Analysis of Key Management and Quantum Cryptography in Wireless Sensors Networks

Vijey Thayananthan and Ahmed Alzahrani
Computer Science Department,
Faculty of Computing and Information Technology,
King Abdul Aziz University,
Jeddah 21589, Saudi Arabia.

ABSTRACT

Key management and quantum cryptography (QC) are very interesting and challenging areas in wireless sensor networks (WSN). In order to make secure communications around WSN, communication between sensor nodes and base station to sensor node communication should be handled carefully. Today's security around WSN needs efficient key management protocol and QC involved with quantum mathematical procedures and quantum physics [1]. According to the key management analysis, computational complexities of conventional and potential cryptography are very high. In order to avoid high complexity in key management, QC can be used because it is involved with quantum computation [4][5]. Quantum key distribution (QKD) is already established with laws of quantum mechanics influenced to quantum computations for some networks such as fiber optic, satellite based communication etc. Therefore, efficient approach of QC will be analyzed to manage the keys with maximum security and less complexity. Key management protocol [2][3] in wireless networks is influenced with authentication which uses symmetric or asymmetric cryptography. Authentication and entities in upper layers use public key cryptography [6].

In this paper, we propose an enhanced version of key management and QC for WSN. Thus, we modify authentication protocol between the access points and wireless sensor network with symmetric polynomial based on QC approach. In modern QC, there are possibilities for which quantum computation techniques allow to expand the bandwidth. It is another interesting area in QC because bandwidth expansion will increase the level of security in WSN.

General Terms

In this paper, QC is considered as my general term. Throughout this research, key management analysis is considered in wireless sensors networks.

Keywords

Key management, QC, complexity, WSN, authentication

1. INTRODUCTION

Key management in wireless networks is influenced with authentication. Cryptography is about scrambling data or information so that it is unreadable known as encryption or cipher text. In the decryption, person who knows the secret key can decode the data or information. So far, cryptosystem use complex software based on long computations to manage keys. Still, intruders are trying to copy the key and decode all the necessary data or information without any evidence of their snooping.

QC is a powerful method to protect voice, data or video over wireless networks and communications. Instead of sending keys, QC technology generates secure key dynamically. In addition to this, QC based on quantum mechanics provides maximum security. In QC, the sender uses a string of quantum bits (qubits) to the receiver where each qubit is represented single photons. If an eavesdropper tries to intercept them, state of the photons will not allow eavesdropper to do that because the state is changing continuously. In addition to this, sender and receiver will be notified if there is any eavesdropping when a string of qubits is transmitted. That particular qubits shouldn't be used for key establishment. In this research, different qubits are analyzed for key management. In digital cryptography, chances of eavesdropping are high, and it is impossible to detect because of binary nature. Entanglement of qubits provides better design solutions in QC algorithms.

Wireless sensors integrated with security monitoring equipment, and wireless networks are widely used in most of the computer and communication applications. WSN is one of the growing areas where we need to focus on maximum security and how to manage and implement the key for future protections. Specially, WSNs are already employed in medical, business and educational organizations without considering any security issues addressed in [4]. In the next generation of cloud computing or current communication, WSNs are predicted to become ubiquitous. They provide a number of advantages economically, so wherever WSN is involved in the networks should be monitored properly. Using correct security mechanism and key management, unique security challenges of active and passive attacks can be minimized. Sensors connected in WSN are interacted by many objects such as physical environments, people etc. Using QC and developing key management for WSNs is quite challenging because sensors' capacities are different.

Thousand to millions of wireless sensors used in the wireless networks with some challenges they are such as processing power, bandwidth, energy consumption and storage. We need to surmount these challenges with QC and efficient key management because security between the sensor nodes and around the sensors is involved directly and indirectly with above mentioned challenges. Some applications of sensor network are emergency response information, energy management, medical monitoring, logistic and inventory management, and battlefield management.

