TQDS: TIME STAMPED QUANTUM DIGITAL SIGNATURE TO DEFEND WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

T. Akila[1], P. Uma Maheswari[2], S.N.Sivanandam[3]

[1]Department of Computer Science and Engineering, Mahendra College of Engineering, Salem, India
[2]Department of Computer Science and Engineering, INFO Institute of Engineering, Coimbatore, India
[3]Eminent Professor, Karpagam College of Engineering & Technology, Coimbatore, India

Abstract

Wireless Sensor Network has a lot of problems related to routing. In routing protocol, wormhole attacker can make interference on the routing process by establishing short circuiting the normal flow of routing packets. This attack makes severe threats to both routing protocol and security enhancement. Such attack may strictly damage the communication among the nodes. Our aspect is to provide the best solutions to secure transmission over the network by using quantum cryptosystem. In this proposed approach, we present a detecting mechanism called Time stamped Quantum Digital Signature (TQDS) along with quantum one-way function, which is unconditionally secure even against wormhole attacks. It is based on node authentication which is implemented by neighbor discovery process. TQDS is based on quantum mechanism for neighbor discovery process. The quantum technique for secure communication against wormhole attackers is carried out. Using TQDS, the sensor nodes can be authenticated with one another and these nodes are communicated through quantum channel.

Keywords: *wormhole attack, quantum cryptography, quantum digital signature, quantum one-way function, quantum channel.*

---***---

1. INTRODUCTION

As the prominent development of popularity and the ease of deployment due to their infrastructure less in nature, WSN is used for various applications such as military, industry, airlines system, government sector, health care system, disaster recovery, automated system, battlefields.

Wireless sensor network consists of collection of small sensor nodes with limited battery power, limited memory capacity, limited computational capability but which are deployed over the environment for sensing information, monitoring and understanding the physical phenomena. These nodes are communicated through wireless medium such as radio signals. Due to the enormous limitation and ease of deployment, WSN is more susceptible to the security for providing more reliable route for transmission between nodes. This leads to the cause of security threats, which can be characterized in many ways such as Sybil attack, sink attack, packet replaying attack, traffic altering etc., A wormhole attack is very powerful because it disturb the overall network routing process and defending against the attack has proven to be very difficult. The main goal of the attacker is trying to get the traffic flow on the network and make them to control over the route path in the transmission.

In this paper, I focus on how to detect and prevent wormhole attacks in the network. To immune from the wormhole attack, I propose the solution based on quantum digital signature with quantum mechanisms rather than mathematical based cryptosystem. And most of the authentication protocols are based on the computational complexity of resolving mathematical problems utilized in the cryptographic scheme which leads to some of the attacks of linear and differential attack, factorization attack, timing attack, exponential attack, power attack etc.

Due to the high computation power of technologies, cryptosystem based detection and prevention approaches are highly vulnerable to the attacker. So, I propose the new way of solution which is entirely based on quantum particles used for node authentication in which TQDS verify that each node in the network is a legitimate node. Here, the entire node in the networks is communicated through quantum channel instead of classical channel. A quantum channel can forward the data in terms of photon using principles of photon polarization.

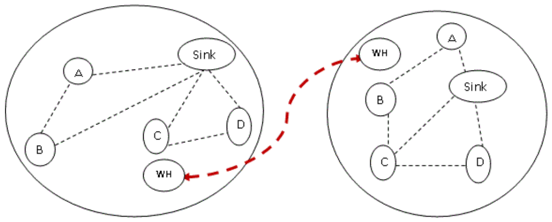
2. WORMHOLE ATTACK

One of the most significant attacks in the network is wormhole attack which affects the routing protocols and connectivity based localization algorithms.

A wormhole is similar to a tunnel or path or link in a network with two ends in which one end belongs to one network and the other end in different network. A wormhole is a path between malicious nodes which forward message faster than normal data flow in the network.

For launching a wormhole attack, a malicious node tries to tunneling links between two distant malicious nodes in the wireless network using low-latency communication link called wormhole tunnel.

