International Scientific Journal of Engineering and Management ISSN: 2583-6129
Volume: 02 Issue: 04 | April – 2023 DOI: www.isjem.com
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

BQSAT: BLOCK QUANTUM COMPUTING FOR SECURE SATELLITE COMMUNICATION

M.Azhagupandi ,G.Govindharaj ,T.Kamalesh ,V.Manojkumar

Mrs.M.Vanitha (AP/CSE)

CSE & Selvam college of technology

Abstract - Satellite communication networks have - gained a lot of attention recently as a solution tomitigate the limitations of terrestrial networks such as stability and coverage. Due to satellitephysical constraints in terms of available power and area, data processing capacity is low, storage and security are limited such that the data may be vulnerable to tampering orcontamination by attackers. Since satellite communication has been more and more important in developing global communication networks, there have been concerns about the security insatellite communication.

***Key Words*:** Quantum Key Distribution(QKD), Quantum Key Pool (QKP),Ground Station, Blockchain

1.INTRODUCTION

A satellite is a body that orbits around another body in space. There are two different types of satellites – natural and man-made. Examples of natural satellites are the Earth and Moon. The Earth rotates around the Sun and the Moon rotates around the Earth. A man-made satellite is a machine that is launched into space and orbits around a body in space. Man-made satellites come in many shapes and size and have different pieces of instruments on them to perform different functions while in space.

1.1 Satellite Communication

Satellite communication is the method of transporting information from one place to another using a communication satellite in orbit around the Earth. Watching the English Premier League every weekend with your friends would have been impossible without this. A communication satellite is an artificial satellite that transmits the signal via a transponder by creating a channel between the transmitter and the receiver located at different locations on the Earth. Telephone, radio, television, internet, and military applications use satellite communications. Believe it or not, more than 2000 artificial satellites are hurtling around in space right above your heads.

1.2 Satellite Communications in India

It's interesting to know that the Indian National Satellite (INSAT) system is one of the largest domestic communication systems that is placed in the geo stational orbit. There are more than 200 transponders in the INSAT system and are used for various purposes such as telecommunications, weather forecasting, television broadcasting, disaster warning, search and rescue operations, and satellite newsgathering**.**

1.3 Cryptography

Cryptography provides for secure communication in the presence of malicious third-parties known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

1.4 Quantum-safe cryptography

The development of cryptographic algorithms, also known as post-quantum cryptography, that are secure against an attack by a quantum computer and used in generating quantum-safe certificates. The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key.

2. Blockchain Technology

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger. 'Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

2.1 Key elements of a blockchain

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks**.**

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more**.**

2.2 Types of Blockchain

All types of blockchains can be characterized as permissionless, permissioned, or both. Permissionless blockchains allow any user to pseudo-anonymously join the blockchain network (that is, to become "nodes" of the network) and do not restrict the rights of the nodes on the blockchain network. Conversely, permissioned blockchains restrict access to the network to certain nodes and may also restrict the rights of those nodes on that network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain. Blockchain Buzzwords Permissionless blockchains tend to be more secure than permissioned blockchains, because there are many nodes to validate transactions, and it would be difficult for bad actors to collude on the network.

3. LITERATURE SURVEY

[1] Eavesdropping Detection in BB84 Quantum Key Distribution Protocols-The nature of quantum mechanics provides us with an opportunity to statistically detect eavesdropping in quantum key distribution (QKD) protocols, which is unimaginable in classical digital communications. By utilizing Hoeffding's inequality, this study analyses the upper bounds of the false positive ratio (FPR) and false-negative ratio (FNR) of eavesdropping detection in the Bennett-Brassard-84 (BB84) QKD protocol, where eavesdropping is detected if the measured quantum bit error rate (QBER) is equal to or higher than a threshold. Proposed a simple eavesdropping detection algorithm that is highly compatible with the classical BB84 protocol. The algorithm judges the intercept-and-resend-attack from Eve by comparing the QBER and θ QBER . By exploring Hoeffding's inequality, we indicate the presence of a trade-off between the accuracy of eavesdropping detection and the economy of quantum resources. The upper bounds of the FPR and FNR of eavesdropping detection in the proposed algorithm exponentially decrease with respect to the increase in K In this study, the author developed simplified models and assumptions to provide straightforward analysis and intuition.

