Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.560 – 569

MPQC: Secure Authentication for Message Passing Via Quantum Cryptography

[1]T.Akila, [2]Dr. P.UmaMaheswari
[1]Research Scholar
[2]Professor & HOD, Department of Computer Science and Engineering
[1]Mahendra College of Engineering, Salem-106, TN
[1]Anna University, Chennai
akilaresearch01@gmail.com
[2]Anna University, Coimbatore
Umamaheshwariresearch01@gmail.com

Abstract— This article presents a classification and system of modern quantum technology of information security in Wireless Sensor network. It can be shown that while classical message authentication schemes are computationally difficult to attack, they are not information-theoretically secure. Furthermore, the computational requirements of a successful attack can be reduced via MPQC (Message Passing Quantum Cryptography) Protocol. The quantum technique for information security against attackers is carried out. The characteristics of the basic directions of quantum cryptography from the point of view of the quantum techniques are used is given. A qualitative analysis of the advantages and imperfections of concrete quantum protocols is made. The proposed scheme presents a novel method to construct secure quantum signature systems for future secure communications using genetic algorithm.

Keywords— Quantum cryptography, quantum key distribution, Error correction code, MPQC (Message Passing Quantum Cryptography), Genetic Algorithm

I. INTRODUCTION

Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities [1]. Wireless sensor networks are composed of a set of devices that communicate without using any permanently installed infrastructure by transmitting radio signals. The devices, also called as nodes of the network, generally use omnidirectional antennas and their transmission range is determined by the power they employ in the

transmission of the messages [2]. Sensors gather information about the state of physical world [3]. These sensors are limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, using some local decision process it can transmit the sensed data to the user. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure various properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is installed for wireless communication to transfer the data to a base station [4]. In a wireless sensor networks which is organized by cluster, there are two statuses of nodes: cluster heads and cluster nodes [5]. The clustering approach is done by cluster heads, in which the cluster heads are selected from sensor nodes and then the nodes become member of the nearest cluster head [6]. The nodes in the sensor networks comprise sensor nodes, sink gateway nodes and management nodes.