If the wormhole link is tunneled successfully, then the malicious node can overhear the packets on one end of the network and forwards the received packets to the other end through the wormhole tunnel with low latency and minimum hop to reach the other end than the default link in the network. Wormhole attack may result in a distraction of network routing process which makes the serious threads in the networks.



Network N 1 Network N 2

Fig -1: Describe about the wormhole attack.

Let us consider that network N1 and N2 are not neighbors. In the above diagram, circle denotes the quantum signal range communication. However node WH in N1 and node WH in N2 are the compromised nodes that are establish the wormhole link immediately and create the false shortest path between the compromised nodes. Whenever a transmission is going on between any nodes, compromised node will attract the data traffic in order to make the route path through that node. As soon as the packets are fascinated to the wormhole, compromised node can get the control over the packets which means they can do either forward them or drop them or make changes in the packet. The compromised node can do harm in overall routing protocol in the network and can initiate a wide variety of attacks against the data traffic flow such as replay attack, sink attack, selective forwarding, denial-of-service attack etc.

In wireless network, Wormholes are deployed in various forms such as wormhole using encapsulation, wormhole using out of band channel, wormhole with high power transmission, wormhole using a packet relay and wormhole using protocol deviation.

In this paper, we propose a novel detection techniques based on Time stamped Quantum Digital Signature against wormhole attack. The simulation results shows about the performance and throughput of the TQDS protocol.

Our contribution in this paper is organized as follows: Section 3 discusses about the related work, Section 4 describes about the importance of quantum cryptography. Section 5 explains proposed solution and Section 6 describe about simulation result; at last Section 7 concludes the research paper.

3. RELATED WORK

In year 2006, TrueLink developed by Jakob Eriksson, [1] is a wormhole detection technique that depends on time based mechanisms. TrueLink verifies whether there is a direct link for a node to its adjacent neighbor. Wormhole detection using TrueLink involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

In year 2008, Yurong Xu, Guanling Chen et al., [2] [3] proposed a distributed detection algorithm for wormhole attack is called Wormhole Geographic Distributed Detection (WGDD). WGDD algorithm detects the disorder of the networks due to the existence of a wormhole in the network. This algorithm has three main procedures: A) Probe Procedure is based on hop-coordinates technique to measure the hop distance from each node to some bootstrap node. After this, each node has the hop coordinate from its neighbors. B) Local Map Computation Procedure. By running Dijkstra's algorithm, each node finds the shortest path for each pair of nodes in the network. Hence, this procedure constructs a local map by MDS (Multidimensional Scaling). C) Detection Procedure, This algorithm compute the diameter of each local map after determining each neighbor node's location.

Finally, According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes.

In year 2011, Pallavi Sharma, Aditya Trivedi [4][7], have proposed An Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature. This paper has presents a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, it creates a secure path between sender and receiver with the help of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

In year 2012, Kuldeep Kaur [5] proposed Detection of Wormhole Attack in Wireless Sensor Networks based on Digital Signature. To detect wormhole, Node authentication is used with digital signature. Node Authentication process is included at each sensor node in the packet header which is forward from source to destination. So, this process can detect the malicious nodes which cause the wormhole attack. In this method, neither the hardware nor the clock synchronization is used for node authentication. At the destination end, recipient node is verified and if the digital signature gives the false information above the sender node which is forward to the sender using DATA_ACK.

In year 2013, Pravin Khandare , N P Kulkarni [6], proposed an algorithm which defends wormhole attack in WSN called public key encryption and 2Ack based approach. This approach provides security and finds misbehaving nodes in the network. Some assumptions are made that each node has a set of public key and private key. At the time of neighbor discovery process, every node shared his public key with another node. Data should be forwarded with constant bit rate. In this approach, each node sends a HELLO message to all the one hop neighbors in the networks. This broadcasted message contains source address and its own public key, which is broadcasted to all nodes. In response to this message, every authentic neighbor sent their own public key to ‘A’. Receiver public key of one hop neighbor sent in the encrypted message format. This message contains source ID, public key of ‘B’ encrypted with the public key of A and destination address.

