International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I2P203
Volume 70 Issue 2, 19-23, February, 2022

Original Article

Internet of Things (Iot) Network Security using Quantum Key Distribution Algorithm

A. Srikrishnan[1], Dr. Arun Raaza[2], Dr. B. Ebenezer Abishek[3]

[1] *Research Scholar,* [2] *Supervisor & Dy.Director,* [3] *Associate Professor,*
[1,2,3]*Department of Electronics and Communication Engineering,*
[1,2,3] *Vels Institute of Science, Technology and Advanced Studies, Chennai.*

[1]*srikrishnan1978.a@gmail.com,* [2]*director.card@velsuniv.ac.in,* [3] *ebenezerabishek@gmail.com.*

Abstract *- Modern networks and future technologies rely on IOT technology. High bandwidth, extensive coverage, and enhanced capacity are key qualities of IOT networks. The IOT mobile network has two parts: Radio Access Network and Core Network. Toll-free radio access will cover macrocells and towers. The IOT network's macrocells use MIMO (Multiple Input Multiple Output) data transmission. IOT network is a wireless communication to build smart cities. The continuous switching of mega cells necessitates system security. The IoT network has its own communication security. Communication between two users will need frequent cell hopping. To improve network security, AES DES are utilised. QKD Algorithm is utilised to encrypt and decrypt in the proposed technique. Quantum computation uses superposition and entanglement to solve problems. This secures quantum computers. The QKD algorithm encrypts and decrypts data in Rectilinear and Diagonal bases utilising randomness. The qubits are transmitted. Encryption is done by turning qubits into photons. The QKD employs symmetric key encryption for authentication and confidentiality. Quantum key exchange delivers secure symmetric secret keys using a public key protocol for all network users. The performance indicators are compared to existing algorithms.*

Keywords - *IOT network security, Quantum computation, Quantum Key Distribution (QKD), BB84 Algorithm, Encryption and Decryption.*

I. INTRODUCTION

The IOT generation will provide extensive coverage and high-speed data transfer. The IOT network delivers smart cities by connecting various wireless devices. A better internet connection, low latency, and mobility are IOT network applications. For successful internet usage, IOT wireless system uses OFDM to provide wide range coverage and millimetre waves to boost channel throughput. IoT devices provide a seamless service.

IoT applications include,

- You can utilise multiple services simultaneously, such as knowing the weather and position while talking to someone else.
- Your smartphone can control your computer.
- Learning will be easier. The programme is available to students worldwide.
- Affordability and convenience of hospital care A doctor can treat a patient in another country.
- It'll be easier to track. A government body can monitor and examine offers anywhere on the planet. It is feasible to reduce crime.
- The solar system, constellations, and celestial bodies will be visible.
- It can track down and find the missing person.
- Tsunamis and earthquakes may be detected sooner.

The IOT network design employs 3GPP cellular standards. The specifications are developed by ITU (International Telecommunications Union) in conjunction with 4G. (LTE). The IOT network uses three frequencies. It operates between 24GHz and 100GHz. Second, mid-band (2–6 GHz) is used in urban and suburban areas. Third, the low band ranges from 2GHZ to 4G-LTE broadband spectrum.

Every IOT system has two modules. Those are ad-hoc, and end- Mobile devices connect to the IOT network's core via data networks. Authentication Server Function (AUSF) validate devices to connect to the Network as per requirements and other functions like SMF, PCF, AF, UDM to control the policy framework to manage system performance. These functions are complex to provide extensive coverage.

The IOT architecture uses LTE RAN for high-speed end-to-end connectivity. The IOT core has an edge data centre that finds the fastest way for communication. The Network is split into segments for applications, including extended IoT, critical IoT, and mobile radio band.