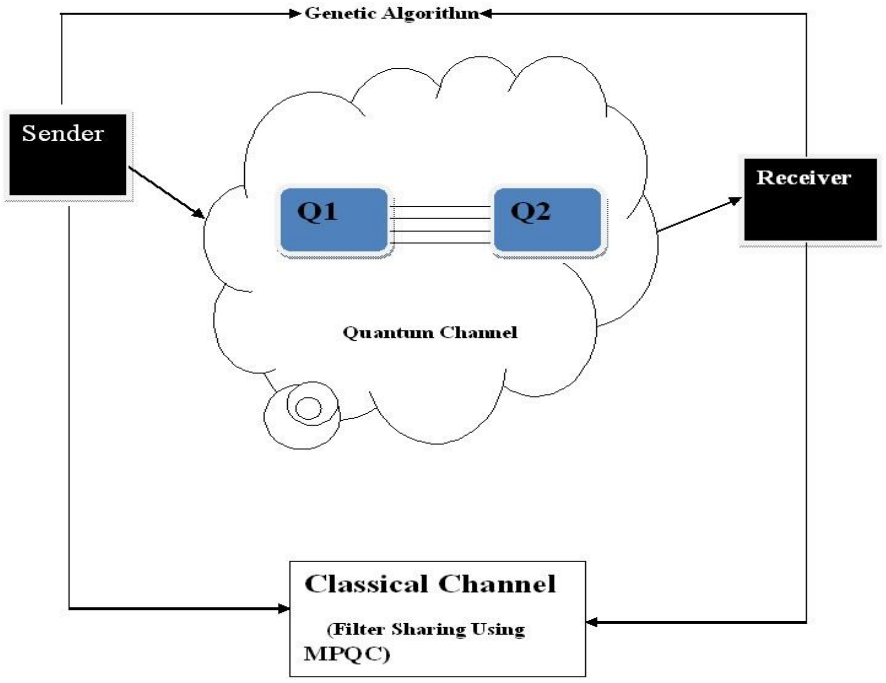

Fig.1 Architecture Diagram in MPQC

MPQC give a cumbersome, but effective, method of message verification using quantum bits that is information theoretically secure. A proof of its safety against forgery is provided. A method by which to distribute the keys necessary for signature verification is also presented. Ideas for further exploration and additional readings presented as well. One of the most effective ways of ensuring confidentiality and data integrity during transmission is cryptographic systems. The purpose of such systems is to provide key distribution, authentication, legitimate users authorization, and encryption. Key distribution is one of the

most important problems of cryptography. This problem can be solved with the help of[4]: classical information-theoretic schemes (requires channel with noise; efficiency is very low, 1–5%), classical public-key cryptography schemes (Diffie-Hellman scheme, digital envelope scheme; it has computational security), classical computationally secure symmetric-key cryptographic schemes (requires a pre-installed key on both sides and can be used only as scheme for increase in key size but not as key distribution scheme), quantum key distribution (provides information-theoretic security; it can also be used as a scheme for increase in key length), Trusted Couriers Key Distribution (it has a high price and is dependent on the human factor). The security has become a big concern in wired and wireless networks. The characteristics of networks pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and no repudiation. Cryptographic techniques are widely used for secure communications [6]. Cryptography is composed schematically by two systems: symmetric encryption and asymmetric encryption.

The cryptosystems of symmetric encryption use the same key for cipher and decipher messages. The key must be preserved secret by the parties of a communication. So in a network of n people wanting to communicate in a confidential way with a cryptosystems of symmetric encryption, it is necessary that the keys are distinct. Precisely, it is necessary to create and distribute $n(n-1)$ 2 keys which are distinct and secret. As we can remark, the cryptosystems of symmetric encryption suffers from the problem of creation and distribution the keys [10]. This problem is mainly solved by the installation of the cryptosystems of asymmetric encryption.

A cryptosystem of asymmetric encryption operates by handling two keys: secret and public. Each participant diffuses a public key with his name. If one wishes to communicate with a participant, it is necessary to recover his public key and cipher with it the message, and send the ciphered message to this participant which is the only person who knows the secret key which makes possible to decipher the received messages. The secret key is of course related to the public key, in practice by a mathematical relation. The power of the security of these cryptosystems is based on algorithmic complexity; it is difficult in practice to deduce the secret key from the public key in a reasonable delay. Nothing proves however that this security is not compromised in a near future because there is an accelerated evolution of the software and the specific hardware. So, many cryptographic schemes in use today would be broken with either unanticipated advances in hardware and algorithm or the advent of quantum computers. Another solution to the delicate problem of distribution of keys met in

cryptography consists at using the laws of the quantum physics[5]. It is precisely to place at the disposal of security of computing systems a Quantum Cryptography protocols in order to carry out a task of exchanged keys with a great security. Quantum Cryptography has been proven secure even against the most general attack allowed by the laws of physics and is a promising technology for adoption in realistic cryptographic applications. Quantum Cryptography allows two parties to expand on a secret key that they have previously shared. Various quantum cryptographic protocols have been proposed in order to achieve unconditional security. In this article, we give in details the descriptions of the famous Quantum Cryptography protocols: BB84, B92 and E91. Also, we provide a short presentation of some others recent protocols. The organization of the remainder of our paper is as follows [9]. We introduce the state-of-the-art of Quantum Cryptography. The description of the protocols BB84, B92, E91 and others protocols is given in section III. Finally, we conclude the paper in section IV.

Quantum mechanical effects can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable. But how can this be turned into a working Message Passing Quantum Cryptography protocol (MPQC)? A combination of quantum processing and well established classical procedures is needed. So, quantum mechanical effects can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable. But how can this be turned into a working cryptographic key distribution protocol? A combination of quantum processing and well established classical procedures is needed. Three distinct phases are needed: raw key exchange, key sifting and key distillation, with the option to discard the secret key at any of the stages if it is deemed that not enough security could be obtained from it. A clear description of these phases can be found on the swiss quantum website [SW10], and is illustrated in Figure 3, where the stages shown with double lines indicate classical authentication is needed.