When the node ‘A’ want to send data to ‘B’ then ‘A’ encrypt data with public key of ‘B’ and this data again encrypted with the private key of sender i.e. ‘A’. When receiver ‘B’ receives data from the sender ‘A’ then first ‘B’ decrypt data with public key of sender A and remaining data is decrypted with its own private key. In this way secure communication is done. For encryption and decryption is based on RSA technique. But RSA algorithm is more vulnerable to attacks such as factorization attack, revealed decryption exponent attack, timing attack etc.,

In year 2013, Himani Deswal, Rahul Kumar Yadav [7] has proposed Wormhole Detection Using Hidden Markov Model Approach. In this approach, node authentication is done by using cryptography based handshaking mechanism. To avoid fake reply from a node, only authenticated node will get the request and can reply properly. By using Hidden Markov Model, they performed the probabilistic analysis of throughput and response time between all pairs of neighbors in the network. Besides, they are effectively analyzed the tunnel attack using all pair neighbors communication. If there is any malicious node in the route path, then such node is blocked and new route is found safely. So no attacked node is the part of route path.

4. QUANTUM CRYPTOGRAPHY

Modern cryptosystem is more vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers [17]. For that reason, for past decade efforts have been made to establish new foundation for cryptography science in the computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics [10, 11, 15, 18]. Quantum cryptography is based on quantum mechanism rather than mathematics which are used to develop secret keys and messages in the form photon.

The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. The Heisenberg Uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system [13, 14, 15]. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first presented by Wootters and Zurek in 1982[16].

Digital signature, as an analogy to hand-written signature for authenticating the origin of a message and ensuring the message not being modified during transmission, is an essential cryptographic primitive. It has been being widely used in various fields, particularly in secure electronic commerce. As Rivest predicted, digital signature may become one of the most fundamental and useful inventions of modern cryptography [12]. However, all of the existing classical (digital) signature schemes whose security depends on the difficulty of solving some hard mathematical problems were threatened by last-increasing power of computers and innovative techniques such as quantum computation. For instance, once quantum computers would be successfully built, most of classical signature schemes would be cracked through Shor’s algorithm [13]. On the other hand, quantum physics has thrown light on the study of cryptography for obtaining unconditional security [14, 15, 16, 17, 18, 19]. Therefore, researchers turn to investigate quantum counterpart of classical signature with the hope that quantum signature

(QS) can provide unconditional security which ensures that the attacker (or the malicious receiver) cannot forge the signature, and, in the same time, the signatory cannot deny the signature even though unlimited computing resources are available.

QS is expected to sign both classical and quantum messages, and the form of each quantum message can be a known or an unknown quantum state. Since known quantum states can be characterized with classical information, the quantum messages being considered in this paper are in the form of unknown quantum states. Over the last decade, researchers have made some progress on QS. In 2001, Gottesman and Chuang proposed a QS scheme based on quantum one-way function, which is unconditionally secure even against quantum attacks [20].

5. PROPOSED SYSTEM

In this proposed paper, we compute a Quantum Digital Signature based on the values of location of the node. Based on quantum one-way function, we construct quantum public keys and private keys. Actually Sender generates both keys such as private key and public key in which private key kept secret and public key publically announces in the network. So the neighborhoods for the sender have received the public keys in the form of photons. They can measure their states after received, according to the value of the polarization of photons. Our algorithm provides higher security than the conventional digital signature schemes. Here, the keys and messages are send over the 'quantum channel '. It is a transmission medium through which the information is send in the form of photons and isolates the quantum state from intervention of the Eve droppers.

In this paper, I will explain above the solution for wormhole attack by using node authentication technique which is based on neighbor discovery process. One way to detect wormhole attack is node authentication techniques. Hence only authentic node can communicate with each other in the sensor network. Here neighbor discovery process is implemented in two phases such as signing phase and verification phase.

At the signing phase, Sender (A) forwards the message to all one hop neighbors in the networks. This broadcasted message comprise the information of A's signature, node-id and nonce (one time pad) value which is broadcasted in the form of photons to all neighborhood in the network. Every authentic neighbor sent their public key as response (ACK) of this message.

