Quantum Communication in Distributed Wireless Sensor Networks

Jung-Shian Li
Institute of Computer and Communication Engineering
National Cheng Kung University
Tainan, Taiwan, R.O.C.
E-mail: jsli@mail.ncku.edu.tw

Ching-Fang Yang
Institute of Computer and Communication Engineering
National Cheng Kung University
Tainan, Taiwan, R.O.C.
E-mail: q3895126@mail.ncku.edu.tw

***Abstract*—In the wireless sensor networks (WSNs), sensor nodes may be deployed in the hostile areas. The eavesdropper can intercept the messages in the public channel and the communication between the nodes is easily monitored. Furthermore, any malicious intermediate node can act as a legal receiver to alter the passing messages. Hence, message protection and sensor node identification become important issues in WSN. In this paper, we propose a novel scheme providing unconditional secure communication based on the quantum characteristics, including no-cloning and teleportation. We present a random EPR-pair allocation scheme that is designed to overcome the vulnerability caused by possible compromised nodes. EPR pairs are pre-assigned to sensor nodes randomly and the entangled qubits are used by the nodes with the quantum teleportation scheme to form a secure link. We also show a scheme on how to resist the man-in-the-middle attack. In the framework, the qubits are allocated to each node before deployment and the adversary is unable to create the duplicated nodes. Even if the malicious nodes are added to the network to falsify the messages transmitting in the public channel, the legal nodes can easily detect the fake nodes that have no entangled qubits and verify the counterfeit messages. In addition, we prove that one node sharing EPR pairs with a certain amount of neighbor nodes can teleport information to any node in the sensor network if there are sufficient EPR pairs in the qubits pool. The proposal shows that the distributed quantum wireless sensor network gains better security than classical wireless sensor network and centralized quantum wireless network.**

Keywords: no-cloning, teleportation, EPR pair allocation;

I. INTRODUCTION

Wireless sensor networks (WSNs) are made up of sensor nodes with wireless communication capabilities. Those devices have the ability to collect, process, and store information as well as communicate with others. Since sensor nodes are often deployed in the malicious environment, the security demand is considered more and more important for WSNs. Attacks like modifying critical information by capturing sensor nodes or assuming the identity of the other node are damaging and should be avoided. Assigning keys to sensor nodes has been regarded as the fundamental and critical issue in the secure WSNs. Many researches about key management in WSNs have been proposed [1].

It is well known that quantum cryptography offers improved security for communication over classical cryptography. We adopt the quantum characteristics in the wireless sensor network to enhance the security. Like the pre-shared key distribution, the proposal allocates Einstein-Podolsky-Rosen (EPR) pairs to each sensor node and the sensor node can transmit quantum information to another sensor node by quantum teleportation. With the quantum characteristics, the information transmitted between nodes is not eavesdropped easily. Since the qubits stored in the sensor node can not be duplicated and can be used only once, the risk of information leakage is decreased even if the node is compromised.

In the quantum system, quantum key distribution (QKD) [2-3] can allocate secure keys due to the quantum nature, such as the uncertainty principle and the no-cloning property. QKD can be used with a symmetric encryption protocol to establish a secure communication and the faraway legitimate parties are able to transmit encrypted binary strings. However, QKD is not suitable for long distance and wireless transmission; the transmitted information would loss its correctness with the increasing transmission distance in the quantum channel. Thus, we adopt quantum teleportation to transmit data over the wireless sensor network with the pre-deployed EPR pairs.

