Wireless Pers Commun (2015) 80:193–202
DOI 10.1007/s11277-014-2003-9

Development of Security WLAN Protocol Based on Quantum GHZ Stats

Hongyang Ma · Shumei Wang

Published online: 15 August 2014

Abstract This paper addresses the security WLAN protocol based on Quantum Greenberger–Horne–Zeilinger stats to overcome the flaws of wired equivalent privacy, temporal key integrity protocol, counter mode with CBC-MAC protocol, IEEE802.11i protocol, and ensure wireless communication information security. Our main theorem have two important corollaries. The first is an ingenious application of quantum mechanics to apply in wireless communication theorem. The second is the proof of the protocol that Eve invariably introduces errors within communication network if it wants to gain useful information. Here the novel idea is that quantum cryptography guarantees the security of wireless communication information.

Keywords WLAN · Security · GHZ stats · 802.11i

1 Introduction

Recently, wireless local area networks (WLAN) [1,2] are encroaching on the traditional realm of "fixed" or "wired" networks, which enables people to connect with each other regardless of location. New technologies targeted at computer networks promise to do the same for Internet connectivity. The most successful wireless data networking technology this far has been 802.11i. As a prior relevant research, Nguyen et al. [3] proposed a scheme integrating quantum cryptography in 802.11i security mechanisms for the distribution of the encryption keys. However, the work of Nguyen et al. only integrate BB84 on 802.11i for wireless communication, did not consider further refer information on multiparty problem. Wijesekera et al. [4] proposed a multi-agent based approach for QKD in WiFi Networks,

H. Ma (✉)
College of Information Science and Engineering, Ocean University of China, Qingdao 266100, China
e-mail: hongyang_ma@yahoo.com.cn

H. Ma · S. Wang
School of Sciences, Qingdao Technological University, Qingdao 266033, China

which discussed the use of QKD for key distribution in 802.11 wireless networks. The work of Wijesekera et al. consider multi-agent, but did not consider more promising starting point.

Now, quantum communication and computation are new areas of information processing that make use of quantum properties in order to permit the realization of new ways of communication. A number of QKD protocols have been presented and extended to quantum encryption and quantum searching. In the mid of 1980s, Bennett and Brassard proposed the first QKD protocol, the so-called BB84 protocol [5]. Ekert developed a QKD protocol using the entanglement of an Einstein–Podolsky–Rosen (EPR) pair [6], in which he described a cryptographic scheme where EPR pairs of particles were used to generate identical random numbers in remote places. The investigations of quantum communication as well as quantum secure direct communication have been carried out by some groups [7–10]. Moreover, a quantum secret sharing between multiparty and multiparty without entanglement has been proposed by Ma et al. [11].

QKD is an ingenious application of quantum mechanics in wireless information field. In the paper, a new security WLAN protocol is developed, which uses quantum Greenberger–Horne–Zeilinger (GHZ) stats to ensure wireless information security. The supplicant send qubits to the access point by the authenticator server, which share GHZ states. The organization of this paper is organized as follows. In Sect. 2, it analyzes the shortcomings of wired equivalent privacy (WEP), temporal key integrity Protocol (TKIP), counter mode with CBC-MAC Protocol (CCMP), and described the quantum GHZ state in detail. In Sect. 3, the protocol is depicted that an ingenious application of quantum mechanics to apply in wireless theorem. Section 4 lists out discusses the security problem. Finally, conclusion remark is drawn in Sect. 5.

2 Overview

2.1 The Challenge of WLAN Protocol

There are many flaws for WEP, TKIP, CCMP. For WEP, it is initially designed to equal to the security wired network, which keys come in two parts: the secret key, which consist of 40 secret bits or 104 secret bits; the initialization vector (IV), which consist of 24 secret bits. This key structure is easy intercepting a number of same IV data packets in the IV space and restores to orignal key by mathematical and statistical analysis, which limits the IV space only to 2^{24}. WEP cann't resist the replay attack and the exhaustion attack.

