- Performance and security based on distance for different QC methods/protocols in the context of IRN are presented.

Lastly, signalling security gaps are identified, and future research directions for enhanced protection of IRN over IPX are discussed.

## 6. Threats to Validity

Conducting a SLR has risks, especially in rapidly evolving fields like quantum-based secure signalling. We mitigated these risks by defining precise search criteria and using logical operators to broaden our search scope across identified impactful databases. We focused on articles from 2018 to 2023, ensuring our review represents the current state of quantum-based secure signalling for IRN over IPX at OSI L1/L2 covering NB-IoT. While the risk of missing unpublished papers exists, we believe our chosen databases are comprehensive and respected in the field and our RQ presents current knowledge and recent developments in QC. Our rigorous approach increases the validity and reliability of our review, we believe we took reasonable steps in minimizing associated risks.

## 7. Conclusion

In this review, we focused on quantum-based secure signalling solutions for NGN-enabled NB-IoT traffic, evaluating their approaches, methods, and limitations. Our comprehensive analysis involved 13 studies that met our selection criteria. These quantum-based solutions are still in their infancy, therefore not ready for widespread use. They leverage QC techniques and protocols to enhance signalling security at the OSI L1/L2 layers, offering protection against emerging threats like quantum cryptanalysis, HiddenArt, and HNDTL. Nevertheless, they come with challenges. Issues related to interoperability and intercommunication can leave networks vulnerable to side-channel and physical attacks. High implementation costs and compatibility concerns with existing hardware restrict their adoption. Additionally, the lack of standardized protocols for interoperability across operator networks hinders broader adoption. Signalling protocols play a crucial role in ensuring seamless interconnection, particularly for securing roaming signals and subscribers in the context of IRN over IPX, which has become increasingly vital for global infrastructure. Developing quantum-based security solutions requires a unique blend of expertise, encompassing roaming experience, cyber-security skills, and quantum computing knowledge. This is essential to create a model that can secure the IPX-IRN ecosystem for NGN networks like 5G. While quantum technologies have been extensively studied across various fields, a significant gap exists in developing quantum models tailored for the integrated and standardized nature of signalling interconnect and roaming L1/L2 networks over IPX to secure roaming traffic. Our study is one of the initial efforts to address this gap by systematically reviewing quantum approaches, methods, and protocols to create a quantum-based signalling model for IRN over IPX, particularly for NB-IoT traffic. This is crucial, as these networks underpin critical infrastructure, including power grids, health systems, and financial markets, making them susceptible to unconventional surveillance threats.

## 8. Future Directions

Future research should focus on evaluating the performance and security of QC methods in IRN, customizing methods for IRN needs, creating interoperable models for seamless protocol interaction, and standardizing quantum protocol operation on OSI L1/L2. Developing a secure quantum-based signalling model for IRN to enhance OSI L1/L2 signalling security over IPX for NB-IoT.

## References


Abdel Hakeem, S.A., Hussein, H.H. & Kim, H. 2022. Security Requirements and Challenges of 6G Technologies and Applications. *Sensors*, 22(5).

Abulkasim, H., Alsuqaih, H.N., Hamdan, W.F., Hamad, S., Farouk, A., Mashatan, A. & Ghose, S. 2019. Improved Dynamic Multi-Party Quantum Private Comparison for Next-Generation Mobile Network. *IEEE Access*, 7: 17917–17926.

COTS Staff. 2023. Enea Urges EU PEGA Committee: Broaden the focus beyond spyware to combat mobile surveillance threats and signaling infrastructure exploitation. – COTS Journal. https://www.cotsjournalonline.com/index.php/2023/05/16/enea-urges-eu-pega-committee-broaden-the-focus-beyond-spyware-to-combat-mobile-surveillance-threats-and-signaling-infrastructure-exploitation/?utm_campaign=Signalling%20Firewall&utm_medium=email&_hsmi=259452321&_hsenc=p2ANqtz-_B7VNxlP2rskn0onouuyW6vgqdGKilYLEcaGJwnJRtXTSePiyPM7Vf8mGbwlh4JHGKvwmchYq11Qzs7hKLqozlMxCx1g&utm_content=259452321&utm_source=hs_email 23 May 2023.

