International Journal of Innovative Computing, Information and Control
Volume **11**, Number **6**, December **2015**

ICIC International ©2015 ISSN 1349-4198
pp. 2119–2133

WIRELESS SENSOR NETWORK BASED ON HIGH-DIMENSIONAL QUANTUM COMMUNICATION

Hui Li, Yuhan Zhao and Yingpei Sun

School of Electrical Engineering and Automation
Henan Polytechnic University
No. 2001, Shiji Road, Jiaozuo 454000, P. R. China
{ li20042007; zyhjames; xiaribingcheng329 }@163.com

Received April 2015; revised August 2015

Abstract. *Wireless sensor network (WSN) has poor security in data transmission. In order to solve this problem, a high-dimensional quantum WSN (QWSN) is designed. In the QWSN, the node is high-dimensional quantum sensor node. On account of d-dimensional Einstein-Podolsky-Rosen (EPR)-pairs, the protocols are designed. The protocols include high-dimensional quantum channel safety testing protocol (HQTP) and high-dimensional quantum entanglement swapping communication protocol (HQCP). The HQTP can detect the third-party eavesdropping and the interference of the surrounding environment. The HQCP is used to transmit the information directly. The analysis and simulation results show that the WSN based on high-dimensional quantum provides the better security, throughput and efficiency than conventional WSN.*

Keywords: Wireless sensor network, High-dimensional quantum, Quantum communication, Superdense coding, *d*-dimensional EPR-pairs

1. Introduction.

Wireless sensor network (WSN), is composed of a large number of micro sensor nodes with wireless communication capabilities [1]. The applications of WSN include healthcare, athletic training, workplace safety, consumer electronics, secure authentication, and safeguarding of uniformed personnel, so the WSN is in ubiquitous, and has broad application prospect and huge market potential [2]. WSN is usually used to monitor inaccessible and dangerous areas. Sensor nodes communication is also faced with security challenges [3]. Message protection and sensor node authentication become important issues in WSN. Quantum communication is built on the basis of quantum mechanics and provides unconditional secure communication based on the quantum characteristics [4], including the Heisenberg uncertainty principle and quantum no-cloning theorem.

Quantum communication has become a recent and future research area and hot spot. The quantum secure direct communication (QSDC) protocol was proposed by Long and Liu [5]. This scheme uses all Einstein-Podolsky-Rosen (EPR) pairs in distributing the key except those chosen for checking eavesdroppers. The scheme is secure, efficient, and has high capacity. In 2003, Deng et al. used the idea of block transfer, and proposed an operation-encoded two-step QSDC scheme [6]. Compared with the QSDC protocol based on hyperdense coding, this QSDC protocol has immunity to the Trojan horse attack strategies with the process for determining the number of the photons in each quantum signal as it is a one-way quantum communication protocol. Luo et al. proposed a quantum dialogue (QD) based on single photons which not only allows two communicants to exchange their secret messages simultaneously via a one-step quantum transmission but also can confirm the message integrity [7]. Li et al. proposed a protocol for direct quantum communication between two parties which is achieved by controlling the phase of the signal photon [8]. This protocol utilizes quantum superdense coding to achieve a high intrinsic efficiency and source capacity. A QSDC scheme is proposed based on multi-body entangled system by Li et al. [9]. Lu et al. presented a security proof of a single-photon four-state deterministic quantum key distribution protocol against general attacks in [10]. Shi et al. proposed two schemes for realizing QSDC by using a set of ordered two-photon three-dimensional hyperentangled states entangled in two degrees of freedom as quantum information channels [11]. Some specific attacks such as denial-of-service attack, intercept-measure-resend attack and invisible photon attack can be prevented in ideal quantum channel. In addition, the scheme is still secure in noise channel. The communication model based on high-dimensional quantum superdense coding aroused widespread concern [12], and four-dimensional two-particle superdense coding scheme was proposed by Zhou et al., in 2010. They extended quantum dense coding to the four-dimensional in the scheme, the sender by sending a particle to the recipient to achieve the goal of transmitting the 2 bits classical information, and improve the communication efficiency of channel. A protocol for quantum secure direct communication with quantum superdense coding is proposed [13]. It combines the ideas of block transmission, the ping-pong quantum secure direct communication protocol, and quantum superdense coding. It has the advantage of being secure and of high source capacity.

QSDC based on high-dimensional entanglement swapping can be used to design a high-dimensional quantum WSN. In the high-dimensional quantum WSN, we use superdense coding QSDC based on d-dimensional EPR state entanglement swapping in the high-dimensional quantum sensor nodes. High-dimensional QSDC is a new communication model combined with the classical channel and quantum channel. In the system, classical channel only transmits a small amount of information needed in quantum communication, such as the quantum state measurement information, and the real information is transmitted through the quantum channel. On account of d-dimensional Einstein-Podolsky-Rosen (EPR)-pairs, the protocols are designed which included HQTP and HQCP. Due to the quantum property and the superdense coding function of high-dimensional quantum systems, we show that it can significantly improve the security of the network and the efficiency of the information transmission.

The rest of this paper is organized as follows. In Section 2, we present a system structure of the high-dimensional QWSN. In Section 3, we propose a high-dimensional QSDC scheme to achieve the communication between nodes in the system. In Section 4, we analyze the performance, security, energy efficiency and reliability of the system. Finally, we offer some concluding remarks in Section 5.

2. **The System Structure of the High-Dimensional QWSN.**

In the paper, according to the traditional WSN [14], we propose a high-dimensional QWSN in Figure 1. It is composed of the high-dimensional quantum sensor nodes, Sink nodes and remote control nodes. The data is collected by high-dimensional quantum sensor nodes, and transmitted by Sink node, through the Internet to the remote control nodes. Sink node is the core of the network, and it connects the WSN with Internet and external network, and also releases the monitoring tasks that comes from remote control nodes and forwards the data to the external network.