In the quantum wireless network, Cheng et al. [4] introduced the quantum routing mechanism by using quantum teleportation and quantum circuits, Nguyen et al. [5] discussed how to integrate quantum cryptography into 802.11i security mechanisms and Lin et al. [6] proposed a scheme to prevent channel attacks and detect malicious nodes by pre-sharing a quantum table between the sender and the receiver in the beginning. Huang et al. [7] presented a framework that combines the QKD and the wireless security standard. The above proposals open the doors to advances in quantum wireless network. However, these studies do not apply a scheme for distributed quantum wireless network. In [4], the quantum wireless network is controlled by the trust central servers that are responsible for generating and allocating EPR pairs as well as maintaining the location information of each mobile device, and thus the communication between mobile hosts depends on the manager hosts. The framework is like the mobile IP scheme and the servers become the attack target. The security of the system will be broken if some server is compromised. The scheme proposed in [6] needs to share tables in advance to authenticate the sender and the receiver and is not suitable in the distributed sensor network.

978-1-4244-5113-5/09/$25.00 2009 IEEE

These studies inspire us to design a framework of quantum wireless sensor network with more robust security than traditional wireless sensor network by quantum teleportation. With advanced quantum sensors [8], this paper proposes an effect EPR pair management scheme in a distributed quantum wireless sensor network without the coordination of any central servers. The EPR pairs are allocated to each sensor node before the nodes are randomly deployed to the wireless network. In such a distributed framework, no central manager and global information are needed and each sensor node communicates with others by quantum teleportation. We also propose an effective scheme to resist the man-in-the-middle attack in the quantum wireless sensor network. The scheme is used to identify the communication pairs and verify the validity of the transmission message.

II. BACKGROUND

A quantum bit (qubit) is a unit of quantum information associated with a two-dimension Hilbert space. The qubit owns state $\alpha|0\rangle + \beta|1\rangle$ that combines the orthonormal bases $\{|0\rangle, |1\rangle\}$, i.e. quantum superposition, where α and β are complex numbers satisfying $\alpha^2 + \beta^2 = 1$. The power of quantum computation is based on superposition of quantum states. Every state in a superposition would be transformed simultaneously, a phenomenon called quantum parallelism. The evolution of a closed quantum system is characterized by a unitary operator U. If the quantum state at the time t_1 is $|\varphi\rangle$, then the quantum state at the time t_2 is $|\varphi'\rangle$ representing by $|\varphi'\rangle = U|\varphi\rangle$. For example, applying the Hadamard operator, $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, on the standard basis $\{|0\rangle, |1\rangle\}$ gets $H|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Any quantum operation acting on a single qubit can be described by a 2×2 unitary matrix. The Pauli matrices, such as $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ are the usual quantum operations in quantum computation. CNOT quantum gate is also a very useful operation that flips the target qubit if the control qubit is $|1\rangle$, otherwise the original state of target qubit are kept. Quantum measurement is an important process in quantum theory. After the measurement of a single qubit coming with state $\alpha|0\rangle + \beta|1\rangle$, the probability of measuring out the results 0 and 1 will be $|\alpha|^2$ and $|\beta|^2$ respectively. Quantum entanglement plays a critical role in quantum teleportation, quantum cryptography and quantum superdense coding. The EPR-Bell states are usually used as a source of quantum entanglement and these states are as following: $|\phi^+\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$, $|\phi^-\rangle = \frac{(|00\rangle - |11\rangle)}{\sqrt{2}}$, $|\psi^+\rangle = \frac{(|01\rangle + |10\rangle)}{\sqrt{2}}$, $|\psi^-\rangle = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}}$. After measuring the first qubit of a Bell state, e.g. $|\phi^+\rangle$, in the standard basis, the probability of measuring the result 0 for the first qubit will be 1/2 and the post-measurement state becomes $|00\rangle$. On the other hand, the measurement of the first qubit results in 1 with the probability 1/2 and the post-measurement state change into $|11\rangle$.