A. Distributed Quantum Keys

Our daily transmissions over various networks require privacy and encryption. Classical encryption techniques for mobile networks are vulnerable to quantum attacks and need advanced fundamental arithmetic. The QKD system provides quantum computer security. A network eavesdropper is located via QKD. To exchange a secret key over the quantum channel, QKD protocols differ in modulating, encrypting, decrypting, and establishing

quantum channels. The first QKD system was DVQKD, which uses photonic polarisation to convert data points. It became BB84 protocol. The BB84 protocol uses single state polarisation to secure fragments as qubits. These qubit forms use diagonal or rectilinear bases. Secure communication uses random bases and photonic energy. All communications use the physical channel. Both the source and the destination agree on the basis. The data is fragmented based on the key to ensuring no data is lost during fragmentation. This protocol is identical to B92 but has just two states instead of four. Unauthorized users do not know how to check the message being sent. Bit entanglement is another way to generate secrets. The QKD protocol for random variables was created using CVQKD rather than two different one-way and two-way methods. In one-way CVQKD, the device sends the concealed message and receives it, whereas, in two-way CVQKD, the destination node initiates contact after receiving inputs. Quantum key distribution QKD is used to send a protected key to distant clients. The QKD is more secure.

II. RELATED WORKS

MA Zheng et al. created NOMA, Massive MIMO, which uses Full-Duplexed device-to-device coded communication with coded Network [1]. This results in a green automated cognitive radio network for mmwave communication. It secures the physical and MAC layers. An improved mobile system with new network architecture and procedures.

When building devices, Mohammad Wazid et al. established a novel protocol to create a safe environment for IOT-enabled devices that increases efficiency, scalability, and data privacy [2]. They created a decentralised authentication [3] over the edge cloud employing one-way hashing for symmetric encryption and public-key security.

Dongsheng Zhao et al. created a secured IOT Heterogeneous Network using vertical and horizontal handover methods [4]. Alejandro Cohen et al. designed a post-quantum public-key network system [5]. This approach calculates a 3-link multipath network using 128 bits to encrypt each link at a 0.91 information rate.

On the IoT networks, Ohood Saud Althobaiti and co-workers devised a cryptography method using lattice driven mechanism [6]. Zunaira Babar et al. devised error-correcting codes for both quantum and classical systems [7]. The Liu and Wang protocol is used to increase mobile user security.

Ahmed A. Abd El-Latif et al. provide Security via a lightweight quantum encryption technique [8]. This method provides End-to-End Security for many IoT applications. Joschka Roffe et al. devised a model using quantum codes [9] to check information parity and repair errors. To ensure system trustworthiness, Daryus Chandra et al. devised a quantum error-correcting [10].

Analyzed by Anshul Jain et al., the ecosystem improves Security while having minimal influence on network design. Charles et al. presented the BB84 as an early quantum key distribution mechanism to compare qubit strings. The channel is maintained by a threshold value recovered from the shared key. Arul et al. [12] presented Quantum key grid management to increase device security. A basic key is created to secure a channel. To compute the two-party environment key, which can be easily overheard by any other network user, quantum mechanics is used. So, keeping secrecy from external parties without data loss due to quantum calculations. In order to keep the private key hidden, the Quantum Key Distribution (QKD) is used. Compared to other validation techniques, QKD provides faultless validation. In the Authenticated Key Exchange (AKE) model, Quantum bits are used to provide uninterrupted validation. This QKD-AKE is a more advantageous model. With the standard AKE concept, a secure network environment is provided.

[13] built a quantum aided Quick UDP connection between users utilising quantum mechanics computing to reduce network latency. Madhusanka Liyanage et al. suggested a routing protocol [14] to improve network device privacy. This routing technology lowers security and trust issues.

III. PROPOSED WORK

A. Design of IOT Network

The IOT network provides a secured environment by using the state of art encryption method that authenticates the Network using a protected signalling method. This method also provides Security during transmission. Security in the IOT network includes a plan, actions and association. The improvement in IOT network security requires Validation authorization, system identity management, low delay and cyphertext. The IOT network has its own security framework to improve secrecy in the Network.