The network system of high-dimensional QWSN has some characteristics, as can be discussed below:

1) Sensor nodes have been arranged in the corresponding positions according to the information we need;

2) The sensor nodes do not move themselves;

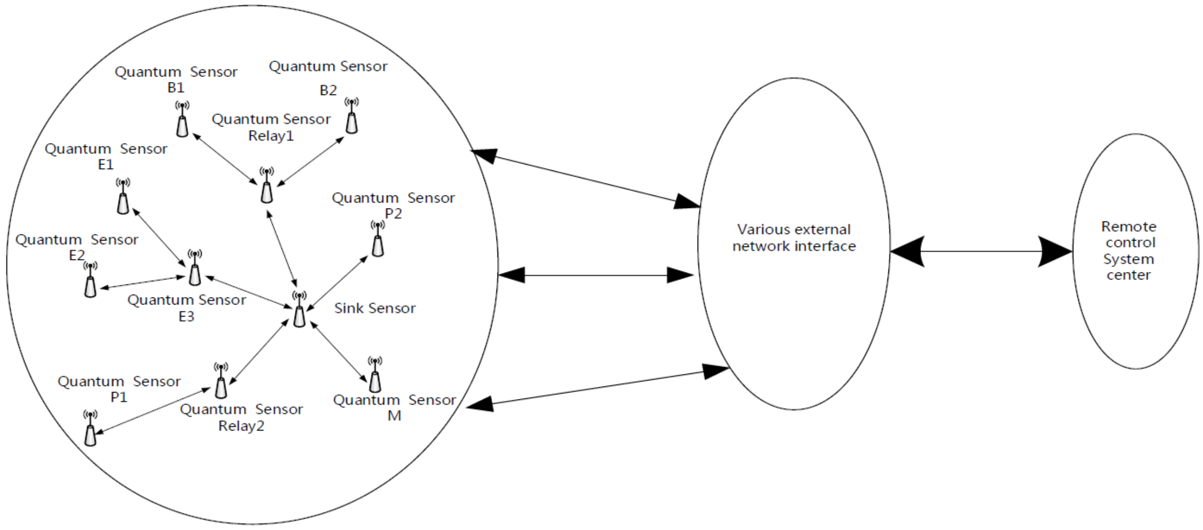

Figure 1. The network system of the high-dimensional QWSN

3) Sink node is located in the network system, and tries to keep the same distance to the other nodes sink;

4) Special devices, called relay nodes or relays can be added to the WSN to collect all the information from sensors and send it to the sink.

After allocating the relevant locations and parameters to the high-dimensional quantum sensor nodes, the entire network is in a dormant state. After receiving the instructions from the remote control center, Sink node sends a command packet to determine the first-level child nodes by way of broadcasting to its nearest nodes. The sensor nodes receiving the command packet from Sink node need to respond to the packet. If the Sink node receives multiple response packets with the same kind of data acquired by multiple nodes, it chooses the nearest node as its first-level child node. If the Sink node receives a packet of the response from the relay node, the relay node will be directly chosen as its first-level child node. Sink node records information of these child nodes, and notices the collection business type of these child nodes of the whole network as well as the trunk nodes through sending confirmation packages.

3. **Network Communication.** For convenience, we take a multihop tree topology diagram and the corresponding logic diagram as example, to describe the communication scheme and communication protocol within the network in detail. In Figure 2 and Figure 3, S is Sink node. The QM represents the high-dimensional quantum sensor node M. The QR1, QR2 are high-dimensional quantum relay nodes R1, R2 and QP1, QP2 on behalf of high-dimensional quantum sensor nodes P1, P2, QE1, QE2, QE3 on behalf of high-dimensional quantum EPR sensor nodes, QB1, QB2 on behalf of high-dimensional quantum sensor nodes B1, B2. Figure 3 is a logical topology diagram of Figure 2. As can be seen from Figure 3, the entire network topology is a multi-hop tree topology based on Sink node as the root node. Figure 3 shows the logic tree of Figure 2.

The advantage of the network topology is that the nodes in the network only need to know the information of their parent and child nodes, but not the whole network information from all nodes. In this way, it can save the storage space, and reduce the amount of information packets, so it can reduce energy consumption.

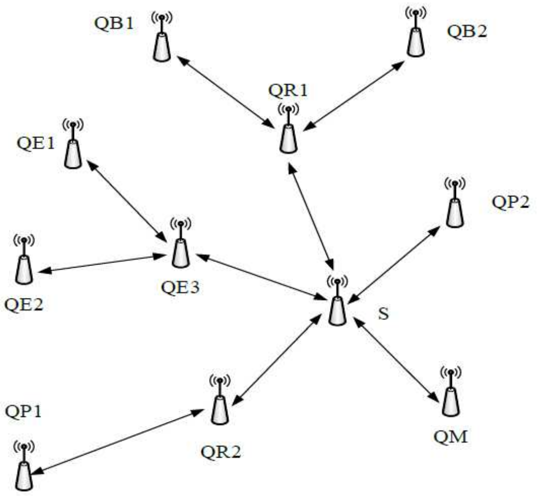

Figure 2. Multi-hop tree topology diagram

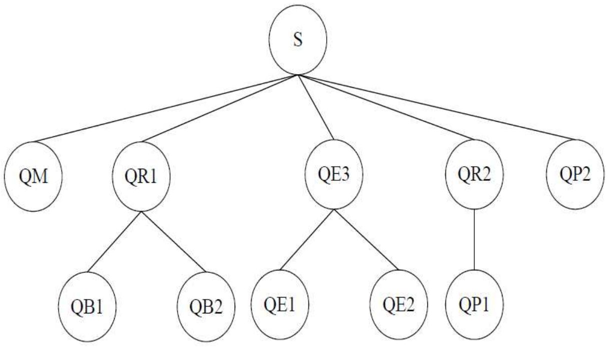

Figure 3. Logical tree structure

3.1. **High-dimensional quantum WSN node communication scheme.** In the high-dimensional quantum WSN, we use QSDC scheme based on high-dimensional entanglement swapping. This scheme is built on high-dimensional quantum Bell state measurement (HDBM), high-dimensional entanglement swapping characteristics and superdense coding based on high-dimensional quantum. "High dimensional" which represents a single quantum of the quantum system has a number of different polarization states and "d-dimensional" refers to a single quantum in the system having $(|0\rangle, |1\rangle, \cdots, |d-1\rangle)d$ polarization states. For the d $(d \geq 2)$ dimensional quantum systems, there exists a common set of Z-basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ and another set of X-basis $\{|X_0\rangle, |X_1\rangle, \cdots, |X_{d-1}\rangle\}$. There are d^2 d-dimensional EPR states, and each d-dimensional EPR state [12] used by high-dimensional Z-basis can be expressed as:

$$|\psi_{nm}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \varpi^{jn} |j\rangle \otimes |(j+m) \bmod d\rangle \tag{1}$$

where $d \geq 2$, $0 \leq n$, $m \leq d-1$, $\varpi = e^{2\pi i/d}$ and the operator $\otimes$ means tensor product. If $n = 0$, $m = 0$, we can obtain

$$|\psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \otimes |j\rangle \tag{2}$$

High-dimensional entangled EPR state $|\psi_{00}\rangle$, said the form of X-basis, and is:

$$\begin{aligned}|\psi_{00}\rangle &= \frac{1}{\sqrt{d}}\left(|X_0\rangle|X_0\rangle + |X_1\rangle|X_{d-1}\rangle + |X_2\rangle|X_{d-2}\rangle + \cdots + |X_{d-1}\rangle|X_1\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|X_k\rangle\left|X_{(d-k)\bmod d}\right\rangle\end{aligned} \tag{3}$$

where $|X_k\rangle = \frac{1}{\sqrt{d}}\sum\limits_{j=0}^{d-1} e^{2\pi ijk/d}|j\rangle = \frac{1}{\sqrt{d}}\sum\limits_{j=0}^{d-1}\varpi^{jk}|j\rangle$, $0 \le k \le d-1$.

