Towards a Key Consuming Detection in QKD-VoIP Systems

Guohong Zhao, Wanrong Yu, Baokang Zhao, Chunqing Wu

Towards a Key Consuming Detection in QKD-VoIP Systems

Guohong Zhao, Wanrong Yu, Baokang Zhao, Chunqing Wu

{ghzhao, wlyu, bkzhao, wuchunqing}@nudt.edu.cn
School of Computer Science, National University of Defense Technology, Changsha, Hunan, CHINA

Abstract. Quantum Key Distribution (QKD) technology, based on laws of quantum physics, can generate unconditional security keys between two communication parties. QKD is nearly a commercial technology and can make it available to the public. In existing QKD networks and commercial QKD systems, classical network is an essential part of the implementation of QKD protocols. With security keys and encryption scheme (one-time pad), we can protect the security of various network applications. But the public classical channel in QKD network may suffers potential key consuming attacks. In this paper, we focus on how to detecting the potential attacks during the security applications in the QKD network. Especially, we propose a Dynamic Key Consuming Detection scheme (DKode) in QKD-VoIP systems which encrypting VoIP streams with security keys from QKD systems.

Keywords: quantum key distribution; VoIP; detection; security

1 Introduction

Quantum Key Distribution (QKD) technology, based on laws of quantum physics, rather than the computational complexity of mathematical problems, can generate unconditional security keys between two communication parties [1]. QKD is nearly a commercial technology and can make it available to the public. The world's first QKD network was established by BBN company in 2004 [2]. In 2005, IDQuantique and MagiQ companies have launched second generation products of commercial QKD systems [3, 4]. The European project SECOQC demonstrated the world's first commercial QKD network for about 30 days in 2008 [5].The QKD network with security audio application was established by USTC in 2009 [6]. Nowadays, researchers have focused on improving the performance of QKD systems and integrating QKD technologies into practical security communication systems.

In existing QKD networks and commercial QKD systems, classical network is an essential part of the implementation of QKD protocols. QKD post-processing and security applications are both based on classical communication [7-8]. In the future, for large-scale QKD network, it will be integrated with the existing internet. The public classical channel in QKD network has potential security risks. With security

keys and security encryption schemes such as one-time pad, Eve can gain nothing about transmitted information. But eve can distinguish the communicating parties by eavesdropping and analyzing network flow data. By dropping or modifying encrypted data, eve may attend to reduce the performance of QKD network. As worst-case scenario, security keys of QKD network will be consumed totally and security messages can't be exchanged between two communication parties.

In this paper, we focus on how to detecting the potential attacks during the security applications in the QKD network. Especially, we propose a Dynamic Key Consuming Detection scheme (DKode) in QKD-VoIP systems which encrypting VoIP streams with security keys from QKD systems.

2 Security VoIP Application in QKD Network

2.1 The Framework of QKD-VoIP Systems

QKD network can be logically divided into two layers: quantum layer and classical layer, as it shown in Fig. 1. Quantum signals are transmitted in quantum layer. In classical layer, the communication parties (Alice and Bob) collect quantum information, and conduct post-processing procedures to generate unconditional security keys through security authenticated classical channel.

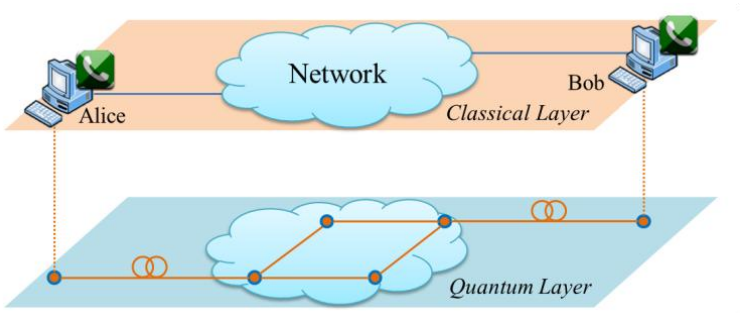

Fig. 1. The QKD network framework

VoIP is unquestionably the most popular real-time service in IP networks today. After Alice and Bob established a VoIP session, their audio stream will be encapsulated into RTP (Real-Time Transport Protocol) packets [9-10]. The framework of QKD-VoIP systems is shown in Fig. 2. During audio stream exchanging between Alice and Bob, QKD-VoIP systems gain the security keys from QKD engines, encrypt/decrypt RTP packets with these keys by one-time pad (OTP) method. Though eavesdropping and analyzing network flow data, eve can gain nothing about transmitted VoIP stream.

2.2 Vulnerability Analysis of QKD-VoIP Systems

Combining security keys generated by QKD network and OTP security encryption method, QKD-VoIP system can provide unconditional security network applications. Actually, the key generation rate of QKD network is limited. The state of art reported rate is about Mbps [11]. Thus, QKD network can supply only a few network applications. By dropping or modifying encrypted data, eve may attend to reduce the performance of QKD network. As worst-case scenario, security keys of QKD network will be consumed totally and security messages can't be exchanged between two communication parties. