Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: March, 2023 **2023, 20(5 Suppl.): 2077-2085** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2023.7460

Improving Wireless Sensor Network Security Using Quantum Key Distribution

Laith H. Alhasnawy* ***Ameer K. AL-Mashanji***

Presidency of University of Babylon, University of Babylon, Babylon, Iraq
*Corresponding authors: laith.alhasnawi4@uobabylon.edu.iq
E-mail address: amir.mashanji@uobabylon.edu.iq

Received 26/5/2022, Revised 6/11/2022, Accepted 7/11/2022, Published Online First 20/3/2023, Published 28/10/2023

Abstract:

Wireless Sensor Networks (WSNs) are promoting the spread of the Internet for devices in all areas of life, which makes it is a promising technology in the future. In the coming days, as attack technologies become more improved, security will have an important role in WSN. Currently, quantum computers pose a significant risk to current encryption technologies that work in tandem with intrusion detection systems because it is difficult to implement quantum properties on sensors due to the resource limitations. In this paper, quantum computing is used to develop a future-proof, robust, lightweight and resource-conscious approach to sensor networks. Great emphasis is placed on the concepts of using the BB84 protocol with the AES algorithm in WSN security. The results of analysis indicated a high level of security between the data by depending on the generation of secure keys, and reached an accuracy rate of about (80-95) % based on using NIST statistical. The efficiency of the work increased to 0.704 after using the Quantum Bit Error Rate equation, eventually increasing the network performance. This results in the reduction of the overall amount of energy, and the time required for performing the key exchange in the encryption and decryption processes decreased.

Keywords: AES, BB84 protocol, QBER., QKD, WSN

Introduction:

A Wireless Sensor Network consists of a large number of sensor nodes that communicate wirelessly. Healthcare, sports training, workplace safety, consumer electronics, secure authentication, and protection of uniformed personnel are just a few of the applications of WSN, meaning it is ubiquitous and has broad market potential[1]. In a wireless sensor network, data aggregation reduces packet transmissions and enhances network duration, as sensor data is collected and delivered to the base station by aggregation nodes. A WSN is typically used to monitor inaccessible or hard-to-reach websites. There are security issues in the communication between sensor nodes[2].

In WSN, message security and sensor node authentication have become major concerns while data collection, security is the most important in the matter of the paper[3].

Network security is a concept of securing data in a designed manner that requires few resources and provides high throughput while consuming little power. Two types of light weight algorithms are symmetric and asymmetric, stream ciphers and block are both symmetric ciphers[3, 4].

The WSN environment has many security issues being unable to secure the privacy of user data. One of the most serious security issues with WSN, which is vulnerable to a variety of privacy threatening attacks, one of which is a quantum computer attack that has occurred as a result of rapid advances in the use of quantum physics to break many than traditional algorithms[5].

Quantum computing is based on quantum physics and allows secure communication based on quantum properties, such as quantum no-colning theorem. Because quantum computing properties can solve problems of security and privacy that are unsolvable with classical approaches[6], quantum computing (quantum key distribution QKD) becomes more likely for security in WSN.

In a wireless sensor network, quantum computation is utilized to ensure that data transmission is secure. Quantum key distribution (QKD) is a quantum-based communication system. Using the BB84 protocol, it will generate a shared

secret key that is only known by communicating parties[7,8]. Two basis sequences are employed in the BB84 protocol: rectilinear **(+)** and diagonal **(x).** The horizontal polarization **(0°)** and vertical polarization **(90°)** of the rectilinear basis are separated. Two polarization states, **(45°)** and **(135°),** are found in the diagonal basis[9, 10].

This purpose of this paper is to provide lightweight encryption algorithm for low-resource devices in WSNs. By combining quantum computing and the lightweight algorithm (AES) in WSN, encryption procedures in lightweight cryptographic algorithms are created, implemented, and assessed to improve the security of communication and data transmission in this environment.

Related Work

Heig et al.[2] proposed a future proof lightweight security concept for wireless sensor networks with a permeate filtering mechanism through a multi-stage filtration system that includes encryption and error detection mechanisms in the processing stage. Focuses on conceptual evaluation on the new magic number filter to reduce the special type of denial of service attack that has been worked on the CC1350 Launch-Pad ARM Cortex M3 microcontroller boards.

JV Anand[3] proposes an approach that deals with a routing algorithm that relies on compression sensing data and trust-awareness, to handle routing in a clustered WSN. In this approach five optimization methods were used based on a developed methodology that focuses on maximizing trust in the route, minimizing message overhead, number of hops and maximum distance.

Bhatia and Sumbaly[4] presented a methodology for incorporating quantum encryption and IEEE 802.11 wireless network security into cryptographic key distribution. A new protocol was developed to distribute the secret key needed to encrypt data, as this key provides strong security during the communication session.

Miralem Mohic et al.[5] described a simulated environment of a quantum key distribution network with several nodes and links. In this approach several routing protocols, packet delivery ratio and routing packets are analyzed to find a best solution to the large amount of routing data flowing through the WSN through the QKD network.

Doha AL-Mubayedh et al.[6] used the quantum key distribution protocol BB84 to provide a practical application to IBM QX software. In this approach a statistical analysis of third-party eavesdropping detection in WSN is proposed. Through this proposal, the quantum key distribution protocol BB84 is practically implemented in addition to the possibility of protection against eavesdropping attacks.

Journal, D. In, and P. K. Kishore[7] reviewed how we can use symmetric polynomials and the quantum cryptography method based on key management in key distribution to enhance and analyze the authentication mechanism between wireless sensor network access points.