Entanglement swapping is found by Zukowski and Zeilinger in 1993 [15]. Entanglement swapping has no direct interaction between two quantum systems to produce entangled. For the d-dimensional EPR state entanglement swapping, we take QE1 and QE3 as examples to provide details in this article. Nodes QE1 and QE3 share d-dimensional EPR states $|\psi_{00}\rangle_{12}$ and $|\psi_{00}\rangle_{34}$, node QE1 has particles 1, 2, and node QE3 has particles 3, 4. In the beginning, particles 1, 2 and 3, 4, are respectively entangled, and particles 1, 4 and 2, 3 are not mutually entangled. The four particles system state can be expressed as:

$$\begin{aligned}|\psi_{00}\rangle_{12}\otimes|\psi_{00}\rangle_{34} &= \left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_1\otimes|j\rangle_2\right)\otimes\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_3\otimes|j\rangle_4\right) \\ &= \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}|\psi_{ij}\rangle_{14}\left|\psi_{(d-i)\bmod d,j}\right\rangle_{23}\end{aligned} \tag{4}$$

From the above equation, if the node QE1 uses HDBM on the particles 1 and 4, it will have the probability $\frac{1}{d^2}$ to get $|\psi_{ij}\rangle_{14}$; at this time particles 2 and 3 will constitute a d-dimensional EPR state $\left|\psi_{(d-i)\bmod d,j}\right\rangle_{23}$. Not originally entangled particles respectively entangled on the 1, 4 and 2, 3, and these are characteristics of d-dimensional EPR state entanglement swapping. Thus, we can see a correlation on the measurement of particles 1, 4 and particles 2, 3, so we can take advantage of this association for communication design.

There are a total of d^2 forms of entanglement swapping, and a unified mathematical expression can be expressed as:

$$\begin{aligned}&|\psi_{nm}\rangle_{12}\otimes|\psi_{ld}\rangle_{34} \\ &= (I\otimes U_{nm}\otimes I\otimes U_{ld})\,|\psi_{00}\rangle_{12}\otimes|\psi_{00}\rangle_{34} \\ &= (I\otimes U_{ld}\otimes U_{nm}\otimes I)\,\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}|\psi_{ij}\rangle_{14}\left|\psi_{(d-i)\bmod d,j}\right\rangle_{23} \\ &= \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\varpi^{kj+mi-nm}\left|\psi_{(k+i)\bmod d,(l+j)\bmod d}\right\rangle_{14}\left|\psi_{(n-i)\bmod d,(j-m)\bmod d}\right\rangle_{23}\end{aligned} \tag{5}$$

In expression (5), $|\psi_{nm}\rangle$ and $|\psi_{ld}\rangle$ denote the Bell state in the d-dimensional Hilbert space. U_{nm} and U_{ld} denote d-dimensional quantum unitary operator. For the d-dimensional quantum systems, we can also use the d-dimensional unitary operator to achieve quantum superdense coding operations in order to complete the process of QSDC. D-dimensional quantum unitary operator [12] can be expressed as:

$$U_{nm} = \sum_{j=0}^{d-1}\varpi^{jn}\,|(j+m)\bmod d\rangle\langle j| \tag{6}$$

where $d \geq 2$, $0 \leq n,\ m \leq d-1$. If putting d-dimensional single-particle unitary operation U_{nm} on the first qubit of d-dimensional EPR state $|\psi_{00}\rangle$, you can get d-dimensional EPR state $\left|\psi_{n,(d-m) \bmod d}\right\rangle$:

$$(U_{nm} \otimes I)\left|\psi_{00}\right\rangle = \varpi^{-nm}\left|\psi_{n,(d-m) \bmod d}\right\rangle \tag{7}$$

Thus, available:

$$|\psi_{nm}\rangle = \varpi^{-nm}(U_{n,(d-m) \bmod d} \otimes I)\left|\psi_{00}\right\rangle \tag{8}$$

If putting d-dimensional single-particle unitary operations U_{nm} on the second qubit of d-dimensional EPR state $|\psi_{00}\rangle$, you can get d-dimensional EPR state $|\psi_{(n+w) \bmod d,(m+v) \bmod d}\rangle$. Formula is expressed as:

$$I \otimes U_{nm}\left|\psi_{wv}\right\rangle = \varpi^{nv}\left|\psi_{(n+w) \bmod d,(m+v) \bmod d}\right\rangle \tag{9}$$

Given the nature of the particle entanglement swapping theory and unitary operation, if we act the unitary operator U_{uv} $(0 \leq u, v \leq d-1)$ on the particle 4 of Formula (4), then we can get entanglement swapping form into the following form:

$$\begin{aligned}
&(I \otimes I \otimes I \otimes U_{uv})\left|\psi_{00}\right\rangle_{12} \otimes \left|\psi_{00}\right\rangle_{34} \\
&= (I \otimes U_{uv} \otimes I \otimes I)\frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\left|\psi_{ij}\right\rangle_{14}\left|\psi_{(d-i) \bmod d,j}\right\rangle_{23} \\
&= \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\varpi^{uj}\left|\psi_{(u+i) \bmod d,(v+j) \bmod d}\right\rangle_{14}\left|\psi_{(d-i) \bmod d,j}\right\rangle_{23}
\end{aligned} \tag{10}$$

As can be seen from the above equation, if the node QE1 uses HDBM on particles 1, 4, assuming that the measured result is $\left|\psi_{(u+i) \bmod d,(v+j) \bmod d}\right\rangle_{14}$, then the result of particles 2, 3 measured by node QE3 must be $\left|\psi_{(d-i) \bmod d,j}\right\rangle_{23}$. In other words, there is a correlation between the measurement results of particles 1, 4 and particles 2, 3. Thus, we can encode the information to be transmitted through the d-dimensional unitary operator and the receiver can easily get the information transmitted by the sender.