Asfaw, A., Blais, A., Brown, K.R., Candelaria, J., Cantwell, C., Carr, L.D., Combes, J., Debroy, D.M., Donohue, J.M., Economou, S.E., Edwards, E., Fox, M.F.J., Girvin, S.M., Ho, A., Hurst, H.M., Jacob, Z., Johnson, B.R., Johnston-Halperin, E., Joynt, R., Kapit, E., Klein-Seetharaman, J., Laforest, M., Lewandowski, H.J., Lynn, T.W., McRae, C.R.H., Merzbacher, C., Michalakis, S., Narang, P., Oliver, W.D., Palsberg, J., Pappas, D.P., Raymer, M.G., Reilly, D.J., Saffman, M., Searles, T.A., Shapiro, J.H. & Singh, C. 2022. Building a Quantum Engineering Undergraduate Program. *IEEE Transactions on Education*.

Baraković Husić, J., Bajrić, H. & Baraković, S. 2012. Evolution of Signaling Information Transmission. *ISRN Communications and Networking*, 2012: 1–9.

Chen, N., Shuai, S., Yan, B., Xu, N. & Pei, C. 2020. Multi-hop quantum communication based on greenberger-horne-zeilinger states and teleportation. *IEEE Access*, 8: 52052–52061.

Chih-Lin, I., Han, S., Xu, Z., Sun, Q. & Pan, Z. 2016. 5G: rethink mobile communications for 2020+. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2062): 20140432. https://royalsocietypublishing.org/doi/10.1098/rsta.2014.0432.

Cho, J.Y. 2019. Securing optical networks by modern cryptographic techniques. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11875 LNCS: 120–133. https://link.springer.com/chapter/10.1007/978-3-030-35055-0_8 23 August 2023.

Djordjevic, I.B. 2022. Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography. *Entropy 2022, Vol. 24, Page 935*, 24(7): 935. https://www.mdpi.com/1099-4300/24/7/935/htm 25 March 2023.

Dutta, A. 2022. 5G and Beyond Security Challenges and 5G & Beyond : Security Perspective. *Johns Hopskins University*. https://nsf-nextg-security.cs.ucsb.edu/sites/default/files/2020-11/Ashutosh Dutta.pdf.

ENISA. 2018. Signalling Security in Telecom SS7/Diameter/5G. *European Union Agency for Network and Information Security*, (March): 1–30. www.enisa.europa.eu.

Garcia Cid, M.I., Álvaro González, J., Ortíz Martín, L. & Del Río Gómez, D. 2022. Disruptive Quantum Safe Technologies. *ACM International Conference Proceeding Series*. https://dl.acm.org/doi/10.1145/3538969.3544484 23 August 2023.

Garzon, S.R., Yildiz, H. & Küpper, A. 2022. Towards Decentralized Identity Management in Multi-stakeholder 6G Networks. http://arxiv.org/abs/2203.00300.

GSM Association. 2021. *5GS Roaming Guidelines*. https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v2.0.pdf 19 August 2021.

GSMA. 2020. *GSM Association Non-confidential Official Document IR.67-DNS Guidelines for Service Providers and GRX and IPX Providers DNS Guidelines for Service Providers and GRX and IPX Providers Copyright Notice Antitrust Notice GSM Association Non-confidential Offic*.

Holtmanns, S. 2016. Interconnection Security Standards - We Are All Connected. *Journal of ICT Standardization*, 4(1): 1–18. https://riverpublishers.com/journal_read_html_article.php?j=JICTS/4/1/1 27 November 2021.

Holtrup, G., Lacube, W., Dimitri, ;, David, P., Mermoud, A., Gérôme Bovet, ; & Lenders, V. 2021. 5G System Security Analysis.

