Acta Technica 62 No. 2B/2017, 63–72 © 2017 Institute of Thermomechanics CAS, v.v.i.

Security of robot wireless network remote control system

Yu Lin[1], Ding Mi[1]

Abstract. The purpose is to study the security of wireless remote-control system of robot. A new EAP-TLS Plus protocol is proposed. At the same time, the robot remote control system is simulated by using the advantages of the absolute safety of quantum technology. The security performance is analyzed and studied respectively. In the case of improving the security performance of user access authentication, the simulation and analysis of the robot remote control system based on EAP-TLS Plus protocol are carried out. A quantum secure direct communication scheme and a quantum signature scheme based on four - particle cluster state are proposed. The simulation and performance analysis are carried out. At last, the idea of applying quantum technology to robot remote control system is put forward, and theoretical analysis and research are carried out. The results show that the security performance of the new protocol is enhanced, but the time complexity (authentication delay) is also increased. Therefore, it can be concluded that the improvement is only a temporary solution. Only by physically changing its security performance can this security problem be better resolved.

Key words. Wireless local area network, robot, information security, quantum communication, remote control.

1. Introduction

Human society has entered the era of information. With the rapid development and popularization of computer information technology, people depend too much on the information life. People's awareness of the protection of information has gradually risen from the embryonic stage to a more conscious stage. All kinds of communication means are inseparable from our daily life [1]. It has become the basic requirement to ensure communication fluency and communication security. Wireless local area networks (LAN) has good mobility and low operating cost. It can also organize the network flexibly, and management is very convenient. This makes up for the lack of wired networks [2]. At present, wireless LAN has been widely used in manufacturing, robotics and other fields. With the continuous improvement of the wireless LAN transmission rate, the application of the wireless LAN in the robot

[1] Zhengzhou Shuqing Medical College, ZhengZhou Henan, 450064, China

industry is increasing. Many robots work in dangerous and harsh environments, which can greatly affect the efficiency and personal safety of the operator. Therefore, the control of robots, from traditional field control and wired network control to wireless network control, has become an urgent need for the development of robots [3].

However, the security performance of the wireless local area networks is not as stable as that of wired network. At present, the most widely used wireless LAN is the 802.11 standard. Although 802.1x makes up for some of the 802.11 standard defects, there are still some shortcomings. The reason is that the protocol lacks two-way authentication between the client and the authenticator, and lacks the encryption protection of the authentication message. Illegal users can use these defects to achieve a variety of attacks [4]. There are three main types of attacks: the first is a fake attacker attack, the second is the session hijacking attack, and the third is to refuse service attacks. These security flaws have become the bottleneck of restricting the development of robot remote control technology based on wireless network to a certain extent. Figure 1 is a schematic diagram of the IEEE802.1x protocol architecture. Figure 2 is the IEEE802.1x authentication protocol process.

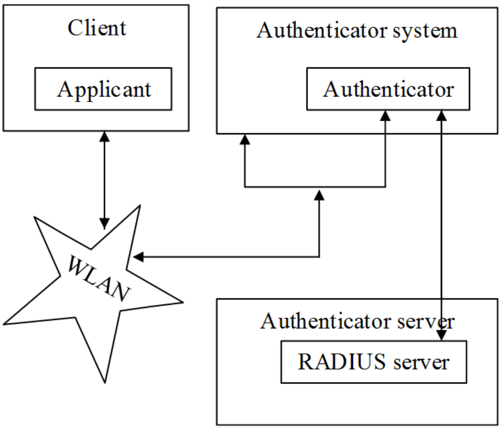

Fig. 1. 802.1x structure diagram

The security performance of robot remote control technology based on wireless network should be improved. Wireless LAN not only can play a greater role in robot development, research and application, but also can make wireless remote-control technology more secure and practical. This is conducive to the further development of robot remote control technology and the popularity of robots in various fields. At the same time, it will also help promote the industrialization of robots, especially industrial robots in our country. Therefore, it is an important task to realize secure information transmission in the wireless remote control of robot. However, so far, no attention has been paid to the security of the robot remote control system in wireless networks.