A. Quantum Teleportation

The most remarkable usage of quantum entanglement is quantum teleportation. In 1993, Bennett et al. [9] first propose a quantum method of teleportation. The protocol implements disembodied transport of the state of a system to a remote system. An unknown quantum state of one qubit can be transferred securely with the aid of EPR pairs from the sender to the receiver by performing local operation and classical transmission. Quantum teleportation has many applications, such as transmission of quantum states in noisy environments and sharing states in distributed quantum networks. As shown in (1), a quantum state $|\phi_0\rangle$ is initially prepared by the tensor product of three separate states that are kept by the sender and the receiver respectively. Then a Hadamard gate is applied to the second qubit and gets the quantum state $|\phi_1\rangle$. Next, the Controlled-Not gate is applied from the second to the third qubit as (3) presents. Again, the Controlled-Not gate is applied from the first to the second qubit, which transforms $|\phi_2\rangle$ into $|\phi_3\rangle$. Afterward the Hadamard gate is used to act on the first qubit and produces state $|\phi_4\rangle$. The expression of state $|\phi_4\rangle$ makes it easy to judge the possible outcomes of measuring the first two qubits. The state of the third qubit transforms into one of the four states, $\alpha|0\rangle + \beta|1\rangle$, $\alpha|1\rangle + \beta|0\rangle$, $\alpha|0\rangle - \beta|1\rangle$ and $\alpha|1\rangle - \beta|0\rangle$ that are respectively corresponding to the measurements of the first two qubits, namely $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Thus, the receiver can change the state of the third qubit to $|\phi\rangle$ by applying the appropriate operations, such as X, Z, Y operators, according to the measurements of the first two qubits received from the sender. Finally, the quantum state $|\phi\rangle$ is teleported from the sender to the receiver.

$$\begin{aligned} |\phi_0\rangle &= |\phi\rangle \otimes |0\rangle \otimes |0\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \\ &= \alpha|000\rangle + \beta|100\rangle \end{aligned} \tag{1}$$

$$\begin{aligned} |\phi_1\rangle &= \alpha|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \beta|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{\alpha}{\sqrt{2}}(|000\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |110\rangle) \end{aligned} \tag{2}$$

$$
\begin{aligned}
|\phi_2\rangle &= \frac{\alpha}{\sqrt{2}}(|0\rangle \otimes CNOT(|00\rangle) + |0\rangle \otimes CNOT(|10\rangle)) \\
&+ \frac{\beta}{\sqrt{2}}(|1\rangle \otimes CNOT(|00\rangle) + |1\rangle \otimes CNOT(|10\rangle)) \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle)
\end{aligned} \tag{3}
$$

$$
\begin{aligned}
|\phi_3\rangle &= \frac{\alpha}{\sqrt{2}}(CNOT(|00\rangle) \otimes |0\rangle + CNOT(|01\rangle) \otimes |1\rangle) \\
&+ \frac{\beta}{\sqrt{2}}(CNOT(|10\rangle) \otimes |0\rangle + CNOT(|11\rangle) \otimes |1\rangle) \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle)
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
|\phi_4\rangle &= \frac{\alpha}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) \\
&+ \frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) \\
&= \frac{1}{2}|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) \\
&+ \frac{1}{2}|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)
\end{aligned} \tag{5}
$$

B. Entanglement Swapping

One of the useful properties of the entanglement is the entanglement swapping that one particle of an entangled pair becomes entangled with one particle of another entangled pair, even though the two never interact initially. For example, let the entangled state of qubits, *a* and *b*, be $|\phi^+\rangle_{ab} = \frac{(|00\rangle_{ab} + |11\rangle_{ab})}{\sqrt{2}}$ as well as another entangled qubits, *c* and *d*, be $|\phi^+\rangle_{cd} = \frac{(|00\rangle_{cd} + |11\rangle_{cd})}{\sqrt{2}}$. The two qubits *b* and *d* are projected into one of the four Bell states, $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$, after measuring qubits *a* and *c*.

$$
\begin{aligned}
|\phi^+\rangle_{ab} \otimes |\phi^+\rangle_{cd} &= \frac{1}{2}(|00\rangle_{ab} + |11\rangle_{ab}) \otimes (|00\rangle_{cd} + |11\rangle_{cd}) \\
&= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{abcd} \\
&= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{acbd} \\
&= \frac{1}{2}(|\phi^+\phi^+\rangle + |\phi^-\phi^-\rangle + |\psi^+\psi^+\rangle + |\psi^-\psi^-\rangle)_{acbd}
\end{aligned} \tag{6}
$$

