JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Performance Evaluation of Quantum Cryptography for Wireless Sensor Networks

[1]Adyasha Behera, [2]Alok Ranjan Tripathy, [3]Rabindra Nath Mishra

[1] PhD Scholar of Author, [2]Assistant Professor of 2nd Author, [3] Professor of 3rd Author
[1,2]Department of Computer Science 1st Author,
[3]Department of physics 3rd Author
[1]ravenshaw University of 1st Author, Cuttack, India.

Abstract: The term "wireless," as defined in the dictionary, signifies "having no wires." In the context of networking, wireless refers to a computer network where there exists no physical wired connection between the sender and receiver. Instead, communication within the network is established through the utilization of radio waves and/or microwaves. This allows for connectivity without the reliance on physical cables. Addressing Wireless Sensor Network Security Challenges: The Role of Quantum Cryptography in the realm of communication, network security stands out as a critical concern, especially in the face of prevalent cyberattacks. Quantum cryptography, representing the next generation of cryptographic solutions, emerges as a promising candidate to counter these threats. Consequently, the existing landscape of public key cryptography requires adaptation to effectively combat eavesdropping attempts. This paper endeavors to introduce a Quantum Key Distribution (QKD) framework, where both the public key channel and the quantum key channel coexist. The proposed approach outlines a five-step key security process, seamlessly integrating both public key cryptography and quantum key cryptography.

IndexTerms **– Quantum Key Distribution (QKD), Wireless Sensor Network (WSN), Quantum cryptography.**

I. INTRODUCTION

In its entirety, a wireless sensor network can be defined as follows: A Wireless Sensor Network (WSN) **Error! Reference source not found.**constitutes a collection of spatially dispersed and dedicated sensors designed for the purpose of monitoring and recording the physical conditions of the environment. The collected data is then centralized at a designated location. Comprising "nodes" ranging from a few to potentially several hundred or even thousands, each node is linked to one or, in some instances, several sensors. A typical sensor network node consists of multiple components, including a radio transceiver equipped with an internal antenna or connected to an external one, a microcontroller, an electronic circuit facilitating sensor interfacing, and an energy source, often in the form of a battery or embedded energy harvesting. WSN topologies exhibit diversity, ranging from a straightforward star network to a sophisticated multi-hop wireless mesh network. A Wireless senor device is responsive to a physical stimulus, such as heat, light, sound, pressure, magnetism, or specific motion, is capable of transmitting a resultant impulse, often employed for measurement or control operations. A network, in broader terms, denotes a collection of devices capable of communication. It is formed by interconnecting various computer systems through physical and/or wireless connections, facilitating seamless communication between devices within the network.

Network topology refers to the structure of a network, encompassing its nodes and the connections between them. The arrangement of a network can be defined in two ways: the physical topology and the logical (or signal) topology in Fig.1.. Wireless mesh topology is a network configuration where each node in the network has the capability to relay data to other nodes. In this topology, nodes are interconnected, and communication can occur through multiple paths, creating a mesh-like structure. Unlike traditional wireless topologies where devices typically connect directly to a central access point, wireless mesh networks allow for more flexibility and resilience.

Wireless Sensor Network (WSN) routing refers to the process of determining the paths or routes that data should follow within the network. In a WSN, which typically comprises numerous sensor nodes deployed in a specific area for data sensing and transmission, efficient routing is crucial for optimizing energy consumption, extending network lifespan, and ensuring timely and accurate data delivery.