Next, TKIP retains the basic architecture and operations of WEP, incorporates several new protocol features to defend WEP's weak points against attack, replaces WEP's linear hash with a more robust cryptographic integrity check hashing algorithm, derives a unique RC4 key for each frame to mitigate attacks against weak WEP keys. To mitigate the attacks against IV, it doubles the length of the IV from 24 to 48 secret bits, which effectively prevents exhausting the IV space during the limited lifetime of a key. But, it is only a transitional algorithm, which can not fundamentally solve the security issues of WLAN data encryption.

Then, CCMP initialize a temporary key for each dialogue, which based on Advanced Encryption Standard and the Cipher Block the Chain-Massage Authentication Code. So it can effectively resist the replay attack with the help of the message generated from such dialogue that consists of different serial number. Even if it was faced with an exhaustion attack, the key length is 128 secret bits and the exhaustive workload are 2^{127}. Therefore, it needs to much time to decipher keys with exhaustion attack on a classical computer, which seems impossible to manage it.

However, with the development of new quantum computers, it becomes easier to crack because quantum computers have a super parallel processing capability. There is no secret for CCMP in the face of quantum computer.

2.2 Quantum Cryptography: GHZ Theory

Suppose that Alice, Bob, and Charlie each have one particle from a GHZ triplet that is in the state $\left|\psi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)$, they each choose at random whether to measure the x or y direction. They then announce publicly in which direction they have made a measurement, but not the results of their measurements. Half the time, Bob and Charlie, by combining the results of their measurements, can determine what the result of Alice's measurement was. This allows Alice to establish a joint key with Bob and Charlie, which she can then use to send her message.

GHZ states has been proposed by Hillery et al. [12]. It can be used to split information in such a way that if one is in possession of all of the parts, the information can be recovered, but if one has only some of the parts, it cannot. Eve will introduce errors and can thereby be detected.

3 Quantum Cryptography Architectures In Ieee 802.11 WLAN

3.1 Elements of Network

The protocol based on quantum GHZ stats consist of three major physical components:

Stations (STA), a wireless client, transfer classical and quantum information date. It not only plays the traditional role, but also transfers quantum information date. Access points (AP), is responsible for transmitting the classic and quantum information packet. If it obtains legal authorization after authentication, then it can provide STA with wireless network access services and transmit classical data. Addition, AP has the capacity of quantum communication. Authentication server (AS), is the core of the whole authentication system. In fact, the authentication exchange is logically carried out between STA and AS to complete the actual authentication of users. This device is also required the capacity of quantum communication, and construct quantum GHZ state together with STA and AP.

3.2 Handshake Protocol

The processes of quantized handshake protocol are as follows, which can be seen in Fig. 1:

Step 1: STA associates with the 802.11 network.
Step 2: STA starts the 802.1X exchange with an EAPOL-Start message.
Step 3: After AP receives EAPOL-Start, then tranfer an EAP-Request/Identity frame.
Step 4: STA replies with an EAP-Response/Identity frame, then transfer to AS as a Radius-Access-Request packet.
Step 5: AS determines the type of authentication that is required, sends an EAP-Request for the method type to STA by AP.
Step 6: STA gathers the reply from the user and sends an EAP-Response in return. The response is translated by the authenticator into a Radius-Access-Request with the