[2] Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices-Research on post-quantum cryptography aims to solve the problematic of modern public-key cryptography being broken by attacks coming from quantum computers in the future and, moreover, by using classical electronics. This task is so critical that the National Institute of Standards and Technology is in the final process of standardizing post-quantum schemes for the future protection of embedded applications. Though there are some research works done on embedded systems, it is important to study the impact of these proposals in realistic environments for the Internet of Things, where the limited computational resources and the strict requirements for power consumption can become incompatible with the usage of cryptographic schemes. In this work, the performance of one of the finalists of the standardization process called NTRU is studied and implemented in a custom wireless sensor node designed for applications in the extreme edge of the Internet of Things. The cryptosystem is implemented and evaluated within the processes of the Contiki- NG

ISSN: 2583-6129
www.isjem.com

operating system. Furthermore, additional experiments are performed to check if commonly integrated hardware peripherals for cryptography inside modern microcontrollers can be used to achieve better performance with NTRU, not only at single node level but also at network level, where the NTRU key encapsulation mechanism is tested in a real communication process.

[3] Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System - Quantum cryptography is a promising technology that achieves unconditional security, which is essential to a wide range of sensitive applications. In contrast to optical fibres, the free-space optical (FSO) link is efficiently used as a quantum channel without affecting the polarization of transmitted photons. However, the FSO link has several impairments, such as atmospheric turbulence and pointing errors, which affect the performance of the quantum channel. Paper Objective
This paper proposes a quantum key distribution (QKD) scheme that uses a time-bin entanglement protocol over the FSO channel that suffers from various channel impairments. Due to the interest in unmanned aerial vehicles (UAVs) and their usefulness for many social,
internet-of-things (IoT), civil, and military applications, the proposed QKD-FSO system is integrated with the ground-to-UAV platform. This work proposes an FSO system from Earth to UAV to satisfy on-demand services while achieving security requirements using the E91-QKD protocol. (1) develop an automatic correction-tracking system that minimizes the error-variance of tracking system between mobile UAV and fixed ground station; (2) introduce a QKD system over an optical free space channel applying time-bin with EBP considering a variety of channel impairments; (3) propose closed-form expressions of average-symbol error rate (ASER) and outage probability for UAV-based FSO communication link considering misalignment due to tracking errors
and non-zero boresight pointing errors; (4) obtain expressions of raw-key and secret-key rates to perform the security analysis and capacity of the QKD system.

4. Proposed System

There are essentially three types of orbits classified by the satellite altitude: geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO). Among them, GEO satellites are stationary relative to the earth's surface so that the Doppler shift is negligible and has a lower transmission outage probability than non-GEO satellites. The GEO satellites work at very high altitudes (≈35,786 km) and can offer the most extensive coverage. Thanks to the low outage probability and wide coverage, GEO satellites are preferred in our proposed protocol. Satellite communications systems enable the sending and receiving of information worldwide, offering internet access, television, telephone, radio, and other civilian and military operations. The advent of HTS (high-throughput satellite) systems has greatly enhanced technical capabilities and offered wideband services at lower costs. Significant improvements are expected on the forth coming mega-constellations in low Earth orbits that will deploy thousands of satellites, providing full earth coverage to minimize delays in addition to wide bandwidth. The use of satellites, given these characteristics, can increase efficiency in providing large sets of services and applications that are security-sensitive, such as telemedicine, banking, search and rescue, sensor networks, and content delivery network
feed. However, in many cases, the security of satellite communication has been seriously compromised, resulting in covert dangers. In satellite communications (and even in terrestrial systems), hackers can interfere, intercept, or modify wireless network systems remotely,
attack the equipment of flight crews, and control the positioning and transmission of satellite communication antennas. According to satellite communication protocols, the use of space in satellite communications can be developed independently to enhance communication security. Recommendations have been proposed to further increase the unity and compatibility of communication protocols for space. A single security mechanism is insufficient to meet the security requirements for satellite communication services. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyse the security of satellite communication networks in terms of access control, confidentiality, and security authentication.