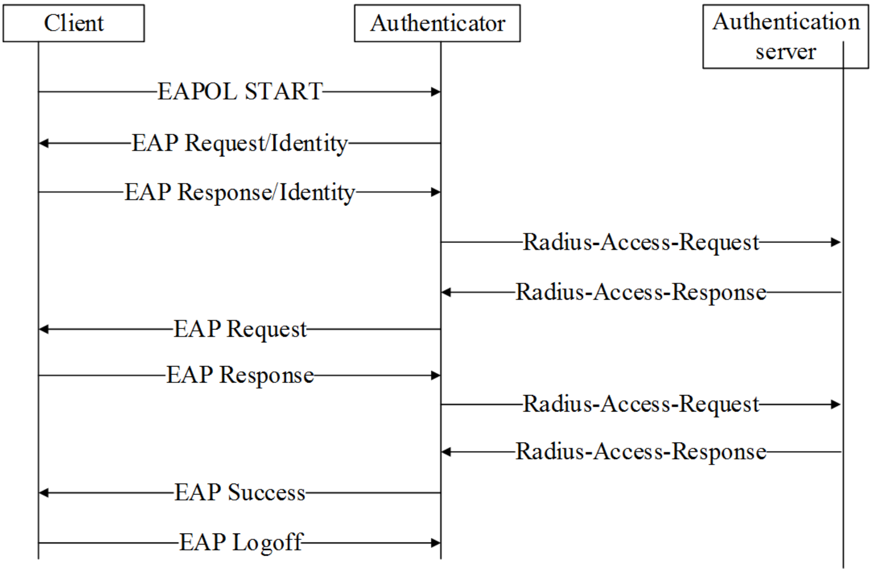

Fig. 2. IEEE802.1x authentication protocol process

2. State of the art

2.1. Research status of wireless network security

At present, both at home and abroad have put forward the wireless LAN security standards. However, they have some security flaws [5]. In 2004, in view of the DCF mechanism in the MAC layer of IEEE802.11 protocol, Ji Xiaomei conducted an analysis and improvement. The improved solution achieves better channel utilization efficiency and more stable performance through two "virtual competition" phases. In 2005, Feng Liuping and Liu Xiangnan analyzed the vulnerability of IEEE802.11 authentication protocol and denial of service attack. In 2006, based on the framework of 802.1x protocol and EAP protocol, Zhao Lin proposed a password based authentication enhancement scheme. The scheme can meet the security requirements of WLAN authentication to a certain extent, and it effectively enhances the authentication mechanism of 802.11i. In 2010, in order to enhance the security of IEEE802.1x protocol, Du Hui and Zhu Zhixiang proposed a new scheme, that is, EAP-DH. Through verification of the identity of the authenticator, the scheme can effectively prevent the impersonation of the IEEE802.1x protocol from attack, so that the security performance of the protocol has been improved. In 2011, Zhou Chao pointed out the root of the 802.1x protocol being vulnerable to attack. Protocol state machines are unequal and incomplete. It lacks protection for message integrity and source authenticity [6]. Then, an improved scheme of bidirectional challenge handshake and offline verification is proposed and implemented.

Quantum cryptography, based on quantum mechanics, is different from classical cryptography. It is the full use of physical characteristics. The quantum cryptography can develop an absolutely secure cryptosystem. Because if there is external eavesdropping, it will disturb the original state of the quantum system. Theoretically, the quantum states of quantum channels in quantum cryptography are not allowed to be measured by illegal users, because illegal measurements are bound to disturb both sides of the communication. In terms of methods, quantum cryptography is not used to transmit secret messages, but rather to transfer and distribute encryption keys (or create a password manual). In practice, quantum cryptography can guarantee the absolute security of communication. However, there are still some shortcomings. The quantum system itself is susceptible to interference from the communication environment, resulting in a higher communication error rate. It will affect the communication quality [7].