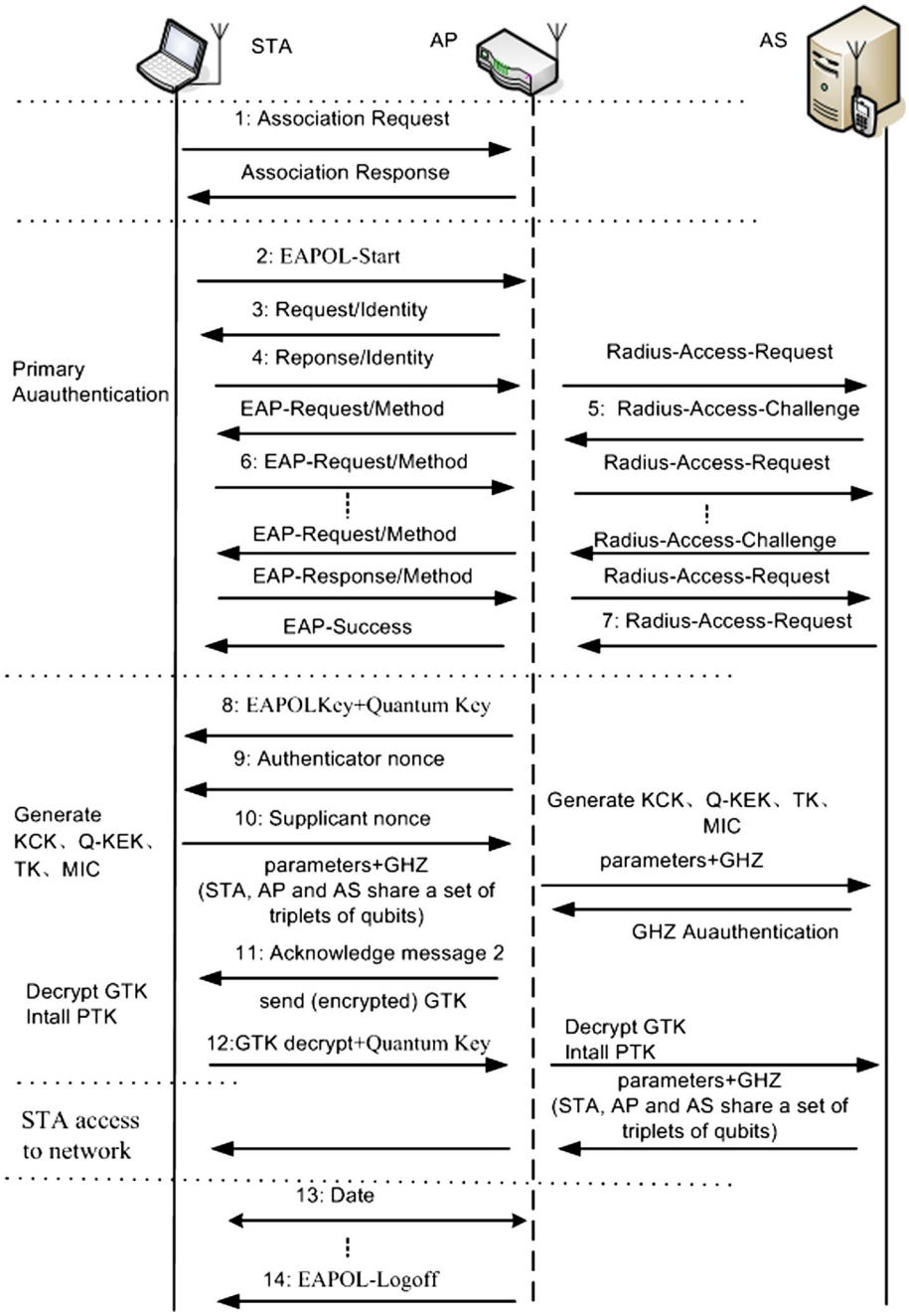

Fig. 1 Handshake protocol

response to the challenge as a data field. Steps 5 and 6 repeat as many times as is necessary to complete the authentication.

Step 7: AS grants access with a Radius-Access-Accept packet, which issues an EAP-Success frame. STA obtains authorized depend on parameters passed back from AS.

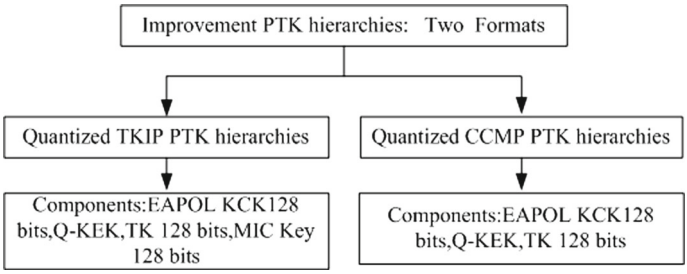

Fig. 2 Quantized TKIP and quantized CCMP hierarchies

Step 8: AP distributes keys to STA using EAPOL-Key messages, following receipt of the Access-Accept packet. And then allocates classical cipher and quantum key through the four-way handshake.