4.1 Proposed Methodology

Blockchain Technology - In the case of GEO satellite network system, consortium blockchain would be more suitable in terms of architecture andvarious demands like being controllable an manageable. QC or QKD - Quantum Key Distribution (QKD),which provides

ISSN: 2583-6129
www.isjem.com

secure access Satellite to DPC.Ultra-secure QKD protocols are developed based on well-accepted laws that govern quantum physics for sharing secret keys among two parties. Cryptographic key material could be generated on demand between a ground station and a satellite (or between two satellites), allowing a satellite to be securely re-keyed on orbit for encrypting the uplinked command path and down linked data path. To distribute keys between widely-separated ground stations with a satellite relay, enabling encrypted communications over even inter-continental distances.

Quantum Key Generation and Distribution

KeyGen SatelliteOperator(SO1): To register Satellite Operator, DPCA selects an identity Satellite Operator Device Unique Features and distribute to Quantum RSA-based private-public key pairs (rBBA ∈ Z* q Pub BBA = r BBA ·G). KeyGen Satellite (SAT1): DPCA picks a unique identity IDα, a unique master key MKα, and Quantum RSA-based private-public key pairs (rα ∈ Z ∗ q , Pub SATVα = r α · G) for each Satellite,SAT α , where {α = 1, 2, · · · , n} and n is the total number of SAT to be registered

Evaluation Metrics

A.Read latency (RL)

Before we define read latency and how it is computed, it is important to differentiate between reading and transaction operations in the blockchain. The read operation refers to an internal mechanism that can be implicitly executed by a blockchain node to fetch the required data to verify specific transactions, but it does not update the blockchain status. On the other hand, a transaction is a state transition that updates data in the blockchain by adding a new block to the chain. Therefore, a transaction is explicitly executed by a blockchain node and verified using a blockchain protocol against a set of rules called a smart contract. If a transaction is valid, the blockchain system will commit the transaction and add a new block to the chain containing all details of this transaction. In our study, a transaction can be satellite communication or sensing of debris moving toward a constellation zone or satellite orbit. Therefore, the RL) is the time between when the read request is submitted by a satellite and when the response is received. Equation 1 formulates the RL calculation

RL = Response Time − Submission time

B. **Transaction latency (TL)**

It refers to a blockchain network-wide view of the amount of time taken for a transaction from creation to be available across the blockchain network. Equation 2 is used to compute the TL.

TL =Confirmation time @ network threshold − submission time

C.Read throughput (RT)

It is a measure of how many read operations are executed in a specified time interval,expressed as reads per second (RPS). Equation 3 is used to calculate RT

RT =∑ (Reads Operations) / ∑ (Times in seconds)

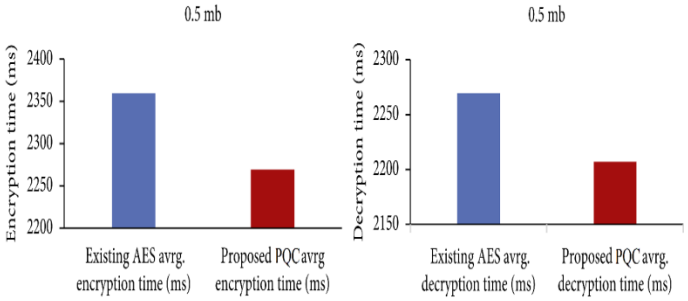
D.Transaction throughput (TT)

It is the rate at which valid transactions are executed by the blockchain system in a defined time interval. This is not the rate at a single blockchain node, but across the entire blockchain network. This rate is expressed as transactions per second (TPS) at a specified network size. Equation 4 is used to calculate TT

TT =∑ (Committed Transactions)/ ∑ (Times in seconds)

E.Encryption and Decryption Time

It presents the execution time test results in milliseconds (ms), which are attained by computing the average encryption/decryption time after encrypting/decrypting the input text in 0.5 MB sizes of the while using the same key run on 16, 32, 64, and 128 bytes. The results of Figures 7–9 specify that the existing AES has a minor rise in the encryption and decryption time after matched to the existing AES algorithm. grapg presents the time comparison between existing AES and different proposed PQC algorithms for a string key.