Compared with foreign countries, China's achievements in quantum cryptography is more significant. China University of Science and Technology achieved a key distribution of 150 km. Through the use of communication fiber optic cable, the long distance QKD was completed in Beijing, Xianghe and Tianjin. After long time monitoring, the bit error rate has been stable below 6 %. At the same time, USTC (University of Science and Technology of China) has successfully developed a prototype of quantum telephone. Through the commercial optical fiber network, a quantum communication network has been set up in Hefei, and a free quantum telephone network has been set up. The network's coverage is 1000 square kilometers, and it has successfully implemented a call encrypted quantum phone. This achievement not only demonstrates the absolute security of quantum communication, but also shows that quantum communication technology can be realized completely. At the 2011 Nobel prize winner forum in Beijing, Professor Pan Jianwei announced that China plans to launch a quantum communications satellite in 2016. Quantum information technology ensures that our calls are not bugged, and quantum unique parallel computing capabilities make quantum computing extremely fast.

2.2. Research status of robot remote control

With the continuous research and exploration of human nature, more and more complex and dangerous working environment is involved in the field of space, ocean and so on. In this context, people began to study the robot remote control technology in the 60s of last century [8]. The robot remote control system (RRCS) can provide basic functions, such as remote operation, data transmission, remote monitoring, network conversation and abnormal feedback. With the continuous development of science and technology, especially the maturity of computer information and communication technology, robot remote control system has become more rapid, convenient and intelligent [9]. The robot remote control system is designed according to the specific task and the actual working environment. As shown in Figure 3, it describes a simple framework for the hardware of a robot remote control system. A robot remote control system usually performs point to point remote control by the control device and the execution device. Furthermore, it can be further designed as remote control of multi-control equipment by multi-control equipment. The robot remote control system is mainly composed of control equipment, execution equipment, wireless communication module and sensor. The hardware frame diagram of the robot remote control system is shown in Fig. 3.

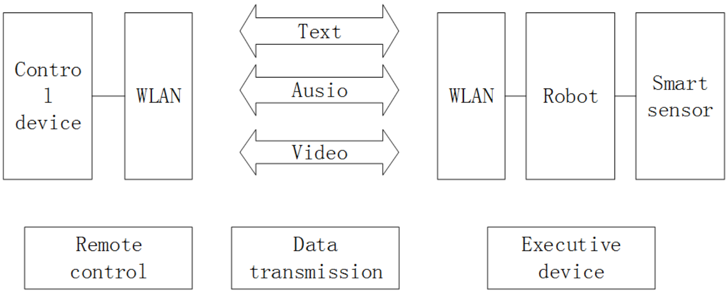

Fig. 3. Robot remote control system hardware frame diagram

When the robot remote control system is working, the staff login to the remote-control client at the control device end, and realize the remote control of the device (robot) in the human-computer interaction interface [10]. The control device communicates with the execution device through the wireless local area network. As shown in Fig. 4, it can be seen that on the basis of wireless LAN communication, this paper is mainly responsible for the authentication of client (control device) and server (execution device). It can ensure the safe communication between the control device and the executing device, and verify the origin, authenticity and integrity of the transmitted data. Further, it guarantees that the remote execution equipment is not damaged, the remote operation is free from interference, and the surrounding operating environment is not polluted and destroyed [11]. The connection and control of the robot can be realized by installing the client at the end of the control device. After the connection is successful, the man-machine conversation can be carried out. The software frame diagram of the robot remote control system is shown in Fig. 4.

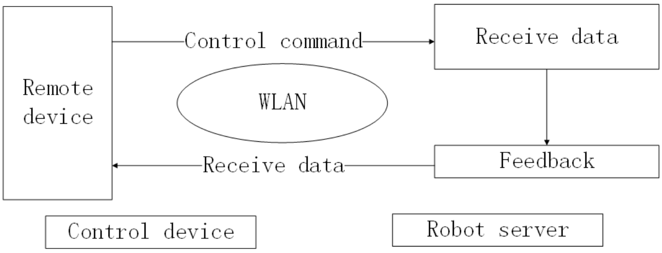

Fig. 4. Robot remote control system software frame diagram

To sum up, the robot remote control technology is an important part of robot technology. The wireless communication technology is used in the robot remote control system, which can not only realize the remote control of the robot, but also make the robot interact with other intelligent software and intelligent sensor. It will make robots more intelligent. The remote control of robot plays an important role in deep-sea exploration, space exploration and dangerous environment operation. At present, the research of robot remote control technology is not mature enough. The security risks of user access control are not noticed. The security defects of wireless networks restrict the development of remote control technology to a certain extent. In the final analysis, its physical limitations limit the security performance of communication technology. Only through breaking through this physical limitation can we fundamentally solve the security problems of access control. Although quantum communication is a new subject, it has shown its strong security advantages. Quantum cryptography can ensure unconditionally secure communications. Therefore, a new EAP-TLS Plus protocol is proposed in this paper. At the same time, the remote control system of robot is simulated by using the advantages of the absolute safety of quantum technology, and the security performance of the robot is analyzed and studied respectively.