The rest of this paper is organized as follows. Related work of key management and its protocols for WSN are reviewed in Section 2. We discuss QC and its advantages for WSN applications in Section 3. Public and secret key with QC are also discussed. In Section 3, symmetric cryptography and QC approach are given. Performance evaluation and an analysis are presented in Section 5. Finally, some conclusions are given in Section 6.

2. KEY MAMAGEMENT FOR WSN

In WSN, key management focused on three key agreements [3] is analysed. They are trusted server, self-enforcing and pre distribution respectively. First two key agreements are not suitable in WSN because the number of sensors and physical properties of each sensor used in the network are different.

2.1 Key management Protocol in WSN

In WSN, number of key management protocols (KMP) is proposed already, but most of them are not depended to QC. Although few of these protocols are depended on QC, they are built for different applications.

Localized Encryption and Authentication Protocol (LEAP) is a one of the KMP [7]. It can be employed in large-scale WSN with four types of keys they are such as individual keys, pair-wise shared keys, cluster keys and group keys respectively. It is memory efficient, but authentication of sensor node needs high computations. As in [8], key management is established with pair-wise key between the access point and wireless sensor nodes. This protocol is not power efficient. The Security Protocols for Sensor Networks (SPINS) is a protocol for data authentication, which provides protection to two parties. In this protocol, two sensor nodes used in the WSN cannot authenticate each other directly. Here, key management and authentication consider the base station as a trusted server.

Low Energy Adaptive Clustering Hierarchy (LEACH) is used in WSN as an interesting security. Although it was proposed to reduce the energy consumption in WSN [10], the improved version of LEACH is supporting to KMP development.

2.2 WSN assumptions

Sensor must be fixed in the network. It means that sensor nodes are not mobile. Key server used as a base station should have long-lasting power. Each sensor is identical in terms of power, computing and communication. Each node should have enough space to store some keying materials. Neighbouring nodes shouldn't be known in advance. Physical layer of WSN should be cleaned.

3. QUANTUM CRYPTOGRAPHY

The literature review presents that QC is a very powerful secure technique in which all tasks are computed by quantum physics and computing theory. It is not pure mathematical evolution but is a combination of conventional cryptography, information theory and quantum mechanics. Here, photons and spin particles are involved to implement QC schemes. In order to understand the design of QC, the behavior and properties of particles used in the QC development should be analyzed. In conventional cryptography and information theory, computations of design and implementation complexities are unavoidable but quantum computing techniques solve these problems in QC developments. The laws of quantum physics and mechanic guarantee the security of QC protocols. The BB84 protocol is the first QC protocol, which was proposed by Bennett and Brassard in 1984.

3.1 Public and secret key with QC

As conventional cryptosystem, there are two types of cryptosystem in QC they are public and secret key cryptography. In public-key cryptography, a pair of keys is used in encryption and decryption. QC often contrasted with security offered by public key cryptography. In secret-key cryptography, also referred to as symmetric cryptography, the same key is used for both encryption and decryption. To build an unconditionally secure authentic channel in the key management, we require a symmetric key cryptography to be pre-distributed to every pair of communicating parties.

3.2 Challenges of QC in WSN

In this paper, the symmetric cryptography is chosen to analyse the key management which will be explained in the next section broadly. In this protocol, sender and receiver use a qubits and quantum channel for their communication.

In security development for WSN, following technical challenges are considered in key management [9].

1) WSN with a large number of sensors, Unanticipated advances calculations in sensor computations, high-performance computing, and the possibility of large-scale QC complexities.
2) WSN configurations and dynamic approach with a group of users in future secure network communications.
3) QC projections in WSN are evolving with future technology, which is growing bandwidth demands, powerful secure communications and less complexity.

4. SYMMETRIC WITH QC

In this approach, key management is established for WSN with where QC is introduced using suitable algorithm. In order to establish trusted communications between sensor nodes, secure protocols should be used with proper key management and QC. In symmetric key cryptographic design, the use of one key is involved. In this design, block cipher based on symmetric and QC is considered as proposed method.