At verification phase, each neighbor decrypts its received message using sender's (A) public key and verify the location of the sender and its node-id with neighborhood table. If these two values are congruent, then receiver (B) accepts the message from A which means A is an authentic node in the network. Hence B forwards its public key as response (ACK) to the sender A and update its neighborhood table with new nonce value, otherwise B did not receive any consequential information that is whose communication is intercepted by the Eve droppers. As a result, interception itself turns the photons into different polarization which gives the incorrect information about the sender.

Here the location information gives the details above the radio propagation range. If the location information from A beyond the propagation range then sender A is not an authentic node even though it has correct node-id in the network and B send immediately NEGACK to the sender A. If the received ACK time by the sender is higher than the threshold, then it could assume that the receiver is a malicious node that is unauthorized node (wormhole) in the network.

Both sender and receiver must communicate with each other through quantum channel in which messages are forwarded in the form of photons. Hence confidentiality is achieved through the photon polarization because any interception of polarized photons makes changes in the polarization of photons. As a result, Eve cannot get the correct information. Hence the information is concealed with polarized photons. Thus prove the confidentiality.

This protocol gives more secure communication by using no-cloning theorem in quantum mechanism, which says that no one can get a copy of the transmitted message without errors. Thus, avoiding attacks like man in the middle attack and replay attack and the traffic analysis attack.

Quantum cryptography is based on quantum mechanism rather than mathematics which are used to develop secret keys and messages in the form of qubits which turn into photons. The messages are transformed into qubits by using the below table.

Table -1: Relationship between binary bits and its qubits

Basis	0	1
+	↑	→
×	↗	↘

5.1 Public Key Generation

1. Sender randomly choose a nonce (one-time pad random number) $x_{i,j}$ Є{0,1}.
2. Compute |yi,j >= |f($x_{i,j}$)> for i,j Є {0,1}. Here f: |x> → |f(x)> is a class of quantum one way function.
3. Sender generates the key pairs of {$x_{i,j}$ | $y_{i,j}$}. Here {|$x_{i,j}$>} is the private key [KR_A]which is kept secret and {|yi,j >} is the public key [KU_A] which is publicly announce in the network.

5.2 Signing Phase

1. The sender (A) generates a random number r which is less than 160 bit prime factor of 1024.
2. Sender (A) randomly choose a nonce (one-time pad random number) R_A.
3. Localization system gives the location information (L_i).
4. Sender includes its node-id [P_i] for its signing process.
5. Sender calculates its signature S_A using hash function

$$S_{A} = h(L \mid y^{r} \bmod p)$$

6. Now, Sender has the Message (M) of [$S_A \| R_A \| P_i$] which is encrypted with its private key.

$$M = E_{KRA}[S_A \| R_{A\,(nonce)} \| P_i]$$

After generated this message, Qubit generation algorithm takes this message as input and produce the qubits in the form of photon. Such qubits are forward to all the one hop neighbours in the network.

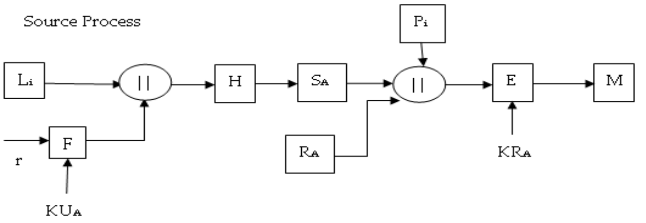


Fig -2: Illustration of sender process

5.3 Wormhole Verification Phase

In this procedure, each link has to verify that, there is wormhole between the sender and its neighbour nodes. Actually, the verification process is done by neighbours. At the receiving end, receiver (B) performs the following steps which is used to verify the location of the sender and its port-id . If the verification is successful, receiver sends ACK with its public key [KU_B] to the sender.

1. Receiver (B) receives the message in the form of photons. By applying Qubit generation algorithm, B received the encrypted information which is further decrypted by using sender's public key.

$$M = D_{KUA}[S_A \| R_{A\,(nonce)} \| P_i]$$

2. Now, B received the information about its sender such as $S_{A\,,}$ $R_{A\,(nonce)}$, P_i.
3. By applying hash function on $S_{A,}$ B receives the location information (Li) of A.
4. As long as B receives Li and Pi, These values are compared with the neighbourhood table. If two values are congruent, then B accepts the message which means transmission is more secure and has not been intercepted. So, B forwards its public key [KU_B] to the sender A. Otherwise B reject the message.