The above related works did not introduced the computing between QKD and AES algorithm to enhance the security of WSN which will be introduced in our paper.

Security Requirements in WSN

The below are the security requirements for wireless sensor networks:

1- **Confidentiality**: The encryption method is employed to keep data confidential[11], because the radio spectrum used in the sensor network is an open resource that may be accessed by anybody with a suitable radio transceiver.
2- **Authentication**: The receiving node of transmitted data should verify that the data came from a trustworthy source[12]. Authentication ensures that the identities of those involved in the communication are verified.
3- **Data Integrity**: Is a term that refers to the quality of data assurance that the sent data is not tampered with, either intentionally or unintentionally. The usage of message integrity code is the conventional method for assuring data integrity[13].
4- **Self-Organization and Self-Healing**: WSN sensor nodes can self-organize and self-heal. There is no fixed infrastructure available for WSN network management due to the capability of sensor nodes to organize[14].
5- **Data Freshness:** The attack may attempt a replay by substituting an old key for a new key; in such instances, data freshness assures that the data is current and that no old data keys are used[15].

Quantum Key Distribution

Quantum physics advancements have prompted new ideas for ensuring communication security. In symmetric encryption systems, designers of encryption systems had to come up with a new encryption scheme and distribute the key safely[7, 15]. A single or entangled quantum is passed between two parties in the quantum key distribution.

A quantum channel is utilized for photon exchange, and a conventional channel is used for basic agreement to find the opponent in this protocol[16]. Both parties will notice an eavesdropper presence on the public media if a third party measures the conveyed quantity. The eavesdropper's measurement will

modify the quantum state according to the rules of quantum mechanics[17, 18], and it will not be able to clone an arbitrary quantum state.

1- BB84 Protocol

Bennett and Brassard introduced the first quantum key distribution protocol in 1984, which has since been documented in a number of publications, as well as proof that it is unconditional. Quantum and classical channels are used in the BB84 protocol[19] for sending polarized light pulses via a quantum channel, such as an optical fiber, with each pulse containing one photon. It allows two parties, Alice as the sender and Bob as the receiver, to create a secret shared key using polarized photons qubits[20, 21]. Conjugate bases are used to polarize photons.

The Standard Basis is the vertical and horizontal polarization) such as:

The rectilinear **bases** +

- Horizontally(0)polarized → represent as **H**
- Vertically (90) polarized ↑ represent as **V**

And the horizontal **bases** v?

- Right (45) polarized ↗ represent as **R**
- Left (135) polarized ↖ represent as **L**

WSN nodes often face resource constraints, such as computing capacity, memory space, and power management. Additional constraints imposed by network communication, especially WSN communications, include low information rates, constant delays, and higher data drops.

Different methods are used to verify the information key exchanged between WSN nodes. The existing method makes use of WSN node classical memories via key information stored in the node that recalls the key that is kept in a secure location. The suggested approach is based on the QKD principle to produce safe keys using the QKD link's local key, which is stored by the node on both ends of the connection, while the secret key is generated on the QKD path link's paths.

***1*- Proposed Network in WSN**

The topology of the WSN consists of some sensors sending data to a sink, which processes the data and encrypts it using the AES algorithm and BB84 to exchange keys before sending it to the Internet. The suggested WSN topology is shown in Fig.1.

Proposed System in WSN

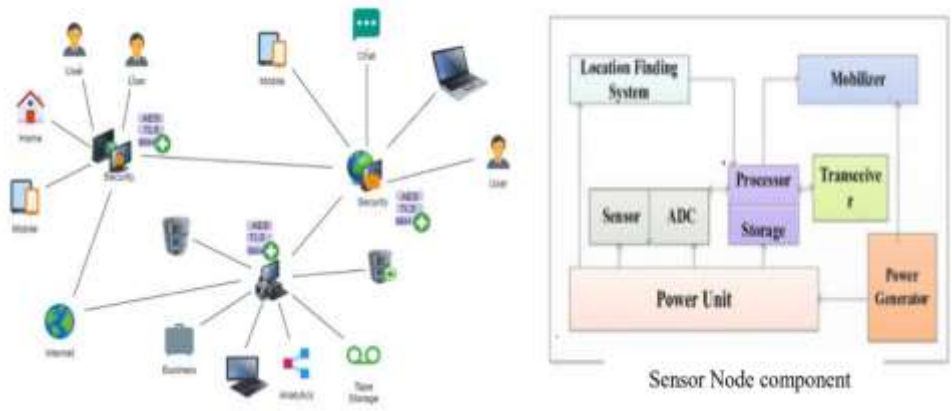


Figure 1: WSN Topology

The QKD principle is used in conjunction with the WSN environment in this system. It is dependent on switching from the classical algorithms used to generate the key in the AES algorithm to another algorithm or protocol based on quantum features, such as the BB84 protocol, which is used to generate secure keys to encrypt data in the WSN. To prevent security threats in WSN, the QKD employs the features of the Transport Layer Security (TLS) protocol to offer safe data by requiring trustworthy parties to interact.

The QKD method in AES is used to authenticate and encrypt data using a key generated by the BB84 protocol, which is utilized to generate key material in AES' data encryption process.

2- Proposed Algorithm for Network

Each work algorithm in the WSN establishes communication between the sensor and the sink, as well as adding security via the AES architecture.

The following technique depicts the major steps for generating keys for WSN security from the sender side using the quantum key Distribution (BB84) protocol, the points below explain to execute steps of algorithm 1.