Basis	**0**	**1**
+	↑	→
×	↗	↘

II. MPQC PROTOCOL

The MPQC protocol consists of sender (Alice) selecting a variable length random key maximum of up to 15 bit. Then sender (Alice) chooses the filter for each random bit. Thus we get qubits, which are sent to the receiver through a quantum channel. While the qubits are being received by the receiver (bob), he/she selects random filters as per the quantum technique. This filter selection is the key to our security of the key as the bits of the random number generated will only be retrieved from the qubits when the filters of the sender and the receiver match. If the filters are mismatched the bit from the qubit is not received, thus the key is not generated until the filters are shared during the communication, thus the key is not at all being transmitted in the public channel instead the filters are being transmitted. Thus, avoiding attacks like the man in the middle attack and the traffic analysis attack to an extent. Apart from these our algorithm uses a genetic algorithm to effectively generate and share the key among the sender and the receiver. The genetic algorithm makes sure that the key is secured.

Key Sifting

Alice and Bob decide (classically) between them which of the measurements will be used for the secret key. The decision making rules depend on which protocol is being used, and some measurements will be discarded e.g. if the settings used by Alice and Bob did not match.

Key Distillation

The need for further processing after the key sifting stage was determined by Bennett et al [CB92a] when reviewing experimental results (practical channels are lossy, and the protocol needs to be workable even in the presence of transmission errors) and in previous work [CB88] on how the use of an authenticated public channel could repair the information losses from an imperfect private channel. Thus **error correction** and **privacy amplification** are required, which are the first two steps in the key distillation phase of the classical post-processing of the remaining secret key bits. The third (and arguably most important!) final process is authentication, which counteracts man-in-the-middle attacks (MITM).

III. BACKGROUND OF WORK

Elboukhari, Quantum Key Distribution Protocols: A Survey Mohamed Elboukhari, Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. The security of most modern cryptographic systems

of key distribution mechanism is based on computational complexity and the extraordinary time needed to break the code. Quantum Key Distribution (QKD) or Quantum Cryptography is attracting much attention as a solution of the problem of key distribution; QKD offers unconditionally secure communication based on quantum mechanics. In this article we survey the most popular QKD protocols. Also, we give a short state of the art of Quantum Cryptography.

Ching-Nung Enhanced Quantum Key Distribution Protocols Using BB84 and B92 Four-state quantum key distribution (QKD) protocol BB84 [1] and two-state QKD protocol B92 [2] can let Alice and Bob share the secret key with idealized maximum efficiencies 50% and 25% over quantum channel, respectively. However, for these two polarization-based systems, the polarization states need to be maintained stable and against the noise of photon over a long distance optical fiber. Due to the alignment of polarization and the need of apparatus, the complexity of a four-state protocol is greater than that of two-state protocol. We herein use average number of polarization states in a QKD protocol as the complexity order. In this paper, we propose two enhanced QKD protocols. One is to enhance the idealized maximum efficiency to 28.6% with the average complexity order 2, and the other has the efficiency 42.9% and the average complexity order 2.86.

C. Kurtsiefera , Long Distance Free Space Quantum Cryptography Quantum cryptography bases the security of key exchange on the laws of quantum physics and will become the first application of quantum information methods. Here we present the design of novel hardware components which enabled the demonstration of secure key exchange over a 23.4 km free-space link.

Charles H, Experimental Quantum Cryptography We describe results from an apparatus and protocol designed to implement quantum key distribution by which two users who share no secret information initially exchange a random quantum transmission consisting of very faint ashes of polarized light by subsequent public discussion of the sent and received versions of this transmission estimate the extent of eavesdropping that might have taken place on it and if this estimate is small enough ,distill from the sent and received versions a smaller body of shared random information which is certifiably secret in the sense that any third party s expected information on it is an exponentially small fraction of one bit Because the system depends on the uncertainty principle of quantum physics instead of usual mathematical assumptions such as the difficulty of factoring it remains secure against an adversary with unlimited computing power.