Table 1. IOT parameters used to design the Network

PARAMETERS	VALUE
Frequency	4.5GHz
Antenna Height	29 m
Transmit power	48 dBm
Attenuation	38 dB
Tilt Angle	0 degree
Bandwidth	28 MHz
Antenna Height	1.9 m
Noise Figure	7.9 dB
Output	Directivity
Azimuth angle	-180:180
Elevation Angle	-90:90
ISD	0.25 – 5 km
Transmission Method	Single-In, Single-Out

From table 1, The IOT parameters are used to design the Network creates an impact like utilizing novel range, the addition of new clusters, increasing the shared

framework, decontrol devising, adjusting fiscal condition, diminishing cost in creating a cluster and evaluating the impact of analysis requirement. The outcome of these parameters results in increasing the capacity improving area coverage and productivity.

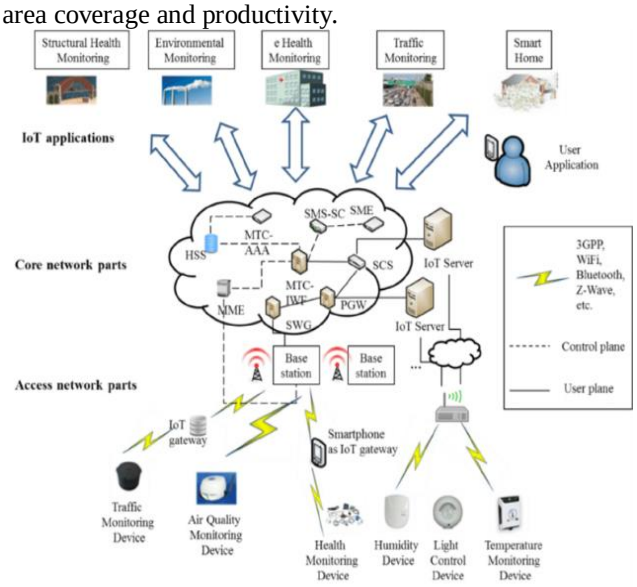

Fig 1. Representation of IOT network

Figure 1 shows the nodes that are located on the map at particular longitude and latitude location.

B. Data Encryption And Decryption Using QKD Algorithm

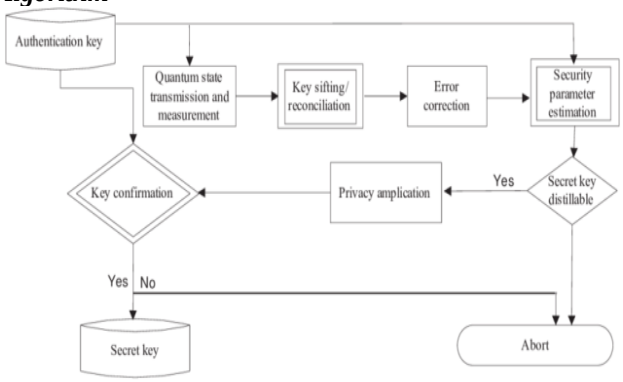

Fig 2 Flow of QKD algorithm in IOT network

Figure 2 shows the general flow of data in the QKD Algorithm in the IOT network. The algorithm begins with node deployment in the Network. Once nodes are deployed within the Network, the nodes are ready for communication. The request from the source to the destination has been sent. If the destination node accepts the request, Data transmission begins between the Network. The intermediate nodes are used to transmit the data to the destination successfully. The data that is being transmitted is encrypted using BB84 Quantum Distribution Algorithm (QKD). The bits of the data are converted into Qubits- quantum bits. The conversion of bits is done using the superposition principle. By using the superposition principle, the bits are converted into qubits using polarization techniques. The qubits are represented as,