The following aspects are mainly studied. The basic knowledge and existing problems of IEEE802.1x protocol and EAP protocol are introduced. The authentication process and authentication method of IEEE802.1x protocol and EAP protocol are analyzed, and several security defects of IEEE802.1x/EAP authentication protocol and the specific reasons for these defects are deeply studied. The EAP-TLS Plus protocol is proposed, and the robot remote control technology is used to analyze it. First of all, the IEEE802.1x / EAP authentication protocol security flaws were studied. A kind of targeted improvement protocol is proposed and its safety performance is simulated and analyzed. Then, the robot remote control was introduced. In the case of improving the security performance of user access authentication, the simulation and analysis of the robot remote control system based on EAP-TLS Plus protocol are carried out. A quantum secure direct communication scheme and a quantum signature scheme are proposed. According to the strong correlation degree and large entanglement of four particle cluster states, a quantum secure direct communication scheme based on four particle cluster states and a quantum signature scheme are proposed. The simulation and performance analysis are also carried out. Then, the idea of applying quantum technology to robot remote control system is put forward, and theoretical analysis and research are carried out.

3. Methodology

3.1. Research on RRCS based on EAP-TLS Plus

EAP-TLS protocol is vulnerable to session hijacking. From the three points of view, the shared secret instruction, the shared encryption and decryption key and the increase of the authentication between the client and the authenticator, the EAP-TLS protocol is improved. A more secure EAP-TLS Plus authentication protocol is proposed. The pre-shared secret instruction completes the authentication of the client identity at the first time, and the legal user refuses directly. If an illegal user initiates an authentication request, when the authentication server's Challenge is queried, the illegal user needs to submit a hash value Xi in the confidential instruction information shared by the client and the authentication server in advance. The possibility of an incorrect user submission is clearly very low. This not only saves the computing resources and storage resources for the authentication server, but also effectively avoids malicious denial of service attacks. Therefore, it effectively protects the key information frames transmitted during the authentication process. The improved EAP-TLS Plus authentication protocol is applied to RRCS. The security performance of the new authentication protocol is analyzed by simulation and compared with the EAP-TLS protocol.

3.2. Research of RRCS based on quantum technology

Traditional cryptography systems are based on mathematical calculations, whereas quantum cryptography is based on quantum mechanics. Quantum cryptography is an absolute security cryptosystem based on quantum attributes. The Heisenberg uncertainty principle shows that if a quantum state is measured, it must cause some degree of interference to the original quantum state. The measured quantum states will be different from those of the original state. Similarly, if a quantum system is measured, the resulting measurements cannot include complete information about the original system. According to the uncertainty principle, it can be known that both sides of the communication can detect the eavesdropper at the first time. Because the eavesdropper does not measure the quantum states on the quantum channel, it cannot guarantee the undisturbed state. Once disturbed, the measurement results of both sides of the communication will change, and then it will find the existence of eavesdroppers. At present, the safety of the principle of quantum state uncertainty has been proved. Therefore, even a computer with supercomputing power is of no avail. In addition, the quantum has the characteristics of non-cloning. In the case of communication under the conditions of channel security, the third party cannot steal any useful messages. The quantum technology is applied to robot remote control technology. According to the process of quantum secure direct communication protocol, the flow of simulation algorithm is designed. The protocol is simulated by Microsoft Visual 2010 platform, and the information security performance is analyzed and studied.