3.2. **High-dimensional QWSN node communication protocol.** In the high-dimensional QWSN, when the high-dimensional quantum sensor nodes detect new information, in Figure 4, such as QE1, it transmits the information to the father node QE3 in their communication time. QE3 fuses the information. After data fusion process, it transmits the information to the Sink node. If the distance between nodes and Sink node is far, using single-hop is unreliable. In order to transfer the information to Sink node in a more reliable way, multi-hop way is adopted, and at this point, it requires relay node to act as transit node for transmission [16]. The source node will transmit information to the relay node and the information will eventually be sent to Sink node. For example, node QP1, it first needs to transmit the information to QR2, and then the communication task with Sink node is completed by QR2. However, the distance between QP1 and Sink node is very close, so the QP1 communicates with Sink node directly in single-hop way which will save more energy. In this article we focus on how to achieve high-dimensional entanglement swapping QSDC between two nodes.

Without loss of generality, if QE1 intends to transfer a bunch of d-dimensional secret information to its father node QE3, the two nodes execute quantum communication protocols based on high-dimensional entanglement to transmit information.

Protocol packets can be divided into three categories: routing packets, join-request messages and control packets. The routing data packets are used to send data to the next one in the data sub-cycle. It contains several sections: source ID, next hop ID, forwarding the number of slots α_{Source}, accepting the number of slots β_{Source} and packet

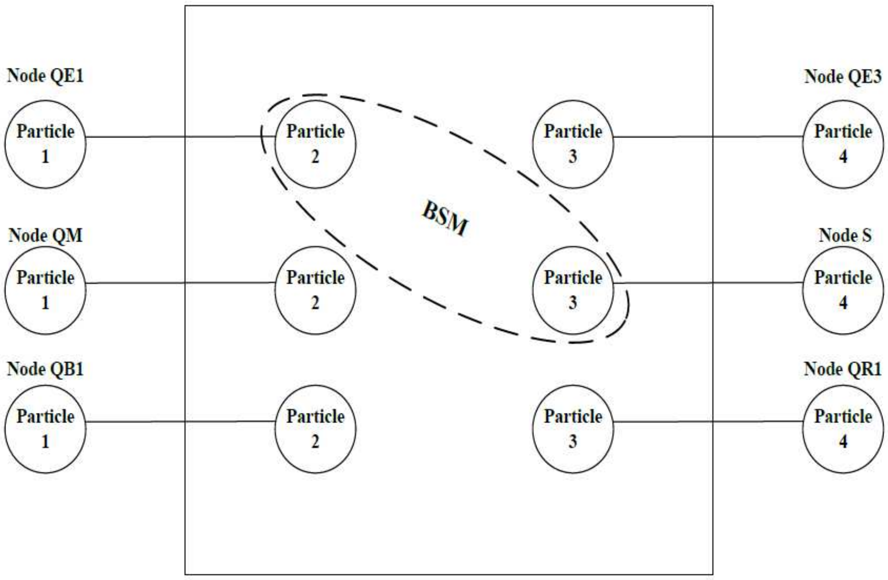

FIGURE 4. Entanglement swapping of the high-dimensional quantum WSN

Source node ID	Msg ID	Msg legth	payload

Source node ID	Next hop ID	α_{Source}	β_{Source}	packet

FIGURE 5. The routing packet

Source node ID	Next hop ID	α_{Source}	β_{Source}

FIGURE 6. Join-request message format

which includes source ID, message ID (Msg ID), the length of the message (Msg length) and payload.

Join-request message is mainly used for the adding of a new node when slot contention. It does not contain the data packet information, and simplify the routing packet format. HELLO message also has a similar definition. It mainly includes four parts: source ID, next hop ID, forwarding the number of slots α_{Source} and accepting the number of slots β_{Source}.

Assume a node has the number of n sub-nodes, in a control data packet, the control mechanisms of the sub-cycle and data sub-cycle need to be sent by the parent node, and such a control packet must be composed by the following parts: source ID, settings, control mechanisms and data mechanisms.

The specific steps of HQTP between QE1 and QE3 are as follows:

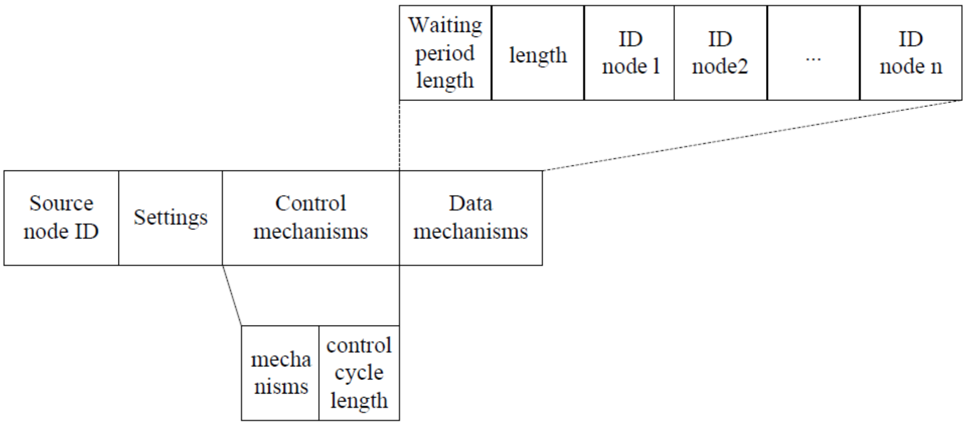

FIGURE 7. The control packet

(1) Nodes QE1 and QE3 respectively have N d-dimensional EPR states $|\psi_{00}\rangle$, which are recorded as $|\psi_{00}\rangle_{12}$ and $|\psi_{00}\rangle_{34}$. The particle sequences PS1 and PS2 are composed of the particles 1 and 2 of all the d-dimensional EPR states $|\psi_{00}\rangle_{12}$ by QE1. The particle sequences PS3 and PS4 are composed of the particles 3 and 4 of all the d-dimensional EPR states $|\psi_{00}\rangle_{34}$ by QE3.