4.1 Security design

In this section, we show the security design of key management and QC. Following figure shows use of symmetric key in the key management.

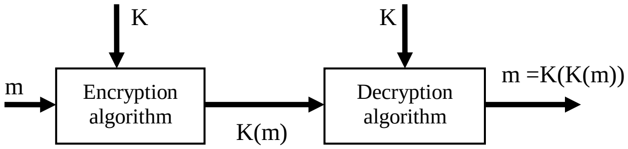

Figure 1: Block diagram of symmetric cryptography

Plain text message (m) key (K) and cipher-text (K(m)) are indicated in Figure 1.

In symmetric key developments, two types of ciphers are considered. They are stream ciphers and block ciphers respectively. In stream ciphers, encryption is performed with one bit at the time. In block ciphers, encryption is performed as a block of bits.

4.2 Steam ciphers

In this processing, key-stream, which is known as pseudo random bits is generated using key-stream generator. For instance, the Figure 1 can be used as steam cipher where the principle of a synchronous and data processing are used with polynomial..

m(i) = ith bit of message
K(i) = ith bit of keystream
C(i) = ith bit of ciphertext
$C(i) = K(i) \oplus m(i)$ ($\oplus$ = exclusive or)
$m(i) = K(i) \oplus C(i)$

In steam ciphers, RC4 steam cipher is a popular to form a symmetric cryptographic development. In addition to this, RC4 stream cipher scheme enables to organize key management and QC efficiently. Different size of keys are obtainable, specifically, 1 to 2048 bits are used in RC4. It also can be used in secure socket layer (SSL).

4.3 Block ciphers

In the WSN environment, block cipher approach increases the efficiency of security. Block ciphers are constructed from three basic components they are permutations (or transposition), substitutions and arithmetic operations. Permutation introduces the diffusion in the cipher text. Substitutions introduce the confusion, which has the effect of making the plain or cipher text transformation depend on the key management. Arithmetic operations such as binary bits and qubits can introduce either diffusion or confusion or both.

The block of bits is processed during the encryption. In the proposed approached 128-bit blocks will be considered to analyse with QC. Table I shows the simple example of 4-bit block ciphers.

Table I Example of 4 bit block cipher

Inputs	Outputs	Inputs	Outputs
0000	1001	1000	1100
0001	1010	1001	1101
0010	1011	1010	1110
0011	1000	1011	1111
0100	0000	1100	0100
0101	0001	1101	0101
0110	0010	1110	0110
0111	0011	1111	0111

Through this example, $2^n! = 16!$ mappings are used. Therefore, processing takes more time to implement the high security in WSN environment.

Proposed method uses 128-bit blocks with table approach, which requires table with 2^{128} entries. In this approach, each entry has 128 bits, it means that the table is too big and high complexity. In order to avoid this high complexity, qubits are used instead of binary bits.