The four possible measured states are $|\phi^+\rangle_{ac}|\phi^+\rangle_{bd}$, $|\phi^-\rangle_{ac}|\phi^-\rangle_{bd}$, $|\psi^+\rangle_{ac}|\psi^+\rangle_{bd}$ and $|\psi^-\rangle_{ac}|\psi^-\rangle_{bd}$ that each occurs with equal probability 1/4. From two entangled pairs, *ab* and *cd*, a joint measurement of *a* and *c* in the Bell basis projects pair *bd* in an entangled state even though *b* and *d* might be far apart. Entanglement swapping discussed in [10] has been widely applied to quantum communication.

node ID	tag	qubit ID
	⋮	⋮
	tag	qubit ID
⋮	⋮	⋮
node ID	tag	qubit ID
	⋮	⋮
	tag	qubit ID

Figure 1. The ID list in the sensor node.

III. THE QUANTUM ENCRYPTION IN SENSOR NETWORK

In the section, we propose the protocol based on quantum properties to enhance the robustness of the security in the sensor network. The basic schemes include EPR-pair allocation and quantum relay path establishment. In the quantum EPR-pair allocation, EPR pairs are allotted to different sensor nodes randomly. The quantum relay path establishment aims to find the optimal path with the minimum number of EPR pairs in series. The pre-allocated EPR pairs are also used to resist the man-in-the-middle attack with the hash function in the sensor network.

A. Quantum EPR-pair Distribution

The quantum EPR-pair distribution consists of three phases, namely EPR-pair pre-allocation, entangled qubits discovery, and quantum relay path establishment. In the EPR-pairs pre-allocation phase, each node is assigned the unique identity in the network of size *n* and is matched up with *m* other randomly selected distinct nodes. The EPR pair is allotted to each pair of nodes. In the entangled qubit discovery phase, every node inquires its neighbors within the wireless communication range to seek for sharing EPR pairs. A secure link exists between two sensor nodes only if they share EPR pairs and thus the data can be delivered by quantum teleportation. The quantum relay path establishment phase builds EPR pairs between the two selected sensor nodes that do not share EPR pairs initially but are connected by two or more links at the end of the entangled qubits discovery phase.

We define the information carried in classical packets and the content stored in ID list in each sensor node. The ID list maintained in each node contains the other nodes' ID that share entangled qubits with itself and the entangled qubits' ID as shown in Fig. 1. The tag entry corresponding to each qubit ID is used to judge whether the qubit has been measured. If the qubit stored in the node is measured, the tag is marked as inactive; otherwise, the tag is shown as active. The classical packets are classified into request packet and response packet. The request packet contains the path_list that is used to record the passing nodes' ID, the dest_node_ID that is used to record the destination node's ID, and the next_node_ID that is used to record the next entangled node ID. The response packet contains the path_list that is duplicated from the request packet.

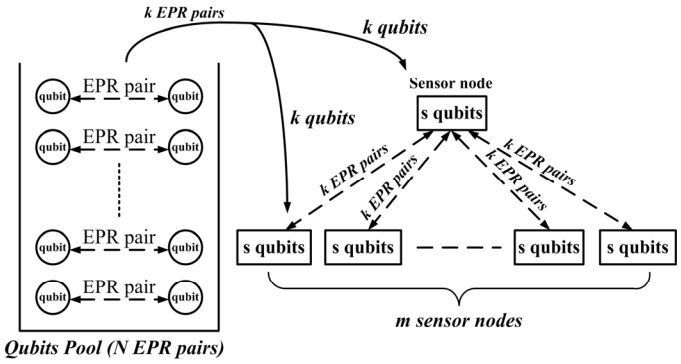

Figure 2. EPR pair allocation among sensor nodes.