(2) Node QE1 retains the particle sequence PS1 and sends sequence PS2 to the father node QE3. QE3 confirms the receipt of the particle sequence PS2 to QE1. The father node QE3 sends particle sequence PS4 to the node QE1, while preserving the particle sequence PS3. Node QE1 acknowledges the receipt of the particle sequence PS4 to the father node QE3.

(3) QE3 randomly selects M ($M << N$, and large enough to analyze the error rate of the transfer particle sequence) particles from the sequence PS2 as the detection particles, and tells the location of the M particles to QE1, and then randomly selects high-dimensional Z-basis $\{|0\rangle, |1\rangle\, |2\rangle, \cdots, |d-1\rangle\}$ or X-basis $\{|X_0\rangle, |X_1\rangle, \cdots, |X_{d-1}\rangle\}$ to measure these detection particles. When the measurement is completed, QE3 informs the basis and measurement results of each detection particle in the sequence to QE1. QE1 uses the same measurement-basis on the corresponding position in the particle sequence PS1 and compares the measurement results and the results announced by QE3.

$$|\psi_{00}\rangle_{12} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_1 \otimes |i\rangle_2 = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |X_i\rangle_1 \left|X_{(d-i) \bmod d}\right\rangle_2 \tag{11}$$

We can know by Equation (11), ideally, if they choose the high-dimensional Z-basis their measurements should be the same. If the measurement result of QE1 is $|i\rangle$, the measurement result of QE3 must also be $|i\rangle$ $(0 \leq i \leq d-1)$ inevitably. If they select the high-dimensional X-basis as the measurement-basis, the measurement result of QE1 is $|X_i\rangle$, and the measurement result of QE3 must be $\left|X_{(d-i) \bmod d}\right\rangle$ $(0 \leq i \leq d-1)$. In view of these theories, QE1 and QE3 can detect the error rate of the transfer particle sequence PS2. QE1 and QE3 use the same method to select M d-dimensional entangled particles to detect the transfer particle sequence PS4. If the error rate of PS2 or PS4 exceeds a certain threshold, it means the noise of the quantum channel is strong or there exists the eavesdropper, they will give up the communication, or that they think the quantum channel is security and begin to implement HQTP.

After the HQTP, QE1 has particle sequences PS1 and PS4, QE3 has particle sequences PS2 and PS3. Set the ordered particle sequences P1, P2, P3 and P4 respectively represent the sequences PS1, PS2, PS3 and PS4 removed detected particles. The specific steps of HQCP between QE1 and QE3 are as follows.

(1) Information transmission is based on the d-dimensional quantum entanglement swapping, when transiting one particle can transfer $2\log_2 d$ bits of classical information. The information that will be sent by QE1 can be expressed as $\{u_k v_k\}$ (k denotes the secret information in the k-th group, $1 \leq k \leq N - M$ and $0 \leq u_k, v_k \leq d - 1$). QE1 selects the unitary operator $U_{u_k v_k}$ encoding on the k-th particle P4(k) in the sequence P4, according to the value of $\{u_k v_k\}$. After operating, QE1 tells QE3 the fact through the classical channel.

(2) After receiving this information, QE3 puts HDBM on the pairs of entangled particles $(\mathrm{P2}(k), \mathrm{P3}(k))$ on the sequence of its own particle sequences P2 and P3, assuming measurement result is $\left|\psi_{(d-i) \bmod d, j}\right\rangle_{23}$, and keeps the result secret. Then, QE1 measures entangled particle pairs $(\mathrm{P1}(k), \mathrm{P4}(k))$ on the sequence of its own particles P1 and P4, and measurement result is $\left|\psi_{x_k y_k}\right\rangle_{14}$ $(0 \leq x_k, y_k \leq d - 1)$, and tells QE3 this measurement result, and the value x_k and y_k. According to the formula, we can set up the following equation:

$$\begin{cases} x_k = (u_k + i_k) \bmod d \\ y_k = (v_k + j_k) \bmod d \end{cases} \tag{12}$$

QE3 can be deduced the secret information transferred by QE1 according to the following formula.

$$\begin{cases} u_k = (x_k - i_k) \bmod d \\ v_k = (y_k - j_k) \bmod d \end{cases} \tag{13}$$

For the unrelated third parties, the values x_k and y_k are random, while for QE3, x_k and y_k can be used to decrypt the secret information of QE1. After decoding secret information, QE3 uses certain error correction protocol to get confidential information QE1 passed to it. Thus, the node QE1 sends the information sequence to QE3 safely, and completes the process of high-dimensional QSDC. Similarly, other nodes transmit a string of d-dimensional secret information to the Sink node, similarly to the above situation, so we will not repeat them here.

4. **System Performance Analysis.**

4.1. **The network throughput analysis.**

In the QWSN, suppose the nodes QE1 and QE3 establish the entanglement in a qubit transfer process successfully, and the probability is P_q. The probability of QE1 successfully carrying on HDBM is P_m. The probability of QE3 successfully receiving the transmitted qubit is P_d. The total time to transfer a qubit can be expressed as:

$$T = T_r + T_q + T_m + T_t + T_d \tag{14}$$

In the formula T_r is the average time that QE1 notices QE3 to prepare to receive the quantum information; T_m is the average time that both sides QE1 and QE3 establish the entangled photon pair; T_t is the average time that QE1 carries on HDBM; T_d is the average time that carries on the d-dimensional unitary operator to resume the quantum information according to the measurement results of QE1.

Suppose the number of entangled pairs that the entanglement needs to transmit at a time being successfully established, the number of times that successfully carry on HDBM and the number of transmission times that QE3 successfully examines the transmission qubit to be subject to the geometric distribution. The time of establishing entanglement once is q. The time that carries on HDBM is m. The receiving end QE3 examines transmission qubit time is d, and then we can get the following formula:

$$T_q = \frac{q}{P_q} \quad T_m = \frac{m}{P_m} \quad T_d = \frac{d}{P_d} \tag{15}$$

Assuming that establishing the entanglement, transmitting end QE1 carrying on HDBM and the receiving end QE3 examination transmission qubit are mutual independent. Then the probability of transmitting one qubit successfully can be expressed as:

$$P = P_q \bullet P_m \bullet P_d \tag{16}$$

The approximate throughput rate of quantum information can be represented as:

$$T_P = \frac{P_q \bullet P_m \bullet P_d}{T} \text{ (qubit/s)} \tag{17}$$

In the numerical calculations, take the parameters $T_q = 3\text{ns}$, $T_m = 2\text{ns}$, $T_d = 5\text{ns}$ and set $T_t = \frac{3}{2}T_r$, $P_m = P_d = 0.7$. Figure 8 shows the change of throughput T_p along with P_q.