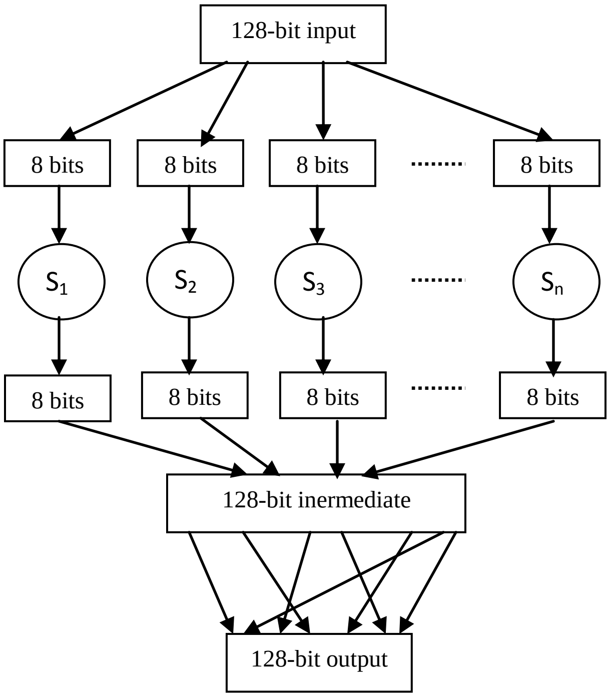

Figure 2: Block cipher based on symmetric cryptography

Basic model of block ciphers configuration is shown in Figure 2, which can be extended to n number of blocks. Here, 8 bits are used in each block, so n = 16.

Figure 2 shows a single loop in the selected (128 bits) block cipher approach. If only a single round, then one bit of input affects at most 8 bits of output. In 2nd round, the 8 affected bits get scattered and inputted into multiple substitution boxes. Here, efficiency of security is depending on the number of rounds.

Authentication uses symmetric cryptography which is created from symmetric polynomials with following terms.

$$\begin{cases} 0 \le N_i - 2 \le t \\ t \ge N_i \left(\sqrt[r+1]{\dfrac{r(r+1)!}{2}} \right) \end{cases} \qquad i = 1,2,3..r \qquad (1)$$

Where N_i is the number of sensor nodes in group i. According to the equation (1), the ratio between t and N_i is given in [2]. In symmetric polynomial, r-tuple identity from the key management is used in sensor nodes and stored in the memory.

$$t \geq \sqrt[r+1]{\frac{N_i^2 r(r+1)!}{2}} \qquad (2)$$

Table II shows the coefficients of polynomial for selected number of sensors with *r*. Here, polynomial degree t is an indication of memory usage, processing capability and security levels used key management.

Table II Coefficients of the polynomial used in WSN

r	**N_i**	**t**
1	1	1
2	10	17.715
3	100	239.19
4	1000	2921.9
5	10000	34058

Coefficients increase complexity and reduce the processing time in the key management of WSN. Therefore, QC can be considered with different qubits implementations. When number of sensors is increased to millions or more, security algorithms based on QC will be better. Specially, symmetric cryptography development with QC approach will not only reduce the complexity but also it will increase the processing time.

5. ANALYSIS

In key management and QC analysis, security details of WSN, number and properties of sensors in WSN, environment and other interaction parameters around WSN have to be considered. Security details are based on the attacks influenced around or within the WSN.

5.1 Security analysis

In this section, we analyse and compare the proposed solution to few existing solutions. Applying LEAP and LEACH protocols in WSN with/without any modifications and addition provides us with some level of security.

5.2 Memory analysis and requirements

In WSN, each sensor node is identified by r-tuple and t coefficients. In this paper, QC helps to reduce the memory size when coefficients are increased in the WSN.

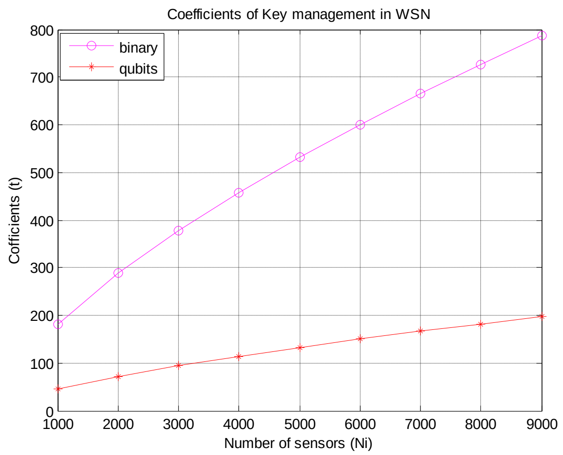

Figure 3: comparison of symmetric cryptography with and without QC

As shown in Figure 3, QC can be employed for a large number of sensors connected in WSN. Here, 2 qubits scheme is used in equation (2). If 2 qubits are allowed, 4 locations are needed to store necessary information mentioned in [5] but QC stores all 4 data simultaneously in given a moment.