B → A: Send [KU_B] with ACK.

After the verification process, B updates its neighbourhood table with new nonce value. Here new nonce gives the present time of the message whereas old nonce gives the past time of the message which means past time of communication between the senders.

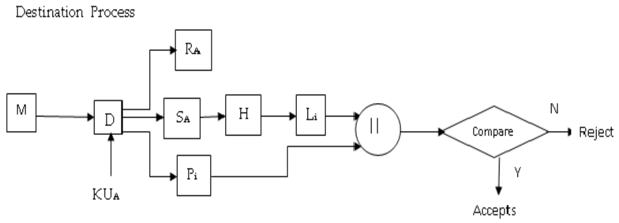


Fig -3: Illustration of destination process

5.4 Qubit Generation Algorithm

This procedure receives the message (M) as input and it is converted into sequence of binary bits. By using polarization filter, sender can generate the sequence of qubits which in turn to photons. Now sender sends photons over a quantum channel to receiver. Now receiver measures the incoming qubits after received, according to the values of the above table. As a result receiver gets the perfectly correlated result otherwise they get uncorrelated results.

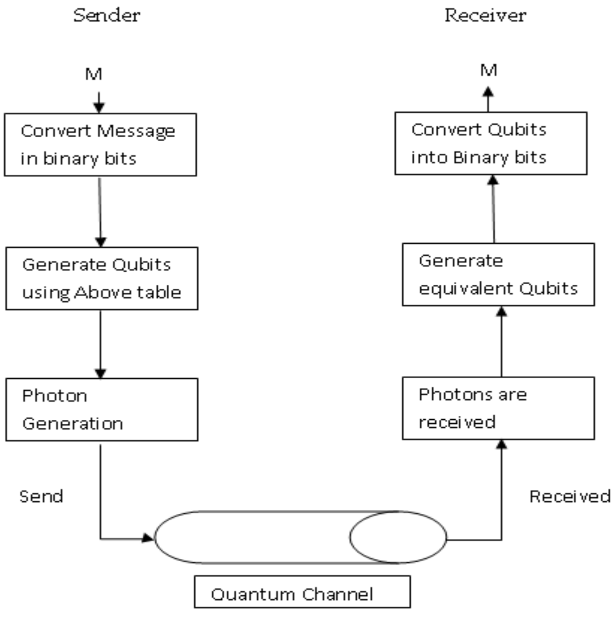

Sender
Receiver
M
M
Convert Message in binary bits
Convert Qubits into Binary bits
Generate Qubits using Above table
Generate equivalent Qubits
Photon Generation
Photons are received
Send
Received
Quantum Channel

Fig -4: Qubit Generation Process

6. SIMULATION

The proposed TQDS protocol is simulated in NS2 with the following scenario.

Table -2: Network Deployment

Parameters	Values
Simulator	NS2 simulator
Protocols Studied	TQDS
The number of nodes	100 nodes
Simulation network Space	1500mx1500m
Node placement	Randomly deployment
Routing Protocol	AODV

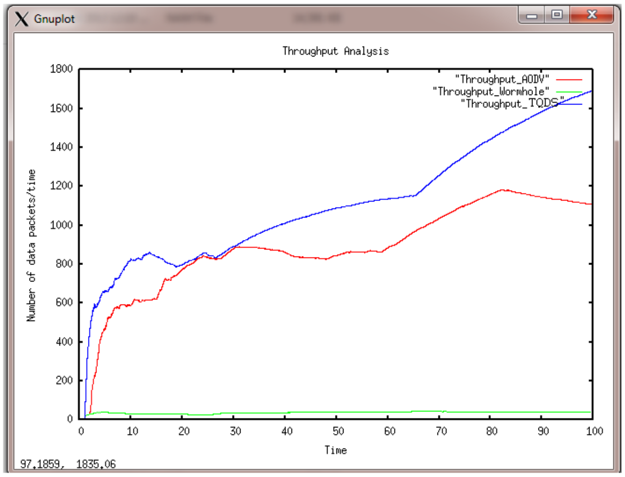


Fig -5: Network Throughput

Here, the figure is showing the comparison graph to represent the number of data packets transmitted over the network in existing AODV protocol with wormhole in the network and proposed TQDS protocol. Here x-axis represents the simulation time and the y-axis is the number of data packets transmitted over the network. Hence, the result shows that our work has higher throughput than the existing protocol.