The EPR pair pre-allocation phase ensures that any two nodes can communicate securely with a certain probability. Erdös and Rényi [11] showed the probability p of any two nodes being connected such that the entire network is connected with high probability. Therefore, the expected degree of a node is $(n\text{-}1)*p$ if the network with n nodes is connected. For clarity, we define some symbols as shown in Table 1. In the beginning, a total of N EPR pairs are generated and allotted to each node. Every EPR pair is separated to two entangled qubits that are put into two different nodes randomly. Each node is assigned s qubits composed of m groups of k qubits. The k qubits of each group in a node are entangled with other k qubits in another node. That is, a node shares EPR pairs with other m nodes as shown in Fig. 2 and the maximum supportable network size is $n=m/p+1$.

Lemma 1: It takes at least ($C_{n-2}^{n}*p*k$) EPR pairs to build a connected and secure network.

Proof: Since each node is matched up with m other randomly selected distinct nodes, we have $m = (n\text{-}1)*p$. There are N EPR pairs assigning to n nodes and each node can store s qubits that is equal to $k*m$. From the above relationships, it is obvious that $s = 2N/n = k*m$ and then we get $m = 2N/(n*k)$. The equation becomes $2N/(k*n) = (n\text{-}1)*p$ after replacing m with $2N/(n*k)$. It is straightforward to obtain $N= C_{n-2}^{n}*p*k$. If the system have at least ($C_{n-2}^{n}*p*k$) EPR pairs, one node can teleport information to any other node in the network. ■

Lemma 2: A node share EPR pairs with $N*n'/(k* C_{n-2}^{n})$ nodes that are within its wireless communication range.

Proof: The expected number of nodes that share EPR pairs with a certain node would be $d = n'*p$ where n' is the number of neighbor nodes. By the equation $(n\text{-}1)*p = m$, we replace p with $m/(n\text{-}1)$ and get $d = n'*m/(\text{n-}1)$. We know that $m = 2N/(n*k)$ in Lemma 1, so the average number of nodes sharing EPR pairs with a node is $d = n'/(n\text{-}1)*2N/(n*k) = N*n'/(k* C_{n-2}^{n})$. ■

The entangled qubits discovery phase means that every node discovers its neighbors in wireless communication range with which it shares EPR pairs during the quantum sensor network initialization. Each node broadcasts its ID list such that both two nodes can find out if they share EPR pairs. If the neighbors are the matched nodes, they reply to the broadcasting node. It is unnecessary for the entangled qubits discovery phase to guarantee sharing of EPR pairs for a sensor node with all nodes in the wireless sensor network, as long as multi-link paths of shared EPR pairs exist among neighbors they can be used to setup a quantum relay path as needed. Since the EPR pair is unique and un-cloning, one EPR pair is shared by only one pair of sensor nodes. If one node shares entangled qubits with the other node in its wireless transmission range, the node can communicate securely with the pairing node by quantum teleportation.

TABLE I. THE SYMBOLS FOR EPR-PAIR ALLOCATION.

d	The expected degree of a node
s	Number of qubits stored in the node
n	Network size
n'	The expected number of neighbor nodes of a given node
p	The probability that two nodes can set up a secure link
N	The number of EPR pairs
k	A constant that present the number of the qubits being teleported.
m	The number of nodes that share EPR pairs with the given node

The quantum relay path establishment phase aims to regenerate EPR pairs between two originally un-entangled nodes. Since the nodes are randomly distributed in the sensor network. The node could teleport messages to the entangled node if both nodes share EPR pairs. However, it is impossible for one device to share EPR pairs with all possible communication parties simultaneously. The basic idea is to use some sensor nodes as trusted intermediaries to establish EPR pairs between the end nodes. Quantum relay scheme applies the solution for two nodes without entangled qubits to share EPR pairs by performing quantum swapping hop by hop across the network. Each node finds the relay path by the following steps.