Table III Comparison of QC with reference [2]

Challenges in key management	Using equation (2) and reference [2]	QC (2 qubits)
Memory requirements	X bits	X/4
Bandwidth consumption	X bits	X/4
Requirement processing	Y bits	Y/4

Bits X and Y given table III depend on the number of nodes, key lengths and coefficients of the symmetric polynomial [2].

6. CONCLUSIONS AND FUTUR WORK

As conclusions, key management and QC is analyzed for future WSN. Key management including key distribution is a difficult problem in all cryptographic algorithm developments but proposed approach can provide a better solution for this problem than potential QC. Key management based on QC will be better for most of the future security control in wireless applications because this new approach uses less complexity and minimum computation time.

In this paper, key management and QC are analyzed for future wireless networks. Key management including key distribution is a difficult problem in all cryptographic algorithm development but quantum approach can provide a better solution for this problem than potential QC because still a limited number of qubits is used in the QC algorithms.

Even though, no real quantum computer has been completed yet properly, prediction results and analysis of trellis coding have been studied thoroughly. When commercial quantum system is available, number of pending problems will be solved.

Specially, cryptography and trellis-coding are expected to use large numbers to make a strong security by 2020. Again, code breakers are also increased because faster system will break it within the fraction of the second than the conventional system.

6.1 Future work

The block ciphers, which increase the efficiency of security in WSN should be optimized with existing technical challenges used in key management and QC. Here, symmetric cryptographic algorithm should be modified. Not only existing challenges but also future innovation will be analyzed to maintain key management with QC. In addition to this, other existing protocols and algorithms of cryptography for WSN should be modified to QC platforms.

7. REFERENCES

[1] S. Fehr. Quantum Cryptography, Centrum Wiskunde & Informatica (CWI), Springer, Amsterdam, The Netherlands, 2010.

[2] Ali Fanian, Mehdi Berenjkoub and T. Aaron Gulliver. An Efficient Authentication and Key Management Protocol for Hierarchical Ad hoc Sensor Networks, WCNC 2009 proceedings, 2009.

[3] J. Jang, T. Kwon, and J. Song. A Time-Based Key Management Protocol for Wireless Sensor Networks, E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328, 2007.

[4] Jason. Palmer, "Quantum computing device hints at powerful future". Science and technology reporter, BBC News, Dallas. http://www.bbc.co.uk/news/science-environment-12811199, 2011.

[5] Vijey. Thayananthan, "Analysis of Quantum Computing and Trellis Coding based on PUM Codes", International Journal of Computer Applications (IJCA), Vol. 30, No. 5, USA, Sept. 2011.

[6] Xu Huang, Shirantha Wijesekera and Dharmendra Sharma, Agent-Oriented Novel Quantum Key Distribution Protocol for the Security in Wireless Network, University of Canberra, Australia 2008.

[7] Rakesh M. Verma y and Bailey E. Basile, Modeling and Analysis of LEAP, a Key Management Protocol for Wireless SensorNetworks, Department of Computer Science University of Houston Houston, TX, 77204, USA http://www.cs.uh.edu Technical Report Number UH-CS-08-12, August 8, 2008.

[8] Q. Huang, H. Kobayashi, and B. Liu, "An unbalanced key establishment scheme for heterogeneous wireless networks," Proc. IEEE Global Telecommun. Conf., pp. 2169-2174, Nov.-Dec. 2004.

[9] Sufyan T. Faraj, Integrating Quantum Cryptography Into SSL, Special Issue of Ubiquitous Computing Security Systems, UbiCC Journal - Volume 5, 2007.

[10] Mohammed A. Abuhelaleh and Khaled M. Elleithy, Security In Wireless Sensor Networks: Key Management Module In SOOAWSN. International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.