Step9: Authenticator nonce (ANonce) is sent by AP, which consist authenticator MAC addresses (APA) and replay counter field values and other information. When STA received, replay counter field value m_1 from Anonce compared with previous legal authorized value m_2. If $m_1 \leq m_2$, STA gives up accepting data. If $m_1 > m_2$, supplicant nonce (SNonce) is generated by STA, which includes supplicant MAC address (SA) and other information. According to different types of network encryption, the original PTK has two formats named TKIP and CCMP. Similarly, improvement PTK hierarchies also has two formats than quantized TKIP hierarchies and quantized CCMP hierarchies, shown in Fig. 2.

The following elaboration is mainly based on quantized CCMP format. Amendment as follows: TKIP's transient key consists of a total of 512 bits, quantized TKIP's transient key consists of a total of 384 bits and qbits. CCMP's transient key consists of a total of 384 bits, quantized CCMP's transient key consists of a total of 256 bits and qbits. Quantized TKIP key hierarchies consists of four parts: the 128-bit EAPOL-KCK for integrity check of message; quantum key encryption key (Q-KEK) is used to encrypt keying messages with STA and AP; the 128-bit TKIP TK is traditional data of encrypted key between AP and STA; the 128-bit TKIP MIC Key for integrity check of Michael. Similarly, quantized CCMP key hierarchies consists of three parts: the 128-bit EAPOL-KCK for integrity check of message; the 128-bit CCMP TK is traditional data of encrypted key between AP and STA; expression of Q-KEK as above.

Step10: AP received Snonce, and add its own address, then convert to AS. AS makes five parameters (PMK, ANonce, SNonce, APA, SA) TKIP and CCMP use the pseudorandom function expansion to expand the 256 bits into the pairwise transient key (PTK). The method of constructing quantized TKIP format and quantized CCMP format is same as previous mentioned. Original KEK is encoded into quantum information Q-KEK, and then these three are transmitted and authenticated. STA, AP and AS share a set of triplets of qubits in GHZ state $\left|\Psi\right\rangle_{ABC} = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle_{ABC} + \left|111\right\rangle_{ABC}\right)$ STA allocates two particles B, C from each GHZ state to AP and AS separately, and reserved a particle A for itself. Among them, GHZ state is a particle that contains three particles meeting the maximally entangled state. Subscript A, B, and C are particles subordinate to STA, AP and AS. STA encoded N qubits, $\left|\varphi\right\rangle = \otimes_{i=0}^{N-1}\left|\varphi_i\right\rangle_D$, which each qubit is represented by D. Through GHZ state, STA sends qubit information to AS. Four qubit quantum system system can then be written as

$$
\begin{aligned}
\left|\theta\right\rangle_{DABC} &= \otimes_{i=0}^{N-1}\left(\left|\varphi_i\right\rangle_D\left|\Psi\right\rangle_{ABC}\right)\\
&= \otimes_{i=0}^{N-1}\left\{\left(a_i\left|0\right\rangle_D + b_i\left|1\right\rangle_D\right)\frac{1}{\sqrt{2}}\left(\left|000\right\rangle_{ABC} + \left|111\right\rangle_{ABC}\right)\right\}\\
&= \otimes_{i=0}^{N-1}\left\{\frac{1}{2\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)_{DA}\left(a_i\left|00\right\rangle + b_i\left|11\right\rangle\right)_{BC}\right.\\
&\quad + \frac{1}{2\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right)_{DA}\left(a_i\left|00\right\rangle + b_i\left|11\right\rangle\right)_{BC}\\
&\quad + \frac{1}{2\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right)_{DA}\left(-b_i\left|00\right\rangle + a_i\left|11\right\rangle\right)_{BC}\\
&\quad \left. + \frac{1}{2\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right)_{DA}\left(b_i\left|00\right\rangle + a_i\left|11\right\rangle\right)_{BC}\right\}. \qquad (1)
\end{aligned}
$$