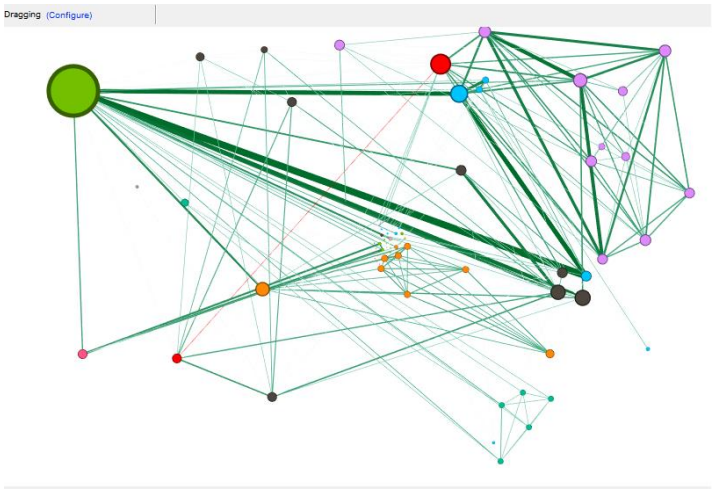

Fig. 1. WSN Mesh Topology

Consider a communication setting where two individuals, denoted as A and B, aim to engage in secure communication. In this context, A takes the initiative to convey a message to B by transmitting a key. This key serves as the mode for encrypting the subsequent message data. The key, generated as a random sequence of bits, is transmitted using a specific scheme that allows two distinct initial values to represent a particular binary value.

Quantum cryptography[4] originates from the principles of physics intending to create a cryptosystem impervious to malicious or unwanted intrusions. It aims to achieve complete security, ensuring immunity against compromise without the knowledge of the message sender or receiver. The term "Quantum" is rooted in the fundamental behaviors described by quantum theory, relating to the smallest particles of matter and energy.

The rise of quantum computing spurred increased interest in quantum cryptography. In cryptographic discussions, the term "key" pertains to a shared secret that governs the ability to conceal and reveal information. Cryptography comprises two primary types: symmetric key and public key cryptography. Quantum computing and Quantum information theory emerge as viable candidates in advancing these cryptographic endeavors. In Fig.2. provided the information regarding the quantum routing framework.

This research comprises five sections. The initial section furnishes a comprehensive introduction to wireless networks and quantum cryptography. Section II provides a succinct literature survey on Quantum Key Distribution (QKD) [5]protocols. Section III presents fundamental notations associated with quantum cryptography. Section IV delves into a comparative analysis between classical network cryptography and quantum cryptography. Finally, Section V encapsulates the concluding remarks of the study.

II. Related Work

In their research, Yasha Istwal and Shashi Kant Verma [1]from the Computer Science Engineering department at GBPEC, Pauri Garhwal, India, emphasize the critical importance of Energy, Network Lifetime, and Stability as pivotal parameters for the proficient management of sensor networks. The researchers propose the Dual Cluster Head Routing Protocol (DCHRP), which incorporates a dual cluster head system with three levels of heterogeneity aimed at enhancing the lifespan of a Wireless Sensor Network (WSN). The primary objective of DCHRP is to minimize energy wastage by reducing the frequency of cluster head selection.

The researchers conducted simulations using Matlab and observed a noteworthy increase of 9.99 in the stability period of DCHRP. This improvement underscores the effectiveness of the proposed protocol in enhancing the stability of the Wireless Sensor Network, thereby contributing to prolonged network lifespan and optimized energy management.

Selvakumar Sasirekha and Sankaranarayanan Swamynathan et. al [2] addressed the challenges inherent in wireless sensor networks (WSNs). These networks, characterized by sensor nodes with limited sensing, computation, and communication capabilities, predominantly operate on battery power in harsh environments with non-replenishable sources. The constrained nature of sensor nodes makes the network susceptible to failures, as a significant portion of energy is consumed in data transmission, sensing, and computation. Applications such as habitat monitoring, military surveillance, and forest fire detection demand prolonged sensor node lifetimes as they operate in human-unattended settings.

The key challenges in WSN design revolve around energy conservation, minimizing data transmission delay, and enhancing network longevity. To tackle these issues, the researchers advocate the use of data aggregation as an intelligent technique in WSNs. Data aggregation involves accumulating information from diverse sources at intermediate nodes, thereby reducing the number of packets to be transmitted to the sink. A literature review indicates the utilization of various routing algorithms based on network topology for data aggregation.