Intelligence, K. & IBASIS. 2020. *5G ROAMING: MNO REQUIREMENTS & OPPORTUNITIES*. https://ibasis.com/wp-content/uploads/2020/05/5G-Roaming_-_IPX_Requirements__Opportunities.pdf.

ITU-R. 2015. IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond M Series Mobile, radiodetermination, amateur and related satellite services. *Recommendation ITU-R M.2083-0*, (September 2015): 1–21. http://www.itu.int/ITU-R/go/patents/en 11 August 2022.

ITU-T. 2021. ITU Workshop on 'Improving the security of signalling protocols'. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1129/Pages/default.aspx 17 September 2022.

Keller, R., Castellanos, D., Sander, A., Robison, A. & Abtin, A. 2021. THE 5G SYSTEM ROAMING ARCHITECTURE. *Review*: 1–36. https://www.ericsson.com/4981f6/assets/local/reports-papers/ericsson-technology-review/docs/2021/roaming-in-the-5g-system.pdf 24 October 2021.

Khawasik, M., Elsayed, W., Rashad, M. & Younes, A. 2022. A Secured Quantum Two-Bit Commitment Protocol for Communication Systems. *IEEE Access*, 10: 50218–50226.

Kim, H. 2020. 5G core network security issues and attack classification from network protocol perspective. *Journal of Internet Services and Information Security*, 10(2): 1–15.

Køien, G.M. 2021. On Threats to the 5G Service Based Architecture. *Wireless Personal Communications*, 119(1): 97–116. https://doi.org/10.1007/s11277-021-08200-0 27 August 2021.

Kozlowski, W., Dahlberg, A. & Wehner, S. 2020. Design-ing a Quantum Network Protocol. *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, 16. https://doi.org/10.1145/3386367.3431293 26 March 2023.

Li, J., Jia, Q., Xue, K., Wei, D.S.L. & Yu, N. 2022. A Connection-Oriented Entanglement Distribution Design in Quantum Networks. *IEEE Transactions on Quantum Engineering*, 3.

Li, J., Zhou, Z., Wang, N., Tian, Y., Yang, Y.G. & Zheng, Y. 2019. Deterministic Quantum Secure Direct Communication Protocol Based on Hyper-Entangled State. *IEEE Access*, 7: 43948–43955.

Lou, X., Long, H., Tang, W., Yang, Y. & Li, J. 2019. Continuous-Variable Arbitrated Quantum Signature Based on Dense Coding and Teleportation. *IEEE Access*, 7: 85719–85726.

Lutu, A., Perino, D., Bagnulo, M. & Bustamante, F.E. 2021. Insights from operating an IP exchange provider. *SIGCOMM 2021 - Proceedings of the ACM SIGCOMM 2021 Conference*: 718–730.

Lutu, A., Trevisan, M., Safari Khatouni, A., Mandalari, A.M., Custura, A., Mellia, M., Alay, O., Bagnulo, M., Bajpai, V., Brunstrom, A., Ott, J. & Fairhurst, G. 2021. Measuring Roaming in Europe: Infrastructure and Implications on Users QoE. *IEEE Transactions on Mobile Computing*.

Manzalini, A. 2020. Quantum communications in future networks and services. *Quantum Reports*, 2(1): 221–232.

Moher, D., Liberati, Alessandro, Tetzlaff, J., Altman, Douglas G, Liberati, A & Altman, D G. 2009. Reprint-Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. http://www.annals.org/cgi/content/full/151/4/264. 12 August 2023.

Ngobeni, T., Kabaso, B. & Mukherjee, A. 2020. A generic framework for the implementation of a secure quantum teleportation infrastructure. *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2020 - Proceedings*.

Ntanos, A., Lyras, N.K., Zavitsanos, D., Giannoulis, G., Panagopoulos, A.D. & Avramopoulos, H. 2021. Leo satellites constellation-to-ground qkd links: Greek quantum communication infrastructure paradigm. *Photonics*, 8(12).

Okoli, C. 2015. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37(1): 879–910.