4. Result analysis and discussion

4.1. Analysis of EAP-TLS Plus and EAP-TLS comparison results

In the simulation of the robot remote control system, the IEEE802.1x / EAP-TLS Plus protocol is simulated by the security performance. On the basis of simulation and simulation, it is found that the security of classical information cannot fundamentally eliminate the attacker's attack. On the basis of the EAP-TLS Plus protocol, the security performance of the wireless remote control system based on the wireless network is greatly improved. However, in the final analysis, its safety performance is dependent on classical cryptography. In the simulation system based on IEEE802.1x / EAP-TLS Plus protocol, the user's authentication from the control device to the user's identity is successfully validated by the robot authentication server, which takes a longer time. In view of this, the simulation program based on IEEE802.1x/EAP-TLS protocol is also made in this paper, and several experiments have been carried out. Through experiments, it can be found that the EAP-TLS Plus protocol takes longer than the EAP-TLS protocol. According to the experimental results, it can be seen that the EAP-TLS Plus protocol has some shortcomings in the speed of authentication. As shown in Fig. 5, it is the result of the 50 times test contrast.

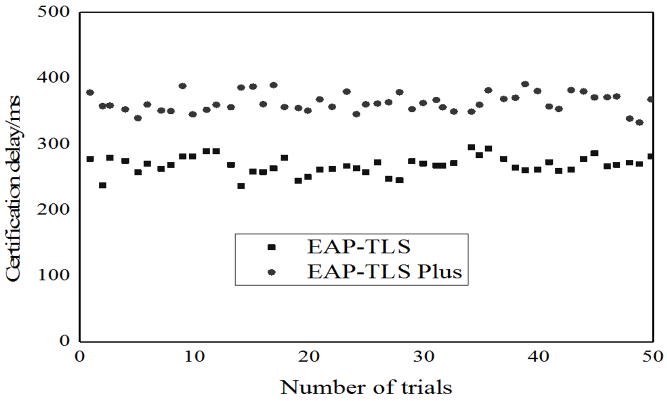

Fig. 5. Comparison of authentication delay between EAP-TLS Plus and EAP-TLS protocols

4.2. *Analysis of RRCS security simulation results based on quantum technology*

Through the previous analysis, in the ideal channel, the quantum communication for the non-coherent attack is safe. The communication efficiency has also been improved. Before formal access to coded communications, probe photons are introduced. It mainly carries on the second detection to the security of the quantum communication channel. The security and defense capability of the communication protocol is improved. In fact, the noise of the quantum channel influences the security of the communication scheme to a certain extent. This scheme has three advantages. First, the secret message is transmitted directly without the need to send a password. Second, the trial photon is inserted in the communication phase, so that the security performance of the communication is strengthened. With the cluster state as the information carrier, the entanglement is the largest, the correlation is the highest, and the communication efficiency is high.

Figure 6 is a statistical survey of the 20 test of channel safety before analog communication. It can be seen that before the communication, the protocol can always detect whether the channel is secure, which provides the security guarantee for the protocol. The dotted line in the picture is a security line, which indicates that the channel is unsafe. The security performance of the protocol can be proved directly from the experimental results. It also reflects the security of quantum communications.

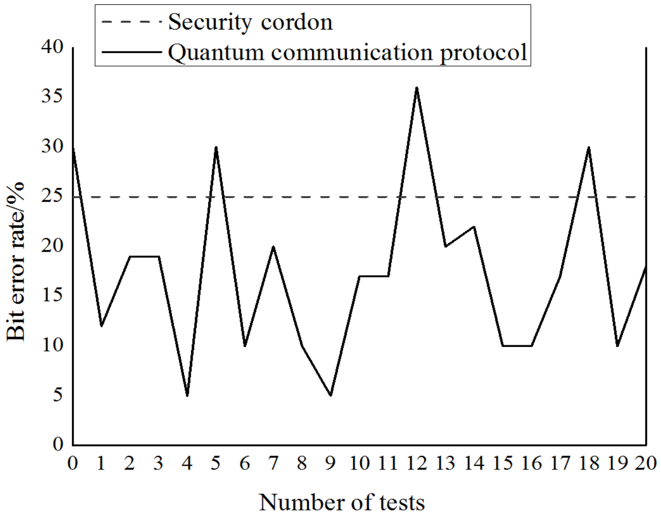

Fig. 6. Experimental results of secure detection for quantum communication channels