To address these challenges and outperform existing approaches, the research introduces a novel routing algorithm known as Cluster-Chain Mobile Agent Routing (CCMAR). This algorithm aims to provide improved performance in terms of energy efficiency, reduced data transmission delay, and enhanced network lifespan compared to existing routing methods in WSNs.

Swati Mishra, Rukhsar Bano, Suresh Kumar, Vimal Dixit, and others have defined a Wireless Sensor Network (WSN) [3]as an arrangement of sensor nodes strategically positioned within an environment. These sensor nodes collectively facilitate the detection and monitoring of various environmental and physical conditions. The effectiveness and security of the system are reliant on WSNs, which serve as the backbone for gathering information and establishing communication systems.

III. PROPOSED WORK

Quantum Key Generation, Quantum Key Distribution (QKD), and Post-Quantum Cryptography represent various forms of proposed Quantum-Safe Cryptography[7][13]. The efficacy of key security heavily relies on the generation of highly random keys, as keys lacking sufficient randomness are susceptible to eavesdropping attempts. Quantum Key Generation addresses this challenge by leveraging the principles of quantum physics to produce exceptionally secure and genuinely random keys. While Quantum Key Distribution cannot completely prevent eavesdropping, it can detect unauthorized access. In the event of such detection, the system can promptly destroy the compromised key before it is exploited.

QKD[14][12] enhances security by facilitating consistent, randomized, and automated key exchanges, coupled with robust protection against external noise entering the system. Post-quantum cryptography specifically focuses on public-key cryptographic algorithms deemed resilient against quantum computer attacks. The following statistical facts draw a comparison between conventional cryptographic algorithms and quantum computation. Cryptographic systems such as RSA, DSA, DH, ECDH, ECDSA, and their variants are identified as highly vulnerable to quantum attacks. It is noteworthy that these figures underpin the security of contemporary public-key cryptography in various products and protocols. The significance lies in recognizing the critical need for advancing cryptographic algorithms in the face of quantum threats.

The Quantum Key Distribution (QKD) protocol involves distinct stages in key generation. Figure 2 illustrates the process where Alice generates a range of randomized keys. Subsequently, Alice transmits polarized photons through a quantum channel to Bob. Bob, in turn, generates a confirmation key that serves to authenticate and certify the actual message. This confirmation key plays a crucial role in establishing the authenticity and integrity of the transmitted data, aiding in error identification within the channel.

Moving on to the next stage, the process involves data encryption, which occurs after implementing the data confidentiality protocol. Each stage of the key generation process undergoes a secure procedure of data exchange, ensuring the overall security and reliability of the Quantum Key Distribution protocol[13].

Quantum cryptography is a method that combines the relative ease and convenience of key exchange in public key cryptography with the unparalleled security[6] provided by a one-time pad. Imagine that the key consists of a stream of photons moving unidirectionally, where each photon particle signifies a single binary bit. These particles not only travel linearly but also oscillate in a specific manner. These oscillations can occur across any conceivable axis within a 360-degree range. However, for the sake of simplifying quantum cryptography, let's assume that these oscillators exist in four particular states: UP-DOWN ("↑↓"), LEFT-RIGHT ("←→"), LEFTUP-RIGHTDOWN ("↗↙"), and vice versa. The angle of this oscillation is referred to as the polarization of the photon.

Polarization essentially acts as a filter, allowing certain photons to pass through with the same oscillation as before, while altering the state of oscillation for others or even completely blocking some photons. Individual A possesses a polarizer that can transmit photons in any one of the four states. They have the option to choose between rectilinear polarization (UP-DOWN and LEFT-RIGHT) or diagonal polarization[8] (UPLEFT-RIGHTDOWN and UPRIGHT-LEFTDOWN) filters.