(S1) The source node checks its own ID list and finds out the mate node that has enough entangled qubits shared with it. The source node writes the entangled node's ID into the next_node_ID field of the request packet and broadcasts the request packet. If there are many nodes having sufficient entangled qubits appearing in the ID list, the source node broadcasts multiple request packets that carry different entangled node's ID. Also, the source node ID is added to the path_list carried in the request packet and marked.

(S2) Each intermediate node receives the request packet and checks if its ID is the same as the next_node_ID recorded in the request packet. If not, the node just adds its ID to the path_list and rebroadcasts the request packet. The node recognizes that it is the entangled node if its ID is the same as the next_node_ID. The entangled node chooses the request packet with minimum length of path_list if it receives multiple broadcasting request packets that contain the next_node_ID same as its ID. The entangled node also checks its own ID list and finds out the mate nodes, except those nodes whose ID is marked in the path_list, and the node regenerates request packets corresponding to different mate nodes and writes the

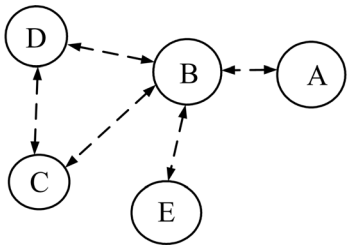

Figure 3. EPR pairs distribution topology.

mate nodes' ID into the next_node_ID field of the separated request packets. The entangled node copies the path_list in the receiving request packet to these new request packets, adds its ID to the path_list and marks, and then re-broadcasts these packets.

(S3) Finally, those request packets arrive at the destination node. The destination node checks these path_list recording in the request packets to count the number of the marked nodes' ID. The path_list that contains the least marked IDs means that there is least consumed EPR pairs in the routing path and the path_list will be chosen. If there are multiple path_list have the same number of marked nodes, the one having the shortest length, i.e. the minimum number of passing nodes, is chosen. The chosen path_list are put in the response packet that is sent back to the source node along the path according to the path_list.

(S4) The intermediate nodes receiving the response packet records the ID of the sending node. After the source node receives the response packet, the quantum relay path is built. The quantum swapping is performed by the nodes in the path to relay the EPR pairs. The intermediate nodes that join quantum swapping must mark the tags of the entangled qubits as inactive after these qubits are measured.

For example as shown in Fig. 3, the node A and node B share EPR pairs, node B share EPR pairs with node C, node D and node E separately; node D and node C also share EPR pairs. According to the above steps, node A finds the shortest path to node C through node B. Then, node A builds EPR pairs with the node C by quantum swapping. We denote the EPR pair shared by source node (node A) and the intermediate node, i.e. node B as $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_{B1}+|1\rangle_A|1\rangle_{B1})$. Similarly, the EPR pair shared by node B and destination node (node C) can be represented by $\frac{1}{\sqrt{2}}(|0\rangle_{B2}|0\rangle_C+|1\rangle_{B2}|1\rangle_C)$. The quantum swapping can be expressed as $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_{B1}+|1\rangle_A|1\rangle_{B1})\otimes\frac{1}{\sqrt{2}}(|0\rangle_{B2}|0\rangle_C+|1\rangle_{B2}|1\rangle_C)$. After applying the CNOT gate and the Hadamard gate, we obtain

$$\frac{1}{2\sqrt{2}}[|00\rangle_{B1B2}(|0\rangle_A|0\rangle_C+|1\rangle_A|1\rangle_C)+|01\rangle_{B1B2}(|0\rangle_A|1\rangle_C+|1\rangle_A|0\rangle_C)$$
$$+|10\rangle_{B1B2}(|0\rangle_A|0\rangle_C-|1\rangle_A|1\rangle_C)+|11\rangle_{B1B2}(|0\rangle_A|1\rangle_C-|1\rangle_A|0\rangle_C)]$$

Therefore, as long as the node B measures its own two qubits, it would set up four terms of entangled qubits between node A and node C. Depending on the measurement outcome in the intermediate node, the destination would have the information about the entangled qubits' state. So it can fix up the entangled qubits via either applying nothing, X gate, Z gate, or both X and Z gates, then the EPR pair between source and destination would be built.