IV. DATA TRANSMISSION

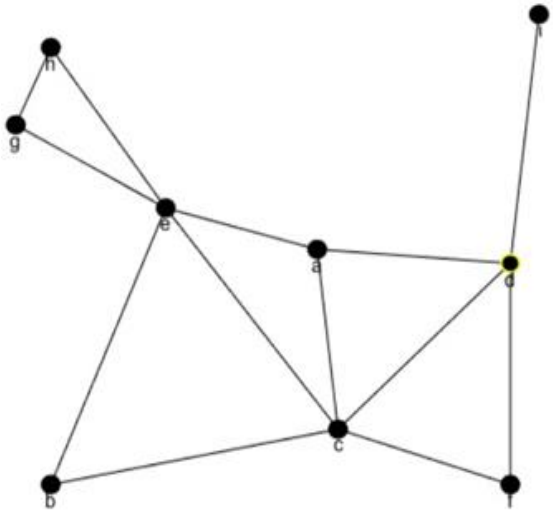

Fig 3. Node Deployment

Figure 3 shows the node deployment in the IOT network. The term "node deployment" includes the process of optimizing the network design by moving nodes around and building the appropriate Network to satisfy tracking requests at a cheap positioning cost.

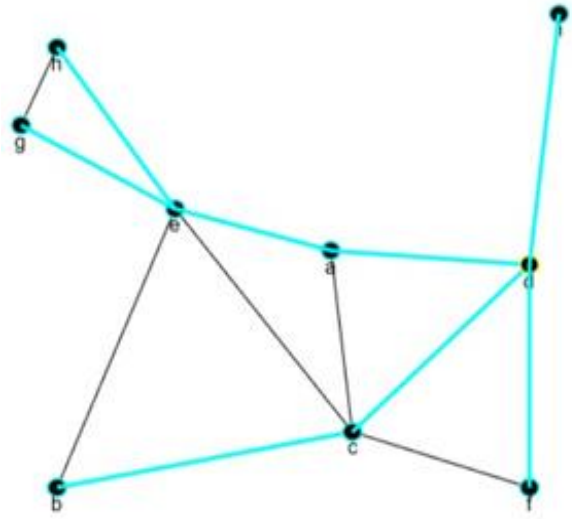

Fig 4. Request from sender to destination

The communication starts between the nodes, and the sender should find the path to reach the destination successfully. Fig.4 shows the ways to communicate between the sender to the destination. All the possible ways are identified to reach the destination. For example, here, we are going to start communication between a node to D to G. The node D tries to identify the destination G by checking all the nodes in the network sends a request to all the possible nodes.

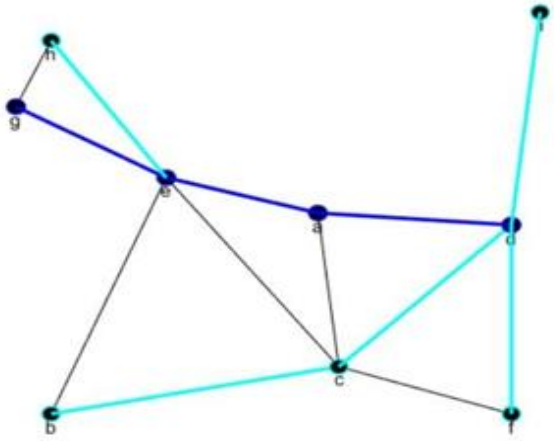

Fig 5. Response from the destination

Fig.5 shows the response from destination G to sender D that shows the path for communication indicated using blue colour.

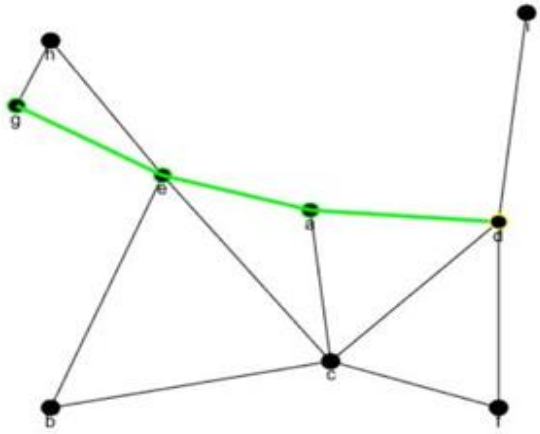

Fig 6. Transmission of data

Fig.6 shows the transmission between source D to destination G that is indicated by using green colour. The data is transmitted from the source to the destination successfully without any loss in reaching their destination.