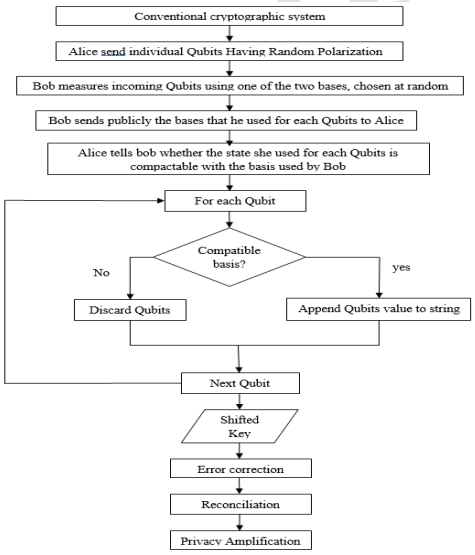

Fig.2. Proposed model for cryptography

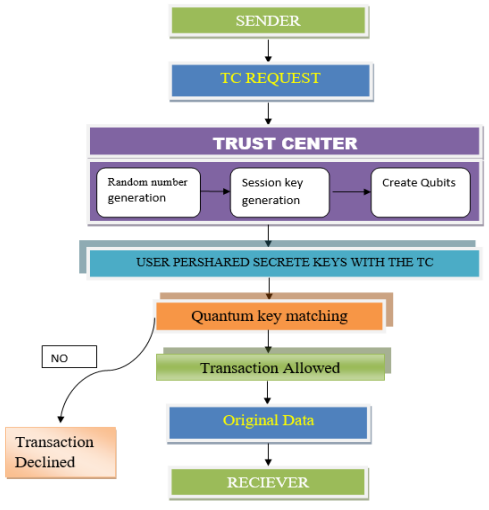

Fig.3. QKD framework for cryptographic approach

IV. RESULTS AND DISCUSSION

Through our research journey, we gained deeper insights into the generation of suitable Quantum Keys using Quantum Key Distribution (QKD). Detecting an invertible key poses a significant challenge for eavesdroppers due to the complexity of key distribution and combination. Consequently, the likelihood of obtaining or extracting the encoded text is extremely low, if not nonexistent.

Quantum Key Generation, Quantum Key Distribution (QKD), and Post-Quantum Cryptography represent categories within the realm of proposed Quantum-safe cryptography. The generation of highly secure keys relies on the principle of high randomness. Inadequately randomized keys are susceptible to eavesdropping, making Quantum Key Generation crucial for establishing exceptionally secure keys. Leveraging quantum physics enables the creation of genuinely random and secure keys.

Quantum Key Distribution (QKD)[12], based on quantum physics, cannot prevent eavesdropping but excels in detecting unauthorized access. In the event of a potential breach, QKD can destroy the compromised key before any unauthorized access occurs. It enhances security by facilitating consistent, randomized, and automated key exchanges. Additionally, it incorporates high-quality protection to prevent noise from compromising the system.

Post-quantum cryptography specifically addresses public key cryptography algorithms deemed secure against potential quantum computer attacks. Statistical comparisons reveal the vulnerability of conventional cryptographic algorithms to quantum computation. Cryptosystems, [16]including RSA, AES, RC4, and their variations, are known to be highly defenceless against quantum assaults, as they can be easily compromised by a quantum computer. Notably, these figures are widely used in contemporary security products and protocols relying on public key cryptography.

Our focus was on encoding large text files and comparing the time taken by Quantum Cryptography against other cryptographic techniques for both encoding and decoding processes. Our findings demonstrated the superiority of our proposed algorithm over traditional cryptographic techniques. This underscores the efficacy and efficiency of Quantum Cryptography in encoding and decoding tasks, particularly when dealing with substantial amounts of data.