1- The sender may select a value (N) that used a random function to generate fragments (0 or 1) and equalize them with the input value and then generate another function to pass N numbers to random bases **(+ or v?)** to create polarization by using these generated bases. Then send these

polarize photons to receiver, polarization are **(→= 0°, ↑ = 90°, ↗ = 45°, ↖ = 135°).**

2- If the bases is +, that state based on the random bit values as follows:
- if bit value =0, polarize state will be → **(H)**
- if bit value =1, polarize state will be ↑ **(V)**

If the bases are x, that state based on the random bit values as follow:
- if bit value =0, polarize state will be ↗ **(R)**
- if bit value =1, polarize state will be ↖ **(L)**

After these steps, the polarization is sent to the receiver.

Algorithm 1: Key exchange in Sender
Input: n (Number of initial photons),i1, Alice_qu [n], Alice_Basis [n].
Output: polarized photon as (H,V,R,L).
Begin
1- for i→0 to n do // **Generate Random Bits …** // **Raw Key** i1 =i1+1
if (i1==0 ||i1==1) then Alice_qu [i] = 0 else Alice_qu[i]==1 end if
If (i1==4) then i1 = -1 end if end for
2- for i→0 to n do **//Generate Random Bases ... //Key IDs**
Alice_ba [i] = "+" or "x" end for
3- function: PreparePhoton(n, Raw Key, Key IDs)
If (Raw Key == 0 & Key IDs =="+") then Polarized photon (H) end if
If (Raw Key == 0 & Key IDs =="x") then Polarized photon (R) end if
If (Raw Key == 1 & Key IDs =="+") then Polarized photon (V) end if
If (Raw Key == 1 & Key IDs =="x") then Polarized photon (L) end if
End PreparePhoton
4- Encoding Key Parameters
5- Send Key Parameters
6- Send Polarized photons via WSN_ quantum channel
End

The major processes for returning the generated bits based on the polarization received are shown in the second algorithm. The server starts by creating a random number and calculating the key to extract the error bit after receiving the polarization and measurement operation by using the steps of algorithm 2.

This algorithms, rather than Deffie Hellman, is used in the AES algorithm to exchange keys based on the features of the BB84 protocol.

Algorithm 2: Key exchange in receiver
Input: r P (Private Key)
Output: Received Polarized Photons through Quantum channel.
Begin
1- Generate Key IDs (N) BB84 Bases **//range (1- N) // N number of Received Polarized Photons**
2- for i →1 to N do
function: Measure Photon (Polarized Photons, Key IDs)
If (Polarized Photon == H & Key ID == '+') then Raw Key = 0 end if
If (Polarized Photon == V & Key ID == '+') then Raw Key = 1 end if
If (Polarized Photon == R & Key ID == 'x') then Raw Key = 0 end if
If (Polarized Photon == L & Key ID == 'x') then Raw Key = 1 end if
End Measuring photons End for
3- Calculate error bits.
End

To set up this network, the Contiki operating system and the Cooja simulator is used to construct a WSN made up of sensors and sinks (**WisMote**) In the cooja simulation, the WSN is shown in Fig. 2.

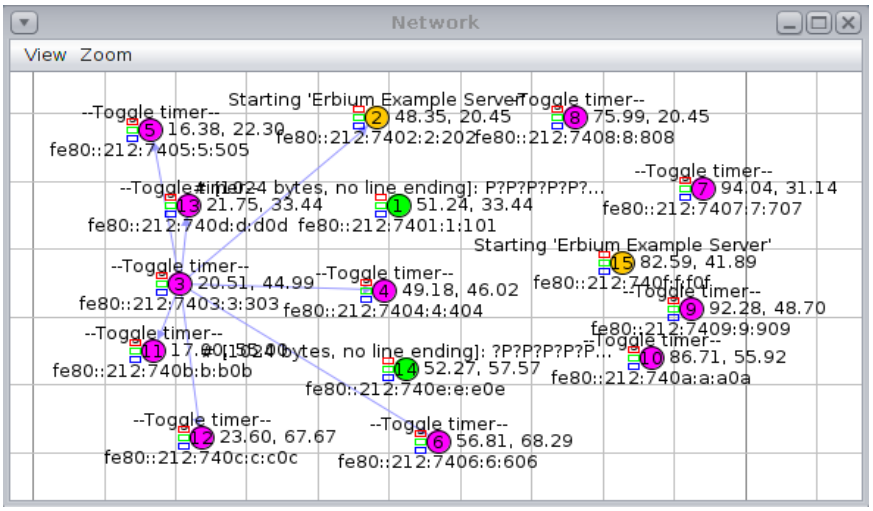


Figure 2 . Network in cooja Simulation

The mechanism of QKD within AES is used to authenticate and encrypt data based on the key generated by BB84. The BB84 protocol key is used to generate key material within the data encryption process in AES algorithm protocol for the WSN environment. Fig. 3 represents the diagram of the properties used for BB84 in QKD with the AES algorithm instead Deffie Hullman, such as a case study to exchange the key for encryption and decryption the data and to enhance the security in WSN.