When P_d is increasing, the quantum communication throughput T_p of the system becomes greater. We can also see that, when T_r increases, the quantum communication throughput T_p of the system is significantly reduced.

Figure 9 shows the relationship between T_p and the number of the system nodes. In Figure 9, we set $P_q = 0.5$, $P_m = P_d = 0.7$. It can be seen from Figure 9, the quantum communication system transmission efficiency is increased with the number of system sensor nodes.

In the high-dimensional QWSN communication program, the effectiveness of the energy can also be guaranteed. Major waste of the energy in the radio equipment communication is idle listening, cross talking and conflicting [17]. Time slot in the control sub-cycle in this protocol has been allocated, and the node explicitly knows when to sleep, when to send data, when to turn on the wireless electrically to accept the data. In data cycle, when it needs to send or receive data nodes it only needs to be waken up. Using these mechanisms, the energy waste is minimized.

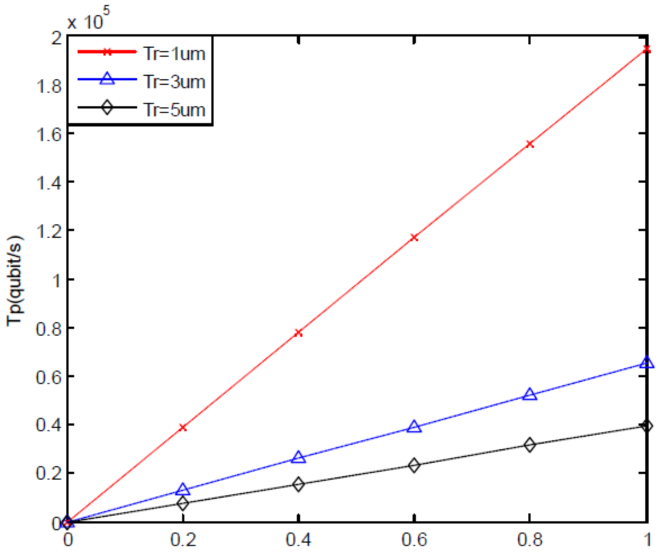

Figure 8. Relationship of throughput T_p and the probability P_q of entanglement

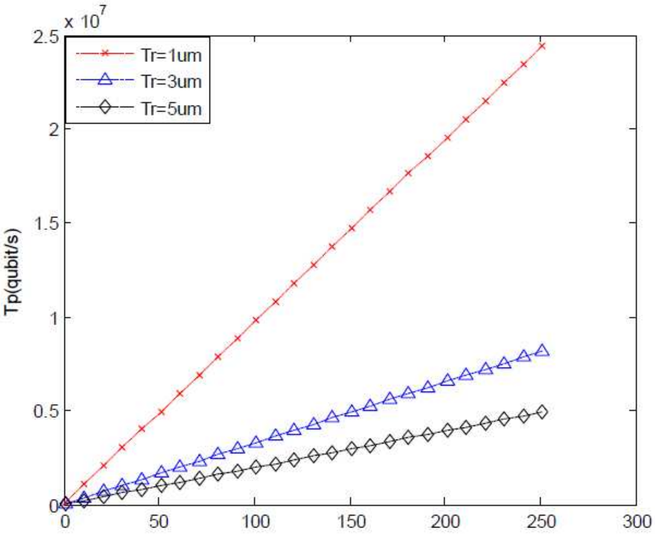

Figure 9. Relationship of throughput T_p and numbers of sensor nodes

4.2. **Safety analysis.** In this paper, the high-dimensional QSDC process does not transmit any qubits, and protocol security is on account of the security of the quantum channel. That is, if the quantum channel is secure, the quantum communication process is safe. Network eavesdropper (Eve) only visits the transmission sequence. Without loss of generality, we analyze Eve eavesdropping on the particle sequence of the sending node. Eve eavesdropping on the sequence of the receiving node is similar. For two-particle system, the sending node and receiving node randomly select Z-basis or X-basis to detect eavesdropping by measuring the detection particles. Such eavesdropping detection method is similar to the eavesdropping detection method of EPR protocol. EPR protocol has been proven to be unconditionally secure. Only after guaranteeing the security of the transmission sequence, the sending node will perform Bell measurement-basis and publish measurement results, so for the two-dimensional quantum systems, security mentioned in this protocol is equivalent to security in the EPR protocol. For example, if the eavesdropper Eve intercepts transmission particle sequence of the sending node and sends a bunch of fake sequence to the receiving node. For the two-dimensional system, assume the sending node and receiving node have the equal probability to select Z-basis or X-basis randomly. If the transmission quantum state is $|0\rangle$, the eavesdropper Eve has 1/2 probability selecting Z-basis to measure, and after the measurement the quantum state is still $|0\rangle$, so the recipient will not notice. When Eve has 1/2 probability selecting X-basis to measure, she will have 1/2 probability to get the result $|0\rangle$, so the probability Eve randomly selects measurement-basis to measure a quantum without affecting the quantum state being $\frac{1}{2} + \frac{1}{2} . \frac{1}{2}$. For d-dimensional system, it is assumed that the quantum state of the transmission of quantum state is $|d-1\rangle$, Eve has 1/2 probability selecting Z-basis to measure, and after the measurement, the quantum state remains $|d-1\rangle$, so the recipient will not notice. When Eve has 1/2 probability selecting X-basis to measure, she will have $\frac{1}{d}$ probability to get the result $|d-1\rangle$, so the probability Eve randomly selects measurement-basis to measure a d-dimensional quantum without affecting the quantum state being $\frac{1}{2} + \frac{1}{2} . \frac{1}{d}$. Therefore, by detecting the M particles to detect eavesdroppers, it detects the probability of the eavesdroppers is $1 - \left(\frac{1}{2} + \frac{1}{2d}\right)^M$.

