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