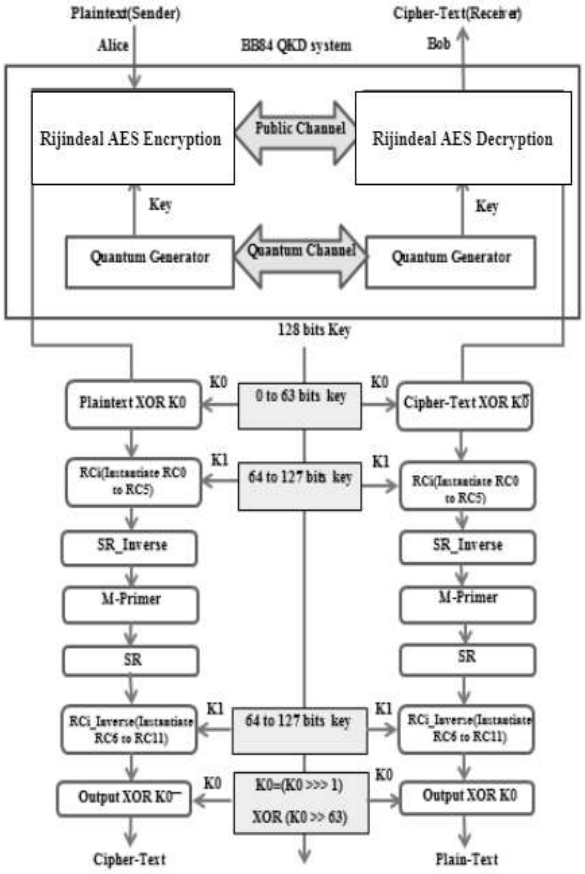


Figure 3 . AES with BB84 Protocol

After designing the WSN, the network was run through simulation, observing the connections between clients and servers, as well as the network's output, which is displayed in Fig. 4 as a Bit Array, packet data, and power trace.

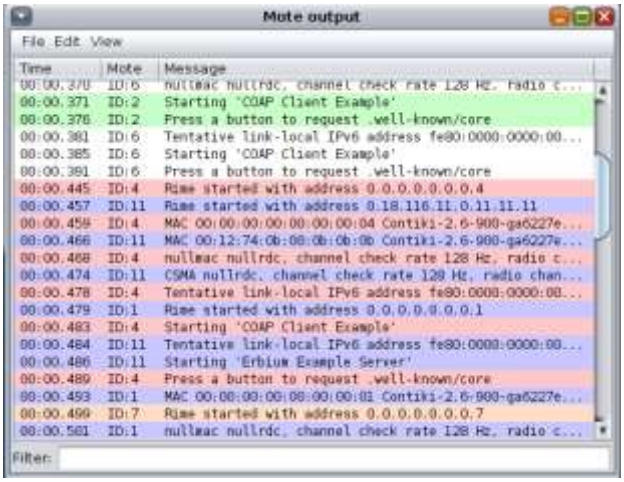


Figure 4. Mote output

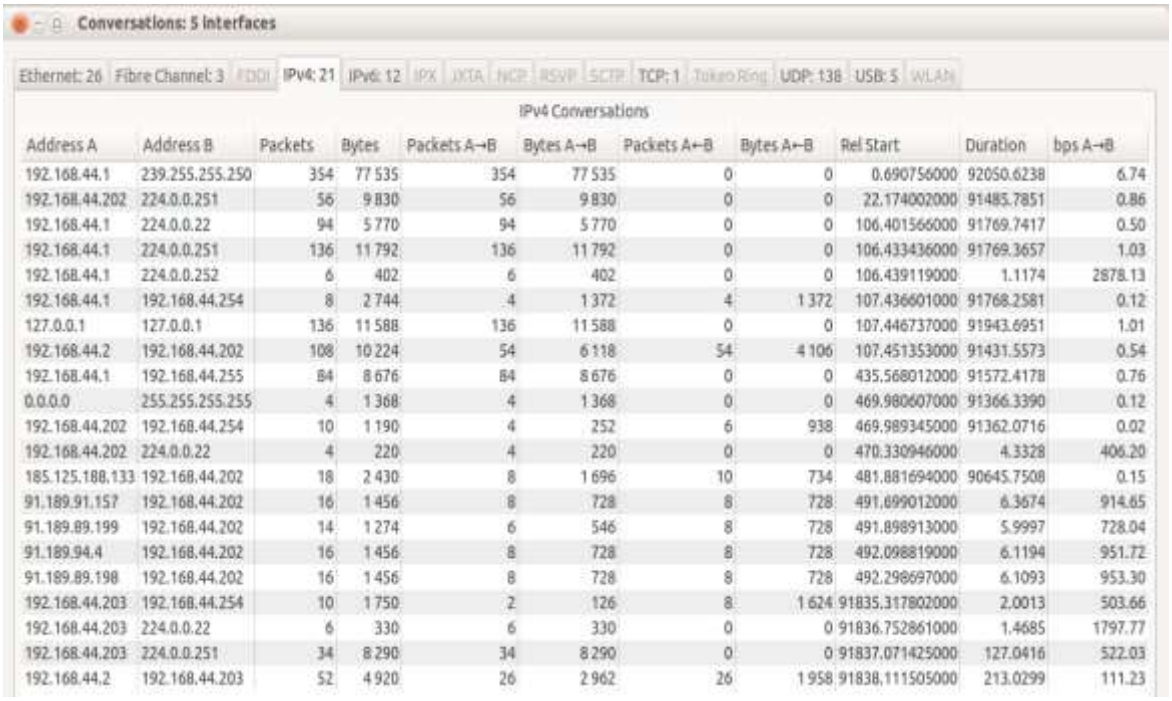
Results and Discussion:

The current study aims towards the identification of the features with the highest significance and which have established and analyzed integrating the WSN in the cooja simulator, which aims to strengthen the environment's security, to prove the enhancement protocol's algorithm.

The network's output shows that data authentication in these nodes takes a bit longer than the conventional protocol, about one second, but is more secure and saves energy for each WSN node.