5. Conclusion

The security defects of IEEE802.1x / EAP authentication protocol are analyzed, and a modified protocol—EAP-TLS Plus is put forward. The EAP-TLS Plus protocol is combined with robot remote control technology. The control system is simulated, and the security performance of the access control is analyzed. Through simulation tests, the results show that the security performance of the new protocol is enhanced, but the time complexity (authentication delay) is also increased. Although the EAP-TLS Plus protocol has enhanced security performance, it can still be deciphered and attacked. Therefore, the improvement is only a temporary solution. Only by physically changing its security performance can this security problem be better resolved. The four particles cluster state is chosen as the information carrier. A quantum secure direct communication scheme and a quantum signature scheme based on four particle cluster states are proposed, and their performances are analyzed respectively. Then, based on the research of quantum technology, the security performance of the robot remote control system is analyzed and studied in detail. Finally, it comes to the conclusion that quantum technology is unconditionally secure. If human beings could design and produce quantum computers, our information would not be stolen by others. However, the quantum channel noise is still not resolved at the moment. The future research should try to improve the feasibility and reliability of quantum experiment.

References

[1] F. Peng, X. P. Fan: *Research on safety monitor system for coal mine based on EPA.* Advanced Materials Research *433–440* (2012), 6128–6133.

[2] H. Zhao, Z. Liu: *Design and implementation of wireless communication subsystem in WLAN-based rescue robot.* Proc. IEEE International Conference on Internet Technology and Applications, 20–22 August 2010, Wuhan, China, IEEE Conference Publications (2010), 1–4.

[3] J. W. Zhao, H. C. Li, G. Q. Chen, J. J. Huang, J. Dai: *Development of numerical control system for 3-PRS-XY series-parallel machine tool.* Proc. Mechanical Engineering and Control Systems, Publisher: WSPC, International Conference on Mechanical Engineering and Control System (MECS), 15–17 April 2016, Wuhan, China, 511–517.

[4] Z. Cai, X. Ren, G. Hao, B. Chen, Z. Xue: *Survey on wireless sensor and actor network.* Proc. IEEE World Congress on Intelligent Control and Automation (WCICA), 21–25 June 2011, Taipei, Taiwan, IEEE Conference Publications (2011), 788–793.

[5] R. Modugu, Y. B. Kim, M. Choi: *Design and performance measurement of efficient IDEA (International Data Encryption Algorithm) crypto-hardware using novel modular arithmetic components.* IEEE Instrumentation & Measurement Technology Conference Proceedings, 3–6 May 2010, Austin, TX, USA, IEEE Conference Publications (2010), 1222–1227.

[6] Q. Wang, S. Liu, Z. Wang: *A new internet architecture for robot remote control.* Proc. IEEE/RSJ International Conference on Intelligent Robots and Systems, 9–15 October 2006, Beijing, China, IEEE Conference Publications (2006), 4989–4993.

[7] G. P. Biswas: *Establishment of authenticated secret session keys using digital signature standard.* Information Security Journal: A Global Perspective *20* (2011), No. 1, 9–16.

[8] X. Qin, B. Jiang, X. Deng, X. Zu, Y. Du, H. Li: *A robot remote control system based on VPN and TCP/IP protocol.* Proc. IEEE International Conference on Mechatronics and Automation, 5–8 August 2008, Takamatsu, Japan, IEEE Conference Publications (2008), 285–289.

[9] X. Xing, E. Shakshuki, D. Benoit, T. Sheltami: *Security analysis and authentication improvement for IEEE 802.11i specification.* Proc. IEEE GLOBECOM 2008–2008 IEEE Global Telecommunications Conference, 30 November–4 December 2008, New Orleans, LO, USA, IEEE Conference Publications (2008), 1–5.

[10] X. Li, G. HE, M. Gu, P. Dai: *Quantum secure direct communication protocol based on four-qubit cluster state.* Proc. International Conference on Information Engineering and Applications (IEA), 26–28 October 2012, Chongqing, China, Springer, Lecture Notes in Electrical Engineering *219* (2013), No. 4, 105–112.

[11] M. Gutiérrez, L. Svec, A. Vargo, K. R. Brown: *Approximation of realistic errors by Clifford channels and Pauli measurements.* Physical Review A *87* (2013), No. 3, ID 030302-1–030302-5.

Received August 7, 2017