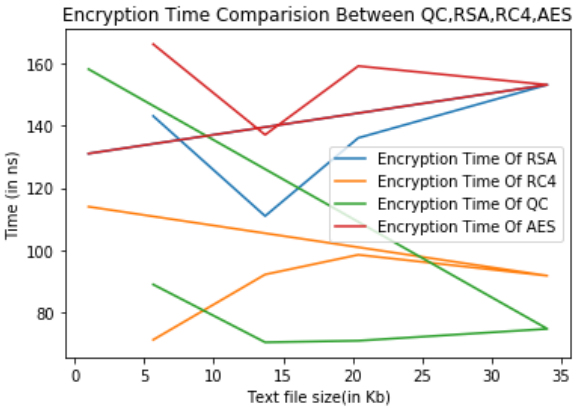

Fig.4. Encryption time difference between RSA, RC4, AES, QC

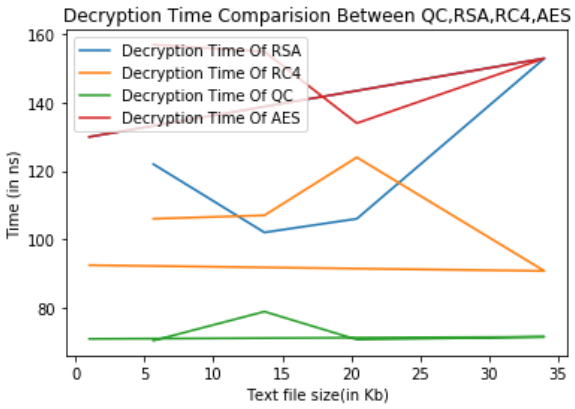

Fig.5. Decryption time difference between RSA, RC4, AES, QC

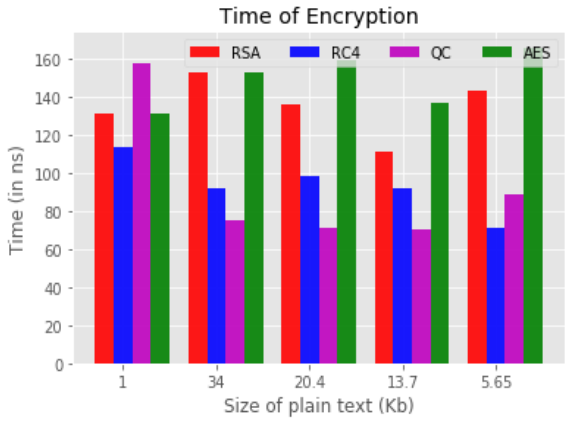

Fig.4. Encryption time difference between RSA, RC4, AES, QC

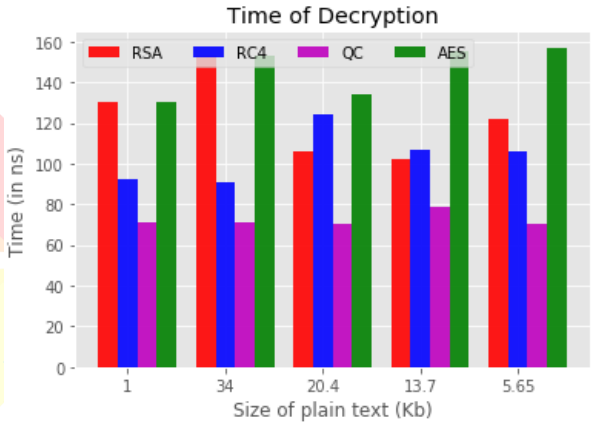

Fig.5. Decryption time difference between RSA, RC4, AES, QC

IV. Conclusion

Our research journey has provided a heightened understanding of the process of generating suitable Quantum keys through Quantum Key Distribution (QKD)[5]. The complexity involved in the distribution and combination of keys poses a significant challenge for eavesdropping attempts. The intricate nature of key generation makes it extremely difficult for adversaries to detect a proper invertible key, virtually eliminating the chance of extracting the encoded text. Our focus was on encoding large text files, and we conducted a comparative analysis of the time taken by Quantum cryptography versus other cryptographic techniques for both encoding and decoding identical files.

Through our study, we demonstrated that our proposed algorithm significantly outperforms other cryptography techniques in terms of efficiency and security. The results underscore the robustness of our approach and its superiority in safeguarding data through effective key generation and encryption processes.