The result of the work analysis using the Wireshark, Fig. 5 represents the captured packet using in the proposed protocol in WSN, IPV4 address of the source and destination, clarification the throughput, and packet loss of WSN.

Where the percentage of transmission, communication delay and the amount of sent and received packets between each nodes in WSN are displayed.



Conversations: 5 Interfaces

Ethernet: 26 | Fibre Channel: 3 | FDDI | IPv4: 21 | IPv6: 12 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 1 | Token Ring | UDP: 138 | USB: 5 | WLAN

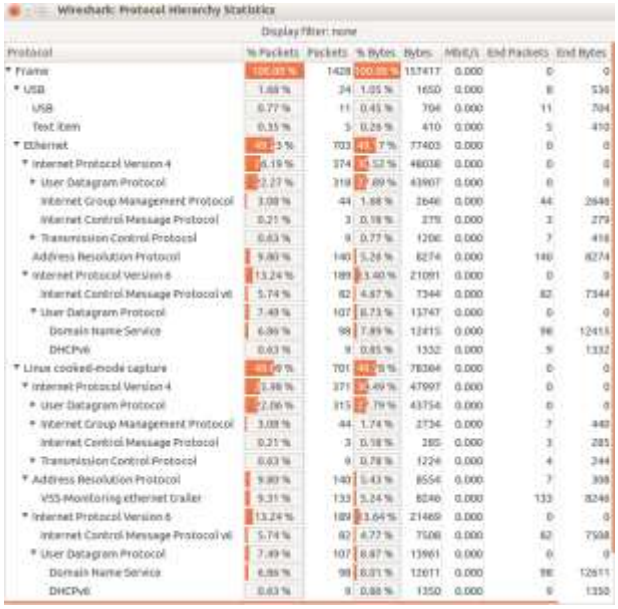
IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B
192.168.44.1	239.255.255.250	354	77 535	354	77 535	0	0	0.690756000	92050.6238	6.74
192.168.44.202	224.0.0.251	56	9 830	56	9 830	0	0	22.174002000	91485.7851	0.86
192.168.44.1	224.0.0.22	94	5 770	94	5 770	0	0	106.401566000	91769.7417	0.50
192.168.44.1	224.0.0.251	136	11 792	136	11 792	0	0	106.433436000	91769.3657	1.03
192.168.44.1	224.0.0.252	6	402	6	402	0	0	106.439119000	1.1174	2878.13
192.168.44.1	192.168.44.254	8	2 744	4	1 372	4	1 372	107.436601000	91768.2581	0.12
127.0.0.1	127.0.0.1	136	11 588	136	11 588	0	0	107.446737000	91943.6951	1.01
192.168.44.2	192.168.44.202	108	10 224	54	6 118	54	4 106	107.451353000	91431.5573	0.54
192.168.44.1	192.168.44.255	84	8 676	84	8 676	0	0	435.568012000	91572.4178	0.76
0.0.0.0	255.255.255.255	4	1 368	4	1 368	0	0	469.980607000	91366.3390	0.12
192.168.44.202	192.168.44.254	10	1 190	4	252	6	938	469.989345000	91362.0716	0.02
192.168.44.202	224.0.0.22	4	220	4	220	0	0	470.330946000	4.3328	406.20
185.125.188.133	192.168.44.202	18	2 430	8	1 696	10	734	481.881694000	90645.7508	0.15
91.189.91.157	192.168.44.202	16	1 456	8	728	8	728	491.699012000	6.3674	914.65
91.189.89.199	192.168.44.202	14	1 274	6	546	8	728	491.898913000	5.9997	728.04
91.189.94.4	192.168.44.202	16	1 456	8	728	8	728	492.098819000	6.1194	951.72
91.189.89.198	192.168.44.202	16	1 456	8	728	8	728	492.298697000	6.1093	953.30
192.168.44.203	192.168.44.254	10	1 750	2	126	8	1 624	91835.317802000	2.0013	503.66
192.168.44.203	224.0.0.22	6	330	6	330	0	0	91836.752861000	1.4685	1797.77
192.168.44.203	224.0.0.251	34	8 290	34	8 290	0	0	91837.071425000	127.0416	522.03
192.168.44.2	192.168.44.203	52	4 920	26	2 962	26	1 958	91838.111505000	213.0299	111.23

Figure 5. IPV4 conversation

Fig. 6 displays the percentage of packets based on the frame, amount of packets and bytes, and other factors in Wireshark's protocol Hierarchy Statistical. The key for encryption is an important parameter in the security process; according to NIST statistics with the different percentage of analysis and statistical that make this protocol safer.

The important parameter in security process is the key for encryption, the percentage of generated bits key around 80%-95% based on NIST statistical (Using Random Test) that makes protocol stronger for security as shown in Fig.6.