As can be seen from Figure 10, when M increases, the probability of detecting the eavesdropper becomes greater, and when it reaches a certain value, the eavesdropper must be detected. We also can see from Figure 11, when the M is certain, the probability

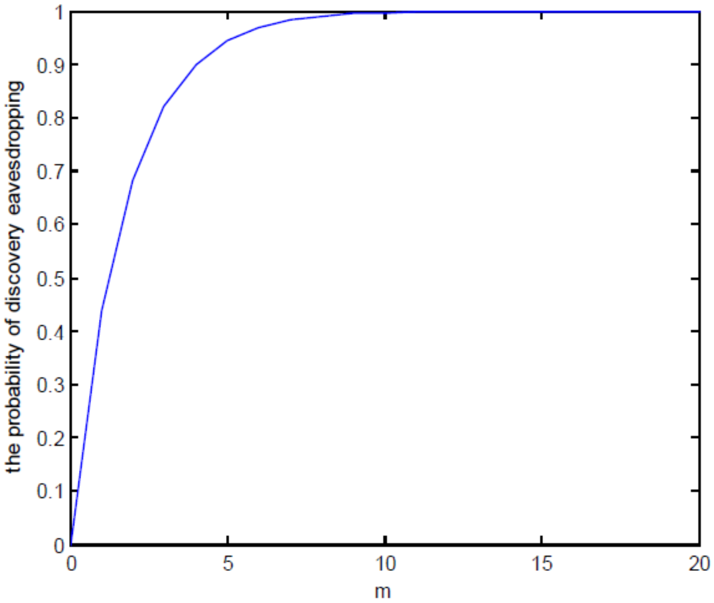

FIGURE 10. Relationship of probability and the numbers of detection particles

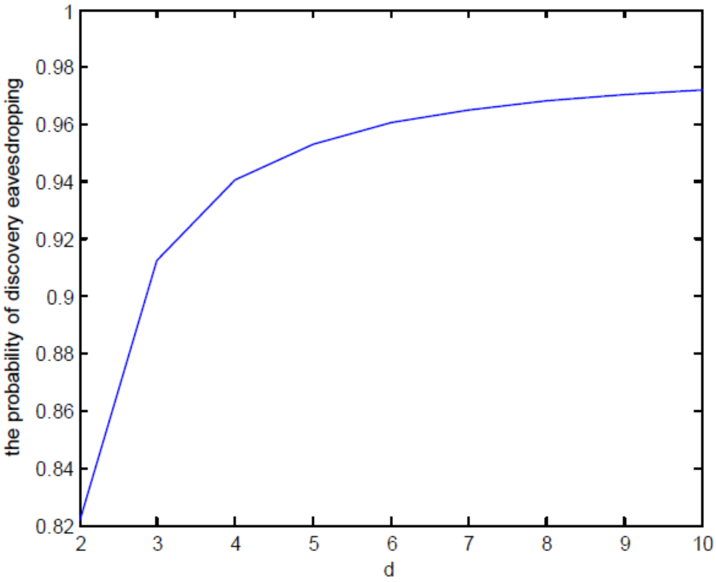

FIGURE 11. Relationship of probability and the dimension

of detecting eavesdropping is significantly higher than the low-dimensional, and security is also higher.

4.3. **Efficiency analysis.** The d-dimensional quantum systems can achieve the super-dense coding, only sending one particle, it can achieve $2\log_2 d$ bits classical information, and it is the $\log_2 d$ times under two-dimensional EPR state. There is no doubt that it can significantly improve the efficiency of information transmission of the network and d-dimensional quantum systems with higher security than the two-dimensional quantum systems [18].

According to Figure 12, d1, d2, d3 represent 3-dimension, 5-dimension, and 8-dimension quantum system respectively. N represents the number of the particles. We can obtain

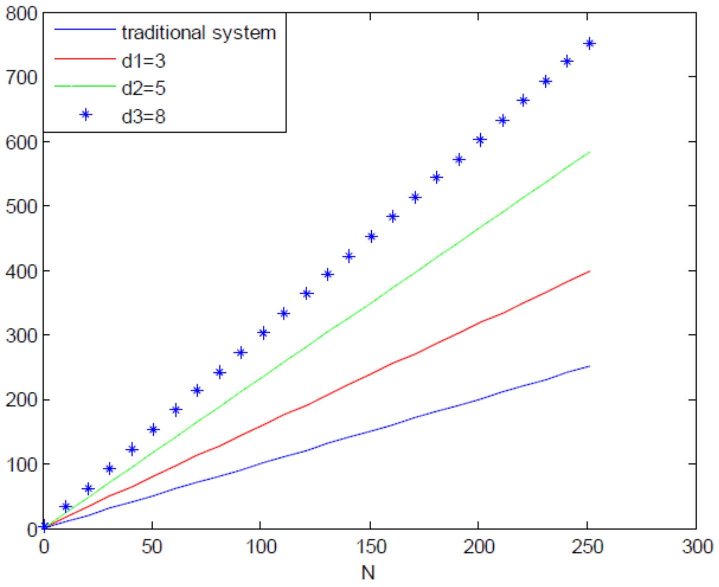

FIGURE 12. Efficiency comparison between traditional system and quantum system

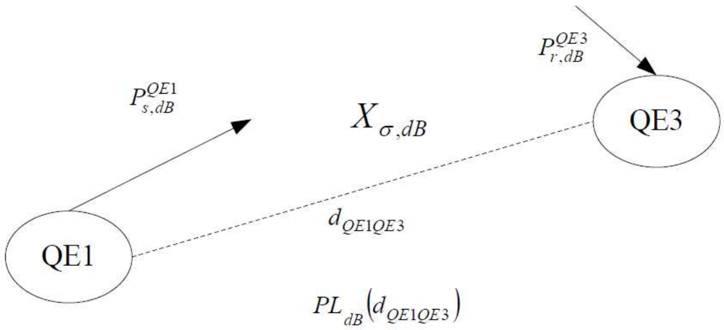

FIGURE 13. Analysis of power between two nodes

from Figure 12, the efficiency of information transmission of the quantum network is higher than the traditional system. When d is increasing, the efficiency is higher.