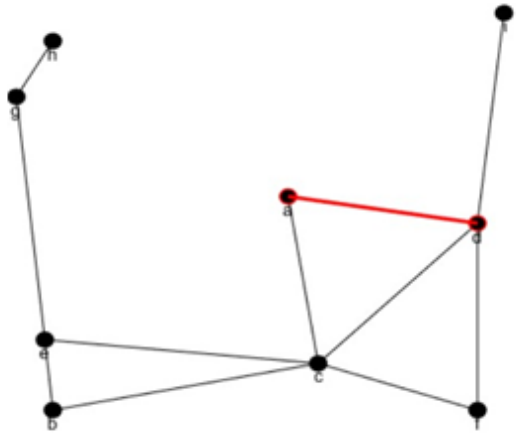

Fig 7. Error in data transmission

Fig.7 shows that sender D tries to reach destination G, but node A tries to collect data from the sender. The eavesdropper tries to collect information from the source that is indicated using red colour.

V. PERFORMANCE MEASURES

Table 2: Performance of the proposed and existing system

Parameters	QKD	AES	DES
Packet delivery ratio	98.65	96.58	98.56
SNR	8.23	15.69	36.58
Throughput	98.93	97.12	96.589
Accuracy	99.94	99.8	99.76
Precision	99.96	98.65	97.65
Recall	99.65	98.45	97.68
F1-Measure	99.38	98.32	98.65
Sensitivity	99.87	98.78	98.3
Specificity	99.8	98.1	99.68

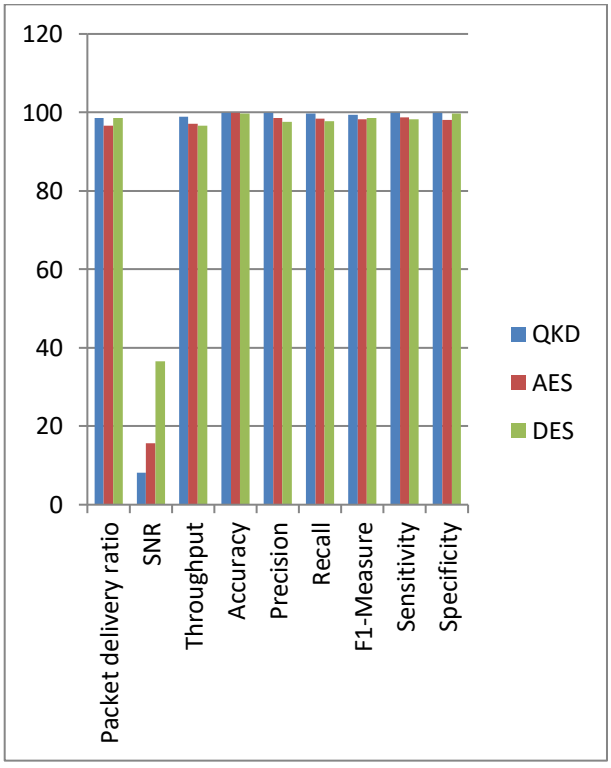

Fig. 8 Performance Metrics of The Network

Table 2 & fig. 8 shows performance metrics like packet delivery ratio, SNR, Throughput, Accuracy, Precision, Recall, F1-Measure, Sensitivity, Specificity. A comparison between the previously existing algorithm with the QKD algorithm is carried out.