Wireshark: Protocol Hierarchy Statistics

Display Filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes
Frame	100.00 %	1428	100.00 %	157417	0.000	0	0
USB	1.68 %	24	1.05 %	1650	0.000	8	536
USB	0.77 %	11	0.41 %	704	0.000	11	704
Text item	0.35 %	5	0.26 %	410	0.000	5	410
Ethernet	49.23 %	703	49.17 %	77403	0.000	0	0
Internet Protocol Version 4	26.19 %	374	29.52 %	46488	0.000	0	0
User Datagram Protocol	22.27 %	318	27.89 %	43907	0.000	0	0
Internet Group Management Protocol	3.08 %	44	1.68 %	2646	0.000	44	2646
Internet Control Message Protocol	0.21 %	3	0.18 %	279	0.000	3	279
Transmission Control Protocol	0.63 %	9	0.77 %	1208	0.000	7	416
Address Resolution Protocol	9.80 %	140	5.24 %	8274	0.000	140	8274
Internet Protocol Version 6	13.24 %	189	13.40 %	21091	0.000	0	0
Internet Control Message Protocol v6	5.74 %	82	4.67 %	7344	0.000	82	7344
User Datagram Protocol	7.49 %	107	8.73 %	13747	0.000	0	0
Domain Name Service	6.86 %	98	7.89 %	12415	0.000	98	12415
DHCPv6	0.63 %	9	0.85 %	1332	0.000	9	1332
Linux cooked-mode capture	49.79 %	701	49.83 %	78384	0.000	0	0
Internet Protocol Version 4	26.58 %	371	29.49 %	47997	0.000	0	0
User Datagram Protocol	22.06 %	315	27.79 %	43754	0.000	0	0
Internet Group Management Protocol	3.08 %	44	1.74 %	2734	0.000	7	448
Internet Control Message Protocol	0.21 %	3	0.18 %	285	0.000	3	285
Transmission Control Protocol	0.63 %	9	0.78 %	1224	0.000	4	244
Address Resolution Protocol	9.80 %	140	5.43 %	8554	0.000	7	398
VSS-Monitoring ethernet trailer	9.31 %	133	5.24 %	8240	0.000	133	8240
Internet Protocol Version 6	13.24 %	189	13.64 %	21469	0.000	0	0
Internet Control Message Protocol v6	5.74 %	82	4.77 %	7508	0.000	82	7508
User Datagram Protocol	7.49 %	107	8.67 %	13961	0.000	0	0
Domain Name Service	6.86 %	98	8.01 %	12611	0.000	98	12611
DHCPv6	0.63 %	9	0.86 %	1350	0.000	9	1350

Figure 6 . Wireshark Statistical

Also, there is a table for QBER for BB84 protocols that show the result of QBER depending on the following equation:

$$\text{QBER} = \frac{Nerror}{Ncorrect + Nerror}$$

$$\left(\frac{Number\ of\ bits\ error}{Number\ of\ correct\ bits + Number\ of\ bits\ error}\right)$$

Table 1 shows the result of equation to calculate the QBER with BB84 protocol in WSN environment which appears the low values of errors and high values of efficiency.

Table 1. QBER and Efficiency for BB84

Nerror	Ncorrect + Nerror	QBER	Efficiency
Nerror : 208	Ncorrect + Nerror is :512 bit	QBER : 0.406	0.594
Nerror : 215	Ncorrect + Nerror is :512 bit	QBER : 0.419	0.581
Nerror : 102	Ncorrect + Nerror is :256 bit	QBER : 0.398	0.602
Nerror : 86	Ncorrect + Nerror is :256 bit	QBER : 0.335	0.665
Nerror : 106	Ncorrect + Nerror is :256 bit	QBER : 0.414	0.586
Nerror : 38	Ncorrect + Nerror is :128 bit	QBER : 0.296	0.704

Fig. 7 shows the mechanism for analyzing the network protocol and network data when the packet is sent through Mote nodes at intervals time using the UDP protocol as a filter.

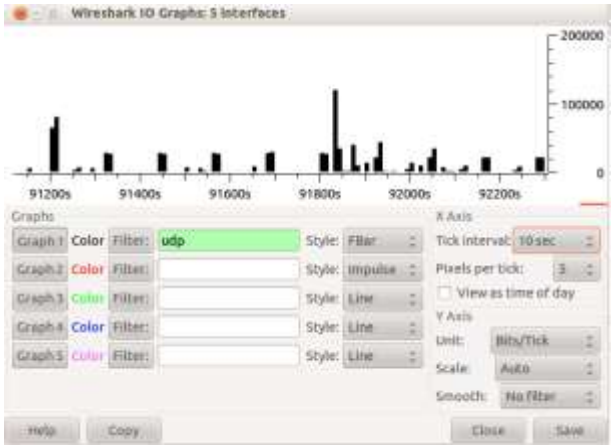


Figure 7 . WSN graph analysis

In Wireshark analysis, the conversation using in the all of the interfaces for (Ethernet, IPv4, IPv6, TCP, UDP), In Ethernet analysis calculates the (time, bytes array, packets, rel start (relative time), duration) that Show the relationship between the byte arrays and time while commencing the operation in Fig. 8, which signifies higher data security based on all result of Wireshark Statistical.