4.4. **Reliability analysis.** In the high-dimensional QWSN communication program, the classical channel only transmits a small amount of information needed in quantum communication, and the real information is transmitted through the quantum channel. According to the quantum mechanics, the quantum channel is secure and reliable. In order to ensure the reliability of the system, we need to ensure the reliability of the classic channel. In fact, the average received power of the classical channel depends on the different position of the nodes. The standard deviation of the distribution σ referred to as “shadow” can be used to express this change. The standard deviation of the amplitude indicates the degree of undulation of the signal caused by the irregularity of the reception and transmission antenna. With zero mean Gaussian random distribution of the changes in the standard deviation, $X_{\sigma,dB}$ represents the shaded portion. In Figure 13, we set node QE3 received signal strength $P_{r,dB}^{QE3}$, the node QE1 transmission d_{QE1QE3} distance required transmission power $P_{r,dB}^{QE3}$, and the relationship between them is represented by the following formula:

$$P_{r,dB}^{QE3}\left(d_{QE1QE3}\right) = P_{s,dB}^{QE3} - PL_{dB}\left(d_{QE1QE3}\right) - X_{\sigma,dB} \tag{18}$$

The connection condition of the receiver QE3 is that the specific $P_{r,dB}^{QE3}$ is higher than the threshold value P_{th}. So the connection probability $p\left(d_{QE1QE3}\right)$ between QE1 and QE3 can be expressed as follows:

$$p\left(d_{QE1QE3}\right) = \Pr\left[P_{r,dB}^{QE3}\left(d_{QE1QE3}\right) > P_{th}\right] = \Pr\left[X_{\sigma,dB} + \mu\left(d_{QE1QE3}\right) < 0\right] \quad (19)$$

Among $\mu\left(d_{QE1QE3}\right) = -P_{s,dB}^{QE1} + PL_{0,dB} + 10n\lg\left(d_{QE1QE3}/d_0\right) + P_{th}$, therefore, the above formula can be again expressed as:

$$p\left(d_{QE1QE3}\right) = \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{0}\exp\left[-\frac{\left(t-\mu(d_{QE1QE3})\right)^2}{2\sigma^2}\right]dt = \frac{1}{2} - \frac{1}{2}erf\left(\frac{\mu\left(d_{QE1QE3}\right)}{\sqrt{2\pi}\sigma}\right) \quad (20)$$

The reliable communication in WSN is low distance covered. We can increase the structural reliability of communications using a single-hop or multi-hop from the above Formula (20). There are n intermediate hops, which can be drawn $p\left(\frac{d}{n+1}\right)^{n+1} > p\left(d\right)$ between two nodes, and the correct rate of the multi-hop communication is significantly larger, multiple paths having a high reliability. Therefore, we place relay nodes in the path between the sending node and the receiver node, to satisfy the conditions for a multi-hop. To the closer nodes, they should communicate directly, and using multi-hop does not make much sense.

5. Conclusions.

WSN has poor security in data transmission, the network attacker can obtain sensitive information by eavesdropping and add fake illegal nodes, for this phenomenon, we present a new system structure of high-dimensional QWSN in this paper, and we also propose a communication scheme of QSDC based on the high-dimensional entanglement swapping with superdense coding between nodes. According to the quantum mechanics, including Heisenberg uncertainty principle, the non-cloning theorem and characteristics of entangled particles, this communication scheme can significantly improve network node communication security and efficiency of information transmission. We compared the throughput, safety, reliability and efficiency of the QWSN and the WSN, and the simulation result shows that the QWSN has better performance.

Acknowledgments. This work is supported by the Henan Provincial Department of Education Science and Technology Research key project (No. 13A510330), Henan Provincial Key Discipline Open Laboratory of Mine Informatization (KY2015-08) and Basic and Advanced Technology Research Project of Henan Province (No. 152300410103).

REFERENCES

[1] J. Q. Duan, D. Y. Gao, C. H. Foh and H. K. Zhang, TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, *Ad Hoc Networks*, vol.11, no.8, pp.2675-2692, 2013.

[2] R. Q. Yan, H. H. Sun and Y. N. Qian, Energy-aware sensor node design with its application in wireless sensor networks, *IEEE Transactions on Instrumentation and Measurement*, vol.62, no.5, pp.1183-1191, 2013.

[3] H. Jeon, J. Choi, S. W. McLaughlin and J. Ha, Channel aware encryption and decision fusion for wireless sensor networks, *IEEE Transactions on Information Forensics and Security*, vol.8, no.4, pp.619-625, 2013.

[4] F. G. S. L. Brandao and J. Oppenheim, Public quantum communication and superactivation, *IEEE Transactions on Information Theory*, vol.59, no.4, pp.2517-2526, 2013.

[5] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, *Physical Review A*, vol.65, pp.032302/1-032302/3, 2002.

[6] F. G. Deng, G. L. Long and X. S. Liu, A two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, *Physical Review A*, vol.68, pp.1-6, 2003.

[7] Y.-P. Luo, C.-Y. Lin and T. Hwang, Efficient quantum dialogue using single photons, *Quantum Information Processing*, vol.13, no.11, pp.2451-2461, 2014.

[8] Z.-H. Li, M. Al-Amri and M. Suhail Zubairy, Direct quantum communication with almost invisible photons, *Physical Review A*, vol.89, pp.052334-1-052334-5, 2014.

[9] W. L. Li, J. B. Chen, X. L. Wang and C. Li, Quantum secure direct communication achieved by using multi-entanglement, *International Journal of Theoretical Physics*, vol.54, no.1, pp.100-105, 2015.

[10] H. Lu, C.-H. Fred Fung, X. F. Ma and Q. Y. Cai, Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel, *Physical Review A*, vol.84, pp.042344-1-042344-5, 2011.

[11] J. Shi, Y. X. Gong, P. Xu, S. N. Zhu and Y. B. Zhan, Quantum secure direct communication by using three-dimensional hyperentanglement, *Communications in Theoretical Physics*, vol.56, no.5, pp.831-836, 2011.

[12] R. Zhou, Y. L. Zhu and Y. Y. Nie, One-way communication scheme based on superdense coding of four dimension two particles, *Acta Photonica Sinica*, vol.1, pp.156-159, 2010.

[13] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, *Physical Review A*, vol.4, pp.1-4, 2005.

[14] X. S. Liu, G. L. Long, D. M. Tong and F. Li, General scheme for superdense coding between multiparties, *Physical Review A*, vol.2, pp.1-4, 2002.

[15] M. Zukowski and A. Zeilinger, Home MA Eker AK Event-ready-detectors Bell experiment via entanglement swapping, *Physical Review Letters*, vol.26, pp.4287-4290, 1993.

[16] H. Hu, H. B. Zhu and Q. Zhu, Performance analysis of multi-hop wireless networks under different hopping strategies with spatial diversity, *KSII Transactions on Internet and Information Systems*, vol.10, pp.2548-2566, 2012.

[17] H. Kwon, T. H. Kim, S. Chio and B. G. Lee, A cross-layer strategy for energy-efficient reliable delivery in wireless sensor networks, *IEEE Transactions on Wireless Communications*, vol.12, pp.3689-3699, 2006.

[18] B. P. Helle and P. Asher, Quantum cryptography with 3-state systems, *Physical Review Letters*, vol.15, pp.3313-3316, 2000.