7. CONCLUSIONS

The most noteworthy attack in the network layer is the wormhole attack which disrupts the routing information and connectivity based protocols in the network layer. In this paper, we propose a solution to detect and prevent the wormhole attack using time stamped quantum digital signature in wireless sensor networks. In order to authenticate neighborhood, this protocol uses the quantum digital signature using nonce (one time pad) and location information of the nodes. This protocol gives higher security than the conventional schemes by using quantum mechanisms. This protocol will progress the network throughput and it gives the more secure, efficient and reliable transmission over the wireless sensor network. In future, more proposal and many metrics will be explored for providing scalable in wireless networks.

REFERENCES

[1] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks”: Proceedings of the 2006 14th IEEE International Conference on Network Protocols, 2006 IEEE 1-4244-0594-7, pp. 75-84.

[2] Y. Xu, G. Chen, J. Ford and F. Makedon, “Detecting Wormhole Attacks in Wireless Sensor Networks” Critical Infrastructure Protection, IFIP International Federation for Information Processing Volume 253, 2008, pp 267-279.

[3] Y. Xu, J. Ford and F. Makedon, “A variation on hop counting for geographic routing”, Proceedings of the Third IEEE Workshop on Embedded Networked Sensors, 2006.

[4] Pallavi Sharma, Prof. Aditya Trivedi,“An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, 978-1-61284-486-2, 2011 IEEE.

[5] Kuldeep Kaur, Vinod Kumar & Upinderpal Singh, “Detection of Wormhole Attack in Wireless Sensor Networks”, IRNet Transactions on Computer Science and Engineering, ISSN: 2279-0470 Volume 1. Issue 1, 2012 PP 21 – 24.

[6] Pravin Khandare, Prof. N. P. Kulkarni, “Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack”, International Journal of Computer Trends and Technology- volume4Issue3- 2013.

[7] H Deswal1, Rahul Kumar, Yadav, “Wormhole Detection Using Hidden Markov Model Approach”, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X IJCSMC, Vol. 2, Issue. 6, (June 2013), pp. 69 – 77.

[8] Majid Meghdadi, Suat Ozdemir1 and Inan Güler2, “A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks “, IETE TECHNICAL REVIEW, VOL 28 ISSUE 2, MAR-APR 2011.

[9] Dhara Buch and Devesh Jinwala, “Prevention Of Wormhole Attack In Wireless Sensor Network” , International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[10] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, A. Tapp, “Authentication of quantum messages”, in Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science, 2002, pp. 449–458.

[11] G. H. Zeng, M. Lee, Y. Guo, G. Q. “He, Continuous variable quantum signature algorithm”, International Journal of Quantum Information 5, (2007) 553–573.

[12] R. Rivest, Cryptography, Vol. 1, Elsevier, 1990, Ch. 13, pp. 715–755, handbook of Theoretical Computer Science.

[13] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, 1994, pp. 124–134.

[14] C. H. Bennett, G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984, pp. 175–179.

[15] A. K. Ekert, "Quantum cryptography based on bell's theorem", Physical Review Letters 67 (1991) 661–663.

[16] G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!", Sigact News 20 (1989) 78–82.

[17] H.-K. Lo, H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances", Science 283 (1999) 2050–2057.

[18] C. H. Bennett, D. P. Divincenzo, "Quantum information and computation", Nature 404 (2000) 247–255.

[19] D. Mayers, "Unconditional security in quantum cryptography", Journal of the ACM 48 (2001) 351–406.

[20] D. Gottesman, I. L. Chuang, "Quantum digital signatures", arXiv:quant-ph/0105032 (2001).