IV. MPQC ALGORITHM

Algorithm: The IGA for Petri Keys

Step1: One node initiates a request for estimating of the network diameter, using MPQC to reach all the nodes in the network and estimate the network diameter as seen from its current position. At the end of this algorithm, every node has received an initial estimate N10. Each node can use 2Nl0 as its estimate, since that is the maximum number of hops between any two nodes the initial sender can communicate with.

Step2: Over time, other nodes perform step 1 and compute a new value Nli, using conventional random waits and perhaps a throttling mechanism to keep the average rate of requests as appropriate for the network.

Step3: Each node remembers the maximum network diameter it has seen, Nlmax = maxi Nli, and uses broadcast transmissions.

Step4: if desired, each new value could be compared with the remembered value only after multiplying the older value by an aging factor (Result Id) ←Max $_{id}$ (m). This makes older values decay over time and makes it more likely the network will converge on a value that is reasonable under current circumstances.

if Msg Type = New Member Selection then

if Check New Member Id(N)=Id then

//Dest Id←Get Dest Id (N1i)

Send Msg (Id, Dest Id)

Collect Msg (Id, Dest Id)

Collect Msg Info (Id, Dest Id)

End if

End if.

V. FEATURES OF MPQC

As reactive routing protocol, MPQC reacts relatively quickly to the topological changes in a network and updates only hosts that may be affected by the change. However, MPQC tends to cause heavy overhead due to the flood search triggered by link failures. As a result, MPQC does not perform well in heavy load.

Main advantages are:

1. Algorithm is nor computationally or memory complex,
2. Data transfer does not generate additional traffic,
3. Scalable, suitable for mobile networks, supports multicasting, tries to minimize the number of required broadcasts.

Table 1. Basic Scenario

Parameters	**Values**
Simulator	NS2 simulator
Protocols Studied	MPQC
The number of nodes	100 nodes
Simulation network Space	1500mx1500m
Node placement	Randomly deployment
MAC Protocol	IEEE 802.15.4

VI. RESULT ANALYSIS

The figures shown below are the results of evaluated measurements of the proposed scenarios. The results show the different characteristic measurements of different data byte variations of small, medium and large scale networks. The following figures show the evaluation results.