Equation (1) can be written

$$
\begin{aligned}
\left|\theta\right\rangle_{DABC} = \otimes_{i=0}^{N-1}&\left\{\frac{1}{2\sqrt{2}}\left|\phi^+\right\rangle_{DA}\left[\left|+\right\rangle_B\left(a_i\left|0\right\rangle + b_i\left|1\right\rangle\right)_C + \left|-\right\rangle_B\left(a_i\left|0\right\rangle - b_i\left|1\right\rangle\right)_C\right]\right.\\
&+ \frac{1}{2\sqrt{2}}\left|\phi^-\right\rangle_{DA}\left[\left|-\right\rangle_B\left(a_i\left|0\right\rangle + b_i\left|1\right\rangle\right)_C + \left|+\right\rangle_B\left(a_i\left|0\right\rangle - b_i\left|1\right\rangle\right)_C\right]\\
&+ \frac{1}{2\sqrt{2}}\left|\psi^-\right\rangle_{DA}\left[\left|+\right\rangle_B\left(-b_i\left|0\right\rangle + a_i\left|1\right\rangle\right)_C + \left|-\right\rangle_B\left(-b_i\left|0\right\rangle - a_i\left|1\right\rangle\right)_C\right]\\
&\left. + \frac{1}{2\sqrt{2}}\left|\psi^+\right\rangle_{DA}\left[\left|+\right\rangle_B\left(b_i\left|0\right\rangle + a_i\left|1\right\rangle\right)_C + \left|-\right\rangle_B\left(b_i\left|0\right\rangle - a_i\left|1\right\rangle\right)_C\right]\right\}. \qquad (2)
\end{aligned}
$$

where $\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right)$, $\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle \pm \left|11\right\rangle\right)$, $\left|+\right\rangle = \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}$ and $\left|-\right\rangle = \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}$.

STA measures Bell state for DA, and then through four possible measured results of STA: AS and AP can transmit qubit BC in the following four forms as $\left(a_i\left|0\right\rangle \pm b_i\left|1\right\rangle\right)_C$, $\left(a_i\left|1\right\rangle \pm b_i\left|0\right\rangle\right)_C$. When $\left(a_i\left|1\right\rangle \pm b_i\left|0\right\rangle\right)_C$ is obtained, the unitary transformation is $X(ZX)$ corresponding to the symbol "+" ("−") in the equations. When $\left(a_i\left|0\right\rangle \pm b_i\left|1\right\rangle\right)_C$ obtained, the unitary transformation is $I(Z)$ corresponding to the symbol "+" ("−"). After these operations, the key is transmitted to the server. STA and AS release part of the quantum information. If the test is correct, then STA is a legitimate user. Otherwise, there must be illegal eavesdroppers. The unitary transformation can be expressed as $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

Step11: Quantum keys authenticate successfully. Then, communication between STA and AP can be transmitted by TK after encrypted, TK is the key format of the original CCMP, so it can be compatible with the original protocol. Second, start the group key authentication, and consult with group temporal key (GTK). According to the same algorithm that generated PTK, AS generates group transient cycle key by utilizing information such as GMK and APA as well as protecting broadcasting information by using codes temporal key from GTK. The generation of GTK does not need customer participation, which can be seen in Fig. 3.

Step12: The negotiation of authenticated response information key pairs that delivered from STA to AS has been successful, and the installation of PTK and GTK is completed.

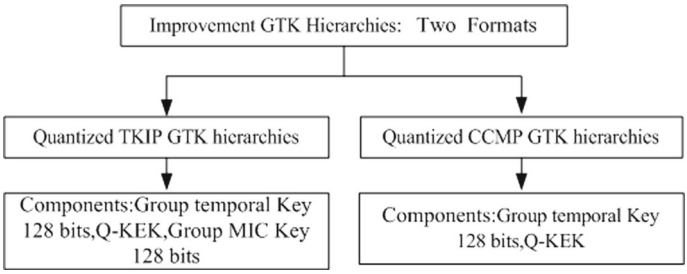

Fig. 3 Improvement GTK hierarchies

Step13: After the data authentication, PTK and GTK of AP and STA are all new, and AP and STA have built a secure data transmission channel, which opened the controlled port and made data transmission impossible. At this point, this case is one of the three modes of IEEE802.1x authentication, which means forced authentication mode. In this mode, the opened controlled port actually has been authorized and then STA can access to network. When data transfer completes, next step is moving on.