B. Quantum Authentication

A large body of research exists on the problem of information privacy, aiming to prevent information leakage to eavesdroppers and protect the users' identities [12-13]. Such approaches typically rely on cryptographic primitives to create a secure architecture and prevent external eavesdroppers from gaining access to the information held by valid network users.

QKD requires a classical public channel with trusted integrity; otherwise an eavesdropper can easily set up a man-in-the-middle attack. In case that the eavesdropper can manipulate messages on the public channel, the imposter could sit between the sender and the receiver and impersonates each of them to the other. As a result, the imposter shares two independent keys with the two valid parties and gain full control of the following communication without being noticed.

The literature has showed that the quantum authentication/identification schemes are used to detect and identify the fake intermediaries. However, these schemes are based on the pre-shared information between any two valid parties or rely on the physical quantum channel. These hypotheses are infeasible in the wireless distributed framework.

We propose a scheme aiming to solve the threat caused by the fake nodes that will alter the public messages or spread meaningless information in the middle of transmitting path. We assume that each node in the quantum sensor network is assigned a one-way hash function H and both the sending node (node A) and the receiving node (node B) share l EPR pairs before their communication begins. Initially, node A randomly generates a l-bits string s and measures the qubits in a basis according to s. If $s_i = 0$, node A chooses the measuring basis R (the rectilinear basis); otherwise, it chooses the basis D (the diagonal basis). If the measuring result of i^{th} qubit is $|0\rangle$ or $|1\rangle$, node A will write down $a_i = 0$ or $a_i = 1$. Consequently, node A obtains the l-bits string a and calculates the hash value h = H(a). Furthermore, it transmits the string s and the hash value h to node B through wireless channel. After receiving the string s and the hash value h, node B measures its own qubits in a basis according to s. If $s_i = 0$, node B measures the i^{th} qubit with the basis R; otherwise, it uses the basis D. Consequently, node B gains the l-bits string b. Then, node B checks whether h = H(b) is true. If h = H(b), node B verifies the correctness of the l-bits message and the identity of the sender. The protocol enhances the security of the message against the attack from the adversary in the middle path.

IV. SECURITY ANALYSIS

A. Defenses against the Man-in-the-Middle Attacks

In the classical sensor network, an attacker is able to read, insert and modify messages between two parties without either

party knowing that the link between the two victims. For example, a malicious node can camouflage itself as other nodes by advertising sham identities to its neighbors, known as the Sybil attacker. The Sybil attacker can create fake nodes that will be selected by other nodes as part of their routing paths. In the quantum swapping process, the fake nodes may also transmit the bogus measurement results to the next nodes through classical public channel and finally lead the destination node to transfer to the wrong state. Then the source node and the destination node could not share correct entangled qubits in the end and the security built by the quantum teleportation will be broken. The fake nodes can also transmit wrong information to the legal node to consume the scarce qubits for authentication. The proposed quantum authentication is used to verify the identity of the valid node and the correctness of the transmitting messages with the aid of the pre-allocated one-one EPR pairs. In the case, a few numbers of qubits can be used for the initial verification and the remainder can be saved for the following quantum teleportation. Since the fake node has no entangled qubits shared with the valid node, the valid node can easily judge that the other side is invalid by quantum authentication scheme. After confirming the identification of the communication node, the identifier can perform quantum swapping process.

B. Resiliency against Node Capture

The quantum sensor nodes also suffer capturing risk in the hostile area. The compromised node will generate fake messages and send to the legal nodes. These fake messages may contain counterfeit information and cause the legitimate nodes into wrong behavior. The malicious nodes could also spread lot of useless message to consume the EPR pairs stored in the normal nodes for authentication and invalidate the nodes. The compromised nodes are unable to detect easily except they transmit abnormal information. Since one node only shares the EPR pairs with certain of sensor nodes, capture of any node does not allow the adversary to decrypt additional information in the network besides the ones that the compromised node is directly involved in, and the security of the entire sensor network can not be broken. Moreover, the malicious node could not teleport wrong information to the legal nodes after it utilizes all stored qubits.