Pan, D., Li, K., Ruan, D., Ng, S.X. & Hanzo, L. 2020. Single-Photon-Memory Two-Step Quantum Secure Direct Communication Relying on Einstein-Podolsky-Rosen Pairs. *IEEE Access*, 8: 121146–121161.

Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S.L. 2015. Advances in Quantum Teleportation. *Nature Photonics*, 9(May): 641–652. http://arxiv.org/abs/1505.07831%5Cnhttp://www.arxiv.org/pdf/1505.07831.pdf.

Suomalainen, J., Kotelba, A., Kreku, J. & Lehtonen, S. 2018. Evaluating the efficiency of physical and cryptographic security solutions for quantum immune iot. *Cryptography*, 2(1): 1–20.

Tan, Z., Ding, B., Zhang, Z., Li, Q., Guo, Y. & Lu, S. 2021. Device-Centric Detection and Mitigation of Diameter Signaling Attacks against Mobile Core. In *2021 IEEE Conference on Communications and Network Security (CNS)*. IEEE. https://ieeexplore-ieee-org.ezproxy.cput.ac.za/document/9705031/ 15 August 2022.

Tan, Z., Ding, B., Zhao, J., Guo, Y. & Lu, S. 2022. Breaking Cellular IoT with Forged Data-Plane Signaling: Attacks and Countermeasure. https://doi.org/10.1145/3534124 15 August 2022.

Tanizawa, K. & Futami, F. 2022. IF-Over-Fiber Transmission of OFDM Quantum-Noise Randomized PSK Cipher for Physical Layer Encryption of Wireless Signals. *Journal of Lightwave Technology*, 40(6): 1698–1704.

Tanizawa, K. & Futami, F. 2020. Quantum Noise-Assisted Coherent Radio-Over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links. *Journal of Lightwave Technology*, 38(16): 4244–4249.

Tezergil, B. & Onur, E. 2021. Wireless Backhaul in 5G and Beyond: Issues, Challenges and Opportunities.

United Nations. 2016. The promotion, protection and enjoyment of human rights on the Internet. *Online Document*, 10802(December 2015): 1–4. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf 29 August 2022.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S. & Zhou, W. 2020. Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks*, 6(3): 281–291. https://doi.org/10.1016/j.dcan.2020.07.003.

You, X., Wang, C.X., Huang, J., Gao, X., Zhang, Z., Wang, M., Huang, Y., Zhang, C., Jiang, Y., Wang, J.J., Zhu, M., Sheng, B., Wang, D., Pan, Z., Zhu, P.P., Yang, Y., Liu, Z., Zhang, P., Tao, X., Li, S., Chen, Z.Z., Ma, X., Chih-Lin, I., Han, S., Li, K., Pan, C., Zheng, Z., Hanzo, L., Shen, X.S., Guo, Y.J., Ding, Z., Haas, H., Tong, W., Zhu, P.P., Yang, G., Wang, J.J., Larsson, E.G., Ngo, H.Q., Hong, W., Wang, H., Hou, D., Chen, J., Chen, Z.Z., Hao, Z., Li, G.Y., Tafazolli, R., Gao, Y., Poor, H.V., Fettweis, G.P. & Liang, Y.C. 2021. *Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts*. Science in China Press. https://www.researchgate.net/publication/347799507_Towards_6G_wireless_communication_networks_vision_enabling_technologies_and_new_paradigm_shifts 9 July 2021.

Yu, C., Chen, S., Wang, F. & Wei, Z. 2021. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. *Computer Networks*, 201: 108532.

Yu, N., Lai, C.Y. & Zhou, L. 2021. Protocols for Packet Quantum Network Intercommunication. *IEEE Transactions on Quantum Engineering*, 2.

Zimmer, P., Weinreich, R., Zenger, C.T., Sezgin, A. & Paar, C. 2021. Keys from the Sky: A First Exploration of Physical-Layer Security Using Satellite Links. *IEEE International Conference on Communications*.