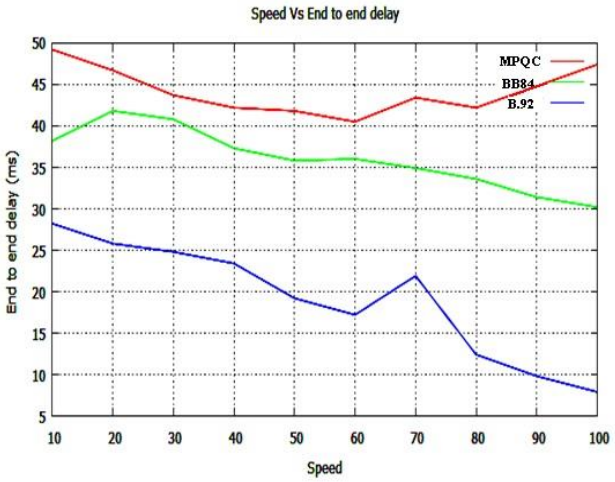

Fig.2 Speed Vs End to end delay

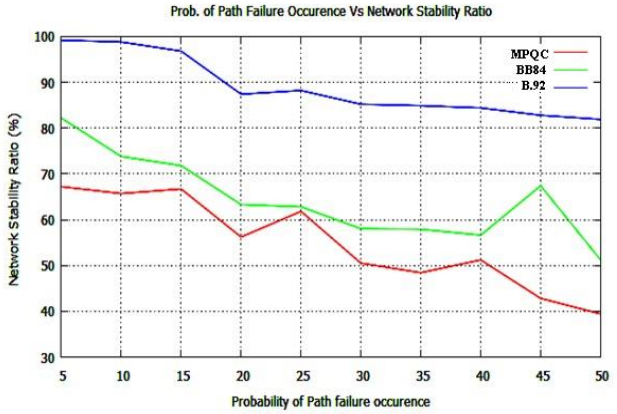

Fig.3 Probability of Path failure Occurrence Vs Network Stability Ratio

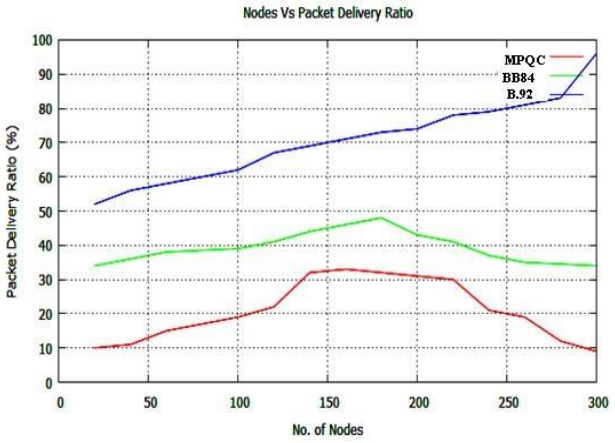

Fig.4 Throughput Vs Network lifetime

End-to-end delay indicates how long it took for a packet to travel from the Virtual server source to the application layer of the destination. It represents the average data delay an application or a user experiences when transmitting data. Above figure shows the result obtained for average of the network. The performance of this experiment shows the different result for different data size variation even though there is no change in the network. In throughput the data size increases the throughput of the network also increases very high. The shows delay decreases in the low data and for high data it increases the delay randomly.

VII. CONCLUSION

This paper describes how location information may be used to reduce the routing overhead in wireless networks. We present two location-aided routing (MPQC) protocols. These protocols limit the search for a route to the so-called request zone, determined based on the expected location of the destination node at the time of route discovery. These performance metrics are used to know how the characteristics of MPQC differs in different parameters change scenarios. This proposal gives very high throughput and small delay in quality of service in MPQC. In future, more proposal and many metrics will be explored for providing scalable in wireless networks.

REFERENCES

[1] C.H. Bennet and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Proceedings of IEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp.175-179, Dec. 1984.

[2] C.H. Bennet, "Quantum cryptography using any two non-orthogonal states", Physical Review Letters, Vol. 68, pp.3121-3124, May 1992.

[3] C.H. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of cryptology, Vol. 5, pp. 3-28, 1992.

[4] J.G. Rarity, P.M. Gorman and P.R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography", Electronic Letters, Vol. 37, No. 8, pp. 512-514, April 2001.

[5] P.D. Townsend, "Secure key distribution system based on quantum cryptography", Electronic Letters, Vol. 30, No. 10, pp. 809-811, May 1994.

[6] P.D. Townsend, J.G. Rarity and P R Tapster, 'Single photon interference in a 10km long optical fibre interferometer',Electronics Letters 29, 1993, 634-5; ibid. 'Enhanced single photon fringe visibility in a 10km long prototype quantum cryptography channel', Electronics Letters 29, 1993, 1291-3.
[7] Muller A., Breguet J. and Gisin N., 'Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km, Europhys. Lett. 23, 383-388, (1993).
[8] G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, 'Fast and User-friendly Quantum Key Distribution', J. Of Mod. Optics 47 (2/3), 517-531 (2000).
[9] C H Bennett et al, 'Experimental Quantum Cryptography', J. Cryptology 5 (1992) 3-28 .
[10] Bennett C.H., Brassard G. and Robert J-M, Privacy Amplification by Public Discussion, SIAM Journal on Computing,(1988) 17, pp210-229.