V. DISCUSSION ON CENTRALIZED AND DISTRIBUTED QUANTUM WIRELESS NETWORKS

In [4], the category of quantum wireless network is like the mobile IP that is suitable for WAN. Both mobile nodes in the local area have to ask the central devices to implement quantum swapping if they need to communicate. The broker server must store large amount of qubits entangled with other qubits assigned to the mobile nodes moving in the local area. Moreover, the framework also needs a global position information keeper that is used to track the location of each mobile node. It is obviously that the central devices become the attack targets and the network bottlenecks. The distributed quantum sensor network is designed to improve the weaknesses occurring in the centralized architecture. The quantum sensor nodes teleport quantum information to the peers by using pre-allocated EPR pairs. The central control device allots the qubits to the sensor nodes in the beginning and does nothing after nodes deployment. In such a case, each node becomes the intermediate coordinator in charge to relay the information and the security of the entire network rises largely even if some nodes suffer from attacks. Furthermore, the EPR pairs stored in the nodes are unique since the no-cloning theorem, thus the adversary could not replicate nodes to cheat the legal nodes. Also, one node can easily verify the identity of other node by the quantum authentication scheme without the help of central device.

VI. CONCLUSION

We present the first study on the EPR pairs management scheme to provide unconditional security among sensor nodes in the quantum wireless sensor network. Our approach shows that the sensor nodes can teleport quantum information to any other nodes in the network. In the quantum relay path establishment process, we primarily consider the consumption of EPR pairs due to the scarce of entangled qubits. We illustrate the quantum authentication scheme against the man-in-the-middle attacks and the node can easily verify the legality of the other side to avoid the impostor. The framework also supplies a good resistance to the threat caused by duplicated nodes since the quantum no-cloning theorem.

REFERENCES

[1] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Elsevier J. Comput. commun., vol. 30, 2007, pp. 2314-2341.

[2] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. 9th ACM Conf. on Computer and communications security, 1984, pp. 175-179.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, 1991, pp. 661-663.

[4] S. T. Cheng, C. Y. Wang, M. H. Tao, "Quantum communication for wireless wide-area networks," IEEE J. Select. Areas Commun., vol. 23, 2005, pp. 1424-1432.

[5] T.M.T. Nguyen, M. A. Sfaxi, S. Ghernaouti-Helie, "Integration of Quantum Cryptography in 802.11 Networks," in Proc. 1st Int. conf. on Availability, Reliability and Security, 2006.

[6] T. S. Lin, S. Y. Kuo, "Quantum Wireless Secure Communication Protocol," in Proc. 41st IEEE Int. Carnahan Conf. on Security Technology, 2007, pp. 146-155.

[7] X. Huang and D. Sharma, "Quantum key distribution for Wi-Fi network security," in Proc. 4th IEEE Int. Conf. on Circuits and Systems forCommunications, 2008, pp. 85-89.

[8] http://www.darpa.mil/sto/space/qsp.html

[9] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels", Phys. Rev. Lett., vol. 70, 1993, pp 1895-1899.

[10] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, "Entanglement swapping of generalized cat states and secret sharing," Phys. Rev. A, vol. 65, 2002.

[11] J. Spencer, The Strange Logic of Random Graphs, Algorithms and Combinatorics, Springer-Verlag, Berlin, 2000.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks," in Proc. ACM conf. on Mobile Computing and Networking, Rome, 2001, pp. 189-199.

[13] S. Pai, S. Bermudez, S. B. Wicker, M. Meingast, T. Roosta, S. Sastry, and D. K. Mulligan, "Transactional confidentiality in sensor networks," IEEE Security Privacy, vol. 6, no. 4, 2008, pp. 28-35.