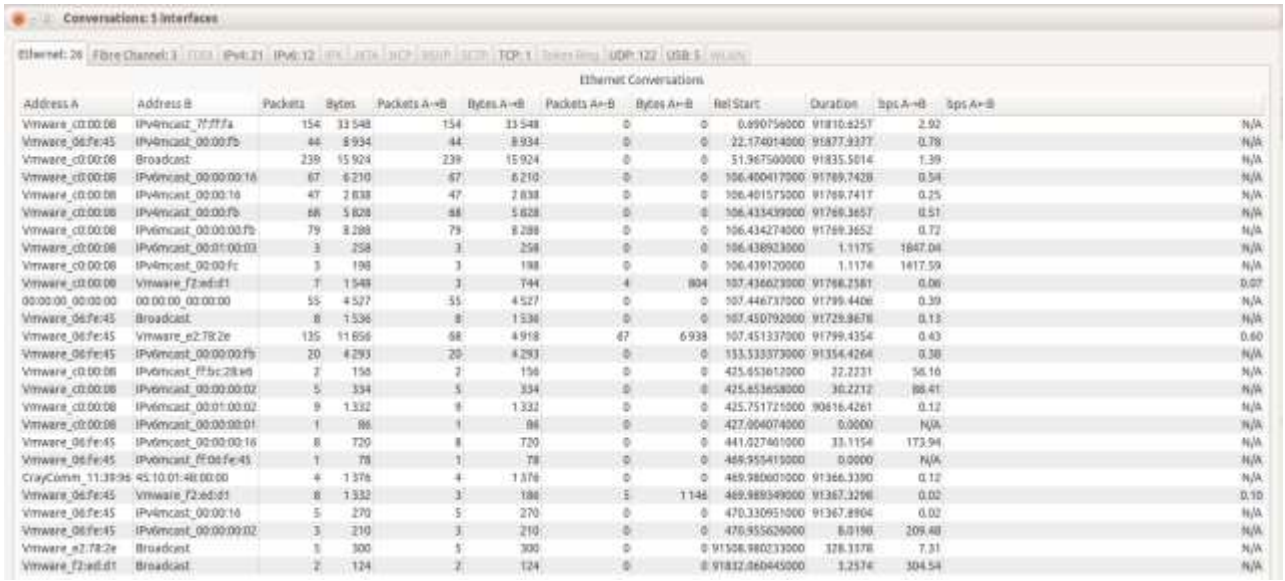


Figure 8 . Ethernet conversation

In addition, the conversation for UDP analysis appears the data result (address(A,B), ports, packets, bytes, real-time start, duration) for request and response between Mote node in WSN, this values and others represented in Fig. 9.

Using UDP statistical can display and know the values and percentage of transmission, communication delay and the amount of sent and receive packets between each nodes in WSN.

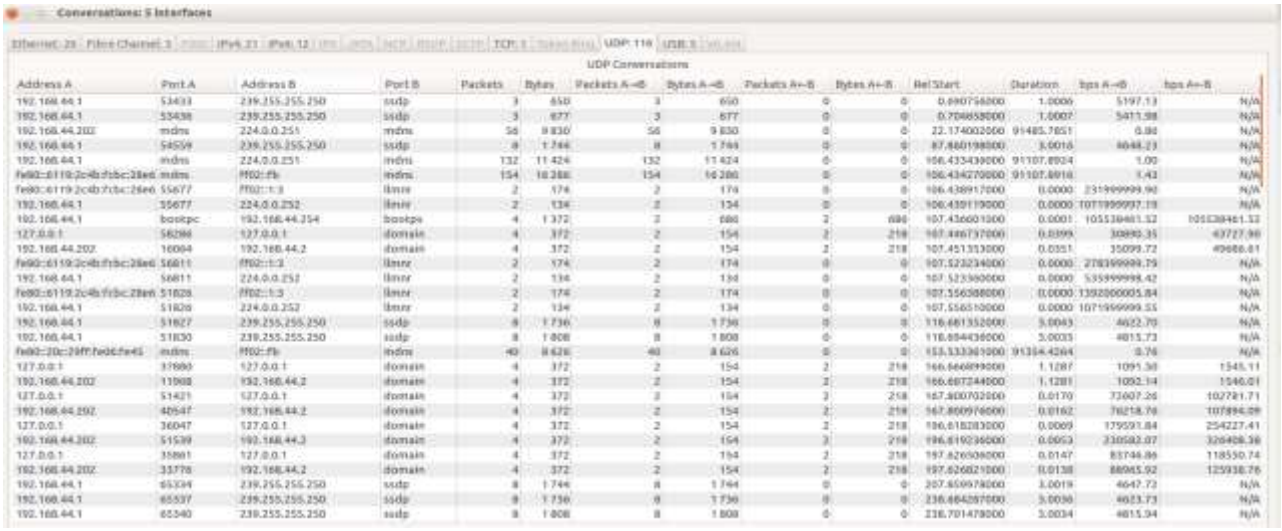


Figure 9 . UDP statistical

Conclusion:

Security requirements for sensors in WSN environments are becoming more stringent, and the interest in using quantum computing has grown significantly, so this paper proposed to enhance WSN security based on quantum properties by using about (80-95)% from randomly generated bits in the BB84 protocol that ensures high security among sensors in WSN. Security was سimproved by exploiting the best proportion of the generated key compared to classical algorithms, to achieve high security and efficiency in the performance of WSN by implementing AES algorithm with quantum computing, which reduces packet lost in the network based on the results obtained. As a result, our proposed method is effective in ensuring the confidentiality of user data in WSN, reducing time consuming of transmitted packets between nodes in WSN and adding high secure key exchange between sender and receiver.

Authors' declaration:

-Conflicts of Interest: None.

-We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.

-Ethical Clearance: The project was approved by the local ethical committee in department of Environmental Engineering, University of Babylon.

Authors' contributions statement:

L.A suggested the idea by Conception, design, execute and drafting the MS. A.A take a part of analysis, interpretation of the results, revision and proofreading the MS, and the reviewers provided some suggestions which improved the quality of the work.