ISSN: 2583-6129
www.isjem.com

CONCLUSION

The satellite communication channel is different not only from the common mobile channel but also from the ground station channel. The satellite communication channel is the fusion of the satellite channel and the mobile communication channel. Satellite communication channels are extremely vulnerable to hackers and external interference signals. Protecting satellite networks from illegal information access and use can be extremely challenging. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyze the security of satellite communication networks in termsm of access control, confidentiality, and security authentication. The proposed scheme is developed to solve the security problem of using a centralized database in satellite communication. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications.

REFERENCE

[1] H. Al-Hraishawi, S. Chatzinotas, and B. Ottersten, ``Broadband nongeostationary satellite communication systems: Research challenges and key opportunities,'' in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), Jun. 2021, pp. 1-6.

[2] R. G.W. Latio, ``Social and cultural issues: The impact of digital divide on development and how satellite addresses this problem,'' Online J. Space Commun., vol. 2, no. 5, pp. 1-17, 2021.

[3] Q. Chen, G. Giambene, L. Yang, C. Fan, and X. Chen, ``Analysis of intersatellite link paths for LEO mega-constellation networks,'' IEEE Trans. Veh. Technol., vol. 70, no.3, pp. 2743-2755, Mar. 2021.

[4] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, ``Satellite communications in the new space era: A survey and future challenges,'' IEEE Commun. Surveys Tuts., vol. 23, no. 1, pp. 70-109, 1st Quart., 2021.

[5] N. U. Hassan, C. Huang, C. Yuen, A. Ahmad, and Y. Zhang, ``Dense small satellite networks for modern terrestrial communication systems: Benefits, infrastructure, and technologies,'' IEEE Wireless Commun., vol. 27, no. 5, pp. 96-103, Oct. 2020.

[6] L. Tian, N. Huot, O. Chef, and J. Famaey, ``Self-organising LEO small satellite constellation for 5G MTC and IoT applications,'' in Proc. 11 th Int. Conf. Netw. Future (NoF), Oct. 2020, pp. 100-104.

[7] L. You, K.-X. Li, J. Wang, X. Gao, X.-G. Xia, and B. Ottersten, ``Massive MIMO transmission for LEO satellite communications,'' IEEE J. Sel. Areas Commun., vol.38, no. 8, pp. 1851-1865, Aug. 2020.

[8] L. Xue, X. Li, W. Wu, and Y. Yang, ``Design of tracking, telemetry, command (TT&C) and data transmission integrated signal in TDD mode,'' Remote Sens., vol.12, no. 20, p. 3340, Oct. 2020.

[9] Technical Specification Group Radio Access Network; Solutions for NR to Support Non-Terrestrial Networks (NTN) (Release 16), document 3GPP TR 38.821, Version 16.0.0, 3rd Generation Partnership Project, 2019.

[10] I. D. Portillo, B. G. Cameron, and E. F. Crawley, ``A technical comparison of three low earth orbit satellite constellation systems to provide global broadband,'' Acta Astronautica, vol. 159, pp. 123-135, Jun. 2019.

[11] Y. Turk and E. Zeydan, ``Satellite backhauling for next generation cellular networks: Challenges and opportunities,'' IEEE Commun. Mag., vol. 57, no. 12, pp. 52-57, Dec. 2019.

[12] S. Xu, X.-W. Wang, and M. Huang, ``Software-defined next-generation satellite networks: Architecture, challenges, and solutions,'' IEEE Access, vol. 6, pp. 4027- 4041, 2018.