Step14: When STA no longer needs to access to network, an EAPOL-Logoff message will be sent out and connection port will be back to the unauthorized state.

4 Analysis of Protocol Security

This protocol security analysis is as follows:

(i) Eve intercept the information sent from STA, and construct illegal GHZ state with AP and AS, These particles the three obtained are represented by E, Y, and Z. Suppose that Eve has triplets of qubits EYZ in the state $\left|\Psi\right\rangle_{EYZ} = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle_{EYZ} + \left|111\right\rangle_{EYZ}\right)$. The whole system can be written

$$\begin{aligned}\left|\Omega\right\rangle &= \left|\Psi\right\rangle_{ABC} \otimes \left|\Psi\right\rangle_{EYZ} \\ &= \frac{1}{2}\Big[\frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)_{BCE}\frac{1}{\sqrt{2}}\left(\left|000\right\rangle - \left|111\right\rangle\right)_{AYZ} \\ &\quad + \frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)_{BCE}\frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)_{AYZ} \\ &\quad + \frac{1}{\sqrt{2}}\left(\left|001\right\rangle - \left|110\right\rangle\right)_{BCE}\frac{1}{\sqrt{2}}\left(-\left|011\right\rangle + \left|100\right\rangle\right)_{AYZ} \\ &\quad + \frac{1}{\sqrt{2}}\left(\left|001\right\rangle + \left|110\right\rangle\right)_{BCE}\frac{1}{\sqrt{2}}\left(-\left|011\right\rangle - \left|100\right\rangle\right)_{AYZ}\Big]. \end{aligned} \tag{3}$$

We can obtain the possible post-measurement states of particles $\frac{1}{\sqrt{2}}\left(\left|000\right\rangle - \left|111\right\rangle\right)_{AYZ}$, $\frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)_{AYZ}$, $\frac{1}{\sqrt{2}}\left(-\left|011\right\rangle + \left|100\right\rangle\right)_{AYZ}$, and $\frac{1}{\sqrt{2}}\left(-\left|011\right\rangle - \left|100\right\rangle\right)_{AYZ}$, depending on Eve's possible measurement outcomes $\frac{1}{\sqrt{2}}\left(\left|000\right\rangle - \left|111\right\rangle\right)_{BCE}$, $\frac{1}{\sqrt{2}}\left(\left|000\right\rangle + \left|111\right\rangle\right)_{BCE}$, $\frac{1}{\sqrt{2}}\left(\left|001\right\rangle - \left|110\right\rangle\right)_{BCE}$, and $\frac{1}{\sqrt{2}}\left(\left|001\right\rangle + \left|110\right\rangle\right)_{BCE}$, respectively. Then Eve transmits the particles to AP and AS. STA, AP, AS proceed as usual, since they do not know that Eve intercept and resent their particles. Therefore a part of messages might be leaked to Eve. However, by testing quantum channel, STA, AP, AS

perform measurements on oneself's particle using the base $\{|0\rangle, |1\rangle\}$ independently, the results will be random without any correlation. If the case has occurred, STA, AP, AS assert that eavesdropper exists and the information should be discarded.

(ii) AS provides only one-way authentication and STA always believes that AS is not faked. Without physical boundaries, data will be present quite literally "in the air" readily available to anybody with the appropriate receiver equipment. Faked AS is not without possible due to the wireless environment and the flaws of 802.11i protocol. Eve passively listens for frames and analyzing dataand fakes AS. It keep normal communication in STA and faked AP. WLAN has the potential to be a side door into the network that is not protected by appropriate AS. When STA and AS may afford a route into the network that bypasses the perimeter security that is in place. So, it is an enormous security threats to WLAN. But, the new security WLAN protocol is improved with which STA, AP and AS share key GHZ, where faked AS without quantum key can not access the data. It solve the problem of faked AS. Like a broad-spectrum antibiotic, quantum key authentication can serve the goal of confidentiality.