References:

1. Medhat K, Ramadan RA, Talkhan I. Distributed Intrusion Detection System for Wireless Sensor Networks. Proc - NGMAST 2015 9th Int Conf Next Gener Mob Appl Serv Technol. 2016; 234–9.
2. JV A. Trust-Value Based Wireless Sensor Network Using Compressed Sensing. J Electron Informatics. 2020; 2(2):88–95.
3. Heigl M, Schramm M, Fiala D. A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication. 2019 IEEE Int Conf Pervasive Comput Commun Work PerCom Work 2019. 2019; 906–11.
4. Mehic M, Fazio P, Voznak M, Chromy E. Toward designing a quantum key distribution network simulation model. Adv Electr Electron Eng. 2016;14(4Special Issue):413–20.
5. Bhatia P, Sumbaly R. Framework for Wireless Network Security Using Quantum Cryptography. Int J Comput Networks Commun. 2014; 6(6):45–61.
6. Batra I, Verma S, Kavita, Alazab M. A lightweight IoT-based security framework for inventory automation using wireless sensor network. Int J Commun Syst. 2020; 33(4):1–16.
7. Journal I, In D, Kishore PK. An Efficiency of Security and Quantum Cryptography in Wireless Sensors Networks. (5):581–6.
8. JV A. Trust-Value Based Wireless Sensor Network Using Compressed Sensing. J Electron Informatics. 2020;2(2):88–95.
9. Lohachab A. Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure. SSRN Electron J. 2018;
10. Saeedi IDI, Al-Qurabat AKM. Perceptually Important Points-Based Data Aggregation Method for Wireless Sensor Networks. Baghdad Sci J. 2022; 19(4):875–86.
11. Rahat AAM, Everson RM, Fieldsend JE. Evolutionary multi-path routing for network lifetime and robustness in wireless sensor networks. Ad Hoc Networks. 2016; 52:130–45.
12. Rathore H, Badarla V, Shit S. Consensus-aware sociopsychological trust model for wireless sensor networks. ACM Trans Sens Networks. 2016;12(3)..
13. Abdullah AA, Mahdi SS. Hybrid quantum-classical key distribution. Int J Innov Technol Explor Eng. 2019; 8(12):4786–91.
14. Jassem YH, Abdullah AA. Enhancement of quantum key distribution protocol for data security in cloud environment. ICIC Express Lett Part B Appl. 2020; 11(3):279–88.
15. Chiadighikaobi IR, Katuk N. A scoping study on lightweight cryptography reviews in IoT. Baghdad Sci J. 2021; 18(2):989–1000.
16. Lavanya M, Natarajan V. LWDSA: light-weight digital signature algorithm for wireless sensor networks. Sadhana - Acad Proc Eng Sci. 2017; 42(10):1629–43.
17. Shahra EQ, Sheltami TR, Shakshuki EM. A comparative study of range-free and range-based localization protocols for Wireless Sensor Network: Using COOJA simulator. Int J Distrib Syst Technol. 2017; 8(1):1–16.
18. Bhatt AP, Sharma A. Quantum cryptography for internet of things security. J Electron Sci Technol. 2019; 17(3):213–20.
19. Heigl M, Schramm M, Fiala D. A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication. 2019 IEEE Int Conf Pervasive Comput Commun Work PerCom Work 2019. 2019; 906–11.
20. Hu C, Cheng X, Tian Z, Yu J, Akkaya K, Sun L. An attribute-based signcryption scheme to secure attribute-defined multicast communications. Lect Notes Inst Comput Sci Soc Telecommun Eng LNICST. 2015; 164: 418–37.

21. Madhu R, Neelima B. Performance analysis of DTLS protocol. 2017 Int Conf Intell Comput Instrum Control Technol ICICICT 2017. 2018;2018-Janua:331–4.

تحسين أمان شبكة المستشعرات اللاسلكية باستخدام توزيع المفاتيح الكمية

ليث حامد الحسناوي **امير علي كاظم**

رئاسة جامعة بابل، جامعة بابل، بابل، العراق.

الخلاصة:

تعمل شبكات الاستشعار اللاسلكية على تعزيز انتشار الإنترنت للأجهزة في جميع مجالات الحياة ، مما يجعلها تقنية واعدة في المستقبل. في الأيام المقبلة ، مع زيادة تطوير تقنيات الهجوم ، سيكون للأمن دور مهم في شبكات الاستشعار اللاسلكية. حاليًا ، تشكل أجهزة الكمبيوتر الكمية خطرًا كبيرًا على تقنيات التشفير الحالية التي تعمل جنبًا إلى جنب مع أنظمة الكشف عن التسلل لأنه من الصعب تنفيذ الخصائص الكمية على أجهزة الاستشعار بسبب محدودية الموارد. في هذا البحث ، تُستخدم الحوسبة الكمية لتطوير نهج مقاوم للمستقبل وقوي وخفيف الوزن ومراعي للموارد لشبكات الاستشعار. يتم التركيز بشكل كبير على مفاهيم استخدام بروتوكول BB84 مع خوارزمية معيار التشفير المتقدم في أمان شبكات الاستشعار اللاسلكية . تشير نتائج التحليل إلى مستوى عالٍ من الأمان بين البيانات بالاعتماد على توليد مفاتيح آمنة وتصل إلى معدل دقة حوالي (80-95)٪ بناءً على استخدام إحصائية NIST. زادت كفاءة العمل إلى 0.704 بعد استخدام معادلة معدل خطأ بت الكم مما أدى في النهاية إلى زيادة أداء الشبكة. ينتج عن هذا تقليل الكمية الإجمالية للطاقة ، وانخفاض الوقت اللازم لإجراء تبادل المفاتيح في عمليات التشفير وفك التشفير.

الكلمات المفتاحية: بروتوكولBB84، توزيع مفتاح الكم ، شبكة الاستشعار اللاسلكية ، معدل خطأ بت الكم، معيار التشفير المتقدم.