VI. CONCLUSION

The IOT network had a wide application with more devices connected to it by reducing the latency of the Network. IOT network has its own security factors to improve the quality and accessibility of the Network. Many algorithms like AES DES are used within the Network to improve network security. The proposed QKD algorithm uses qubits to encrypt and decrypt the data that is to be transmitted in the Network. The ciphertext is transmitted in Network from the sender to the destination. The performance of the Network, like Packet delivery ratio, SNR, Throughput, Accuracy, Precision, Recall, F1-Measure, Sensitivity, Specificity, is measured by comparing the QKD algorithm with the existing algorithm. The performance of the nodes in the network is improved by using the QKD algorithm is more effective in avoiding information collected by the third party in the Network. In future, the new QKD algorithm can be improved to provide more security to the user in Network. Further KDD datasets are used for analysis in the IOT network with the QKD algorithm and other deep learning algorithms.

REFERENCES

[1] Ma, Z., Zhang, Z., Ding, Z., Fan, P. and Li, H., Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives. Science China information sciences, 58(4) (2015) 1-20.

[2] Wazid, M., Das, A.K., Shetty, S., Gope, P. and Rodrigues, J.J., Security in 5G- enabled internet of things communication: issues, challenges, and future research roadmap. IEEE Access, 9 (2020) 4466-4489.

[3] Fan, C.I., Shih, Y.T., Huang, J.J. and Chiu, W.R., Cross-network-slice authentication scheme for the 5 th generation mobile communication system. IEEE Transactions on Network and Service Management, 18(1) (2021) 701-712.

[4] Zhao, D., Yan, Z., Wang, M., Zhang, P. and Song, B., Is 5G Handover Secure and Private? A Survey. IEEE Internet of Things Journal. (2021).

[5] Cohen, A., D'Oliveira, R.G., Salamatian, S. and Médard, M., Network Coding- Based Post-Quantum Cryptography. IEEE Journal on Selected Areas in Information Theory, 2(1) (2021) 49-64.

[6] Althobaiti, O.S. and Dohler, M., Cybersecurity Challenges Associated with the Internet of Things in a Post-Quantum World. IEEE Access, 8, (2020) 157356-157381.

[7] Babar, Z., Chandra, D., Nguyen, H.V., Botsinis, P., Alanis, D., Ng, S.X. and Hanzo, L., Duality of quantum and classical error correction codes: Design principles and examples. IEEE Communications Surveys & Tutorials, 21(1) (2018) 970-1010.

[8] Abd El-Latif, A.A., Abd-El-Atty, B., Venegas-Andraca, S.E., Elwahsh, H., Piran, M.J., Bashir, A.K., Song, O.Y. and Mazurczyk, W., Providing end-to-end Security using quantum walks in 5G networks. IEEE Access, 8 (2020) .92687-92696.

[9] Roffe, J., Zohren, S., Horsman, D. and Chancellor, N., Quantum codes from classical graphical models. IEEE Transactions on Information Theory, 66(1) (2019) 130- 146.

[10] Chandra, D., Babar, Z., Nguyen, H.V., Alanis, D., Botsinis, P., Ng, S.X. and Hanzo, L., Quantum topological error correction codes: The classical-to-quantum isomorphism perspective. IEEE Access, 6 (2017) 13729-13757.

[11] Jain, A., Singh, T., Sharma, S.K. and Prajapati, V., Implementing Security in 5G Ecosystem Using 5G Network Slicing and Pattern Matched Intrusion Detection System: A Simulation Study. Interdisciplinary Journal of Information, Knowledge & Management, 16 (2021).

[12] Arul, R., Raja, G., Almagrabi, A.O., Alkatheiri, M.S., Chauhdary, S.H. and Bashir, A.K., A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario. IEEE Transactions on Industrial Informatics, 16(1) (2019) 681-690.

[13] Yan, P. and Yu, N., The QQUIC Transport Protocol: Quantum assisted UDP Internet Connections. arXiv preprint arXiv:2006.00653. (2019)

[14] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S. and Ylianttila, M., July. 5G privacy: Scenarios and solutions. In IEEE 5G World Forum (5GWF) (2018) 197-203.