(iii) There are two major types of denial of service against 802.11 networks. At the radio layer, noise can severely disrupt communications. Any source of radio noise in the 802.11 frequency bands has the potential to interrupt communications. Attackers may use noise that is known to completely disrupt communications to prevent any data from flowing. However, the attack does not work without quantum key authorization. Once association has established the virtual network "port" on the STA , AP and AS, a new security WLAN protocol based on GHZ stats can be applied. Authorized users can be connected to resources they are allowed to use, and unauthorized users will be kicked off the network.

5 Conclusions

We proposed a new security WLAN protocol, which uses quantum GHZ stats to ensure wireless information security. The idea is to use quantum properties in order to permit the realization of new ways of communication. It is not only adapts to the existing network protocols but also provides a higher level security for WLAN. At the point, four major physical components can be transited the classical information and quantum information, and quantized paired key hierarchy has been improved from the original key structural in the four-way handshake. Eve invariably introduces errors within communication network if it wants to gain useful information. However, it will result in more complex configurations to support two classical information and quantum information in parallel and the method of secure communication in noisy environment come true in the near future. Future work related to this study may also pay attentions to the investigations of developing simplified instrument for generating GHZ states due to that the existing approaches are too complicated, and the investigations of error-correction methods and algorithms for correcting the error information resulted from the noisy quantum environment to ensure a better quality of quantum communication.

Acknowledgments This research was supported by Science and Technology Program of High Education of Shandong, China (Grant No. J11LG07), Qingdao Science and Technology Program—Fundamental Research, China (Grant No. 12-1-4-4-(6)-JCH), National Natural Science Foundation of China (Grant Nos. 61173056, 11304174).

References

1. Chi, K.-H., Shih, Y.-C., Liu, H.-H., Wang, J.-T., Tsao, S.-L., & Tseng, C.-C. (2011). Fast handoff in secure IEEE 802.11s Mmsh networks. *IEEE Transactions on Vehicular Technology*, *60*(1), 219–232.
2. Aizan, N. H. K., Zukarnain, Z. A., & Zainuddin, H. (2010). Implementation of BB84 protocol on 802.11i. In *2010 Second international conference on network applications protocols and services (NETAPPS)*, pp. 130–134.
3. Nguyen, T. M. T., Sfaxi, M. A., & Ghernaouti-Heliie, S. (2006). 802.11i encryption key distribution using quantum cryptography. *Journal of Networks*, *1*(5), 9–20.
4. Wijesekera, S., Huang, X., & Sharma, D. (2009). *Multi-agent based approach for quantum key distribution in WiFi networks. Agent and multi-agent systems, technologies and applications*. Berlin: Springer.
5. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. In *Proceeedings of the IEEE international conference on computers, system and signal processing*, pp. 175–179.
6. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*, 661–663.
7. Bostrom, K., & Felbinger, T. (2002). Deterministic secure direct communication using entanglement. *Physical Review Letters*, *89*(18), 187902.
8. Deng, F.-G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. *Physical Review A*, *69*, 052319.
9. Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S., & Long, G. L. (2005). Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, *71*, 044305.
10. Zhang, Z., Li, Y., & Man, Z. (2005). Multiparty quantum secret sharing. *Physical Review A*, *71*, 044301.
11. Ma, H., Chen, B., Guo, Z., & Li, H. (2008). Development of quantum network based on multiparty quantum secret sharing. *Canadian Journal of Physics*, *86*(9), 1097–1101.
12. Hillery, M., Buvek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Physical Review A*, *59*, 1829–1834.

Hongyang Ma was born in China in 1976. He received the B.S. degree in electronics technology application from Qufu Normal University, Shandong, China, in 1994 and the M.S. and Ph.D. degrees in computer science and technology from the Ocean University of China, Qingdao, China. He is currently an associate Professor with School of Sciences, Qingdao technological university. His main research interests are quantum network, wireless network, information security theory, and so on.

Shumei Wang was born in China in 1975. She received the B.S. degree from Qufu Normal University, Shandong, China, in 1994 and the M.S. degrees in computer science and technology from the Qingdao technological university, Qingdao, China. She is currently an associate Professor with School of Sciences, Qingdao technological university. His main research interests are wireless network, security theory, and so on.