REFERENCES

[1] Y. Istwal and S. K. Verma. 2017. Dual cluster head routing protocol in WSN. 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, doi: 10.1109/ ICCCNT .2017. 8203940.: 1-6

[2] S. Sasirekha and S. Swamynathan. 2017. Cluster-chain mobile agent routing algorithm for efficient data aggregation in wireless sensor network. in Journal of Communications and Networks, vol. 19, no. 4, doi: 10.1109/JCN.2017.000063.: 392-401.

[3] S. Mishra, R. Bano, S. Kumar and V. Dixit. 2017. A literature survey on routing protocol in wireless sensor network. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India. doi: 10.1109/ICIIECS.2017.8276150. : 1-4,

[4] Bennett, C.H. and G. Brassard 2014 Quantum Cryptography: Public key distribution and coin tossing. Theoretical Computer Science, Elseiver, vol. 560: 7-11.

[5] Bennett, C. H., F. Bessette, G. Brassard, L. Salvail and J. Smolin 1992 Experimental quantum cryptography Journal of Cryptology, vol. 5, no. 1,: 3-28.

[6] Bennett, C. 1992. Quantum cryptography using any two nonorthoganol states. Phys. Rev. Lett. 68.:3121-3124.

[7] Bechmann-Pasquinucci, H., and Gisin, N. 1999. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys. Rev. A 59, 127901(1)-127901(4): 4238-4248.

[8] Jinhui Liu, Aiwan Fan, Jianwei Jia, Huanguo Zhang, Houzhen Wang, and Shaowu Mao. 2016. Cryptanalysis of Public Key Cryptosystems Based on Non-Abelian Factorization Problems. TSINGHUA SCIENCE AND TECHNOLOGY, ISSN 1007-0214 10/11 Volume 21, Number 3.:344–351

[9] Changhua He & John C Mitchell. 2004. Analysis of the 802.11i 4-Way Handshake. WiSE‟04 Philadelphia, Pennsylvania, USA ACM 1-58: 113-925.

[10] A.Falahati , Hadi Meshgi. 2009. Using Quantum Cryptography for securing Wireless LAN networks. International Conference on Signal Processing Systems, IEEE DOI 10.1l09/ICSPS.216. :698-701.

[11] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma. 2009. Novel Protocol and Its Implementation QKD in Wi-Fi Networks. Eight IEEE/ACIS International Conference on Computer and Information Science,IEEE 978-0-7695-3641-5/09DOI 10.1109/ICIS.2009.122.:812-817.

[12] R.Lalu Naik , Dr.P.Chenna Reddy , U.Sathish Kumar, Dr.Y.V.Narayana. 2011. Quantum Cryptography with Key Distribution in Wireless Networks on Privacy Amplification. International Journal of Computer Networks and Wireless Communications, vol.1.: 1-5.

[13] S. Wijesekera, X. Huang and D.Sharma. 2010. Quantum Cryptography Based Key Distribution in Wi-Fi Networks - Protocol Modifications in IEEE 802.11. 5th International Conference on Software and Data Technologies (ICSOFT 2010), Athens, Greece.

[14] X. Huang, S. Wijesekera, and D.Sharma. 2009. Quantum Cryptography for Wireless Network Communications. IEEE International Symposium on Wireless and Pervasive Computing, 11-13th, Melbourne, Australia, ISBN: 978-1-4244-2966-0, Security.:1-5.

[15] X. Huang, S. Wijesekera, and D.Sharma. 2011. Performance Analysis of QKD Based Key Distribution for IEEE 802.11 Networks. Ninth Annual International Conference on Privacy, Security and Trust, 978-1-4577-0584-7/11/$26.00©2011 IEEE.

[16] Song-Kong Chong, Tzonelih Hwang. 2010. Quantum key agreement protocol based on BB84. Optics Communications 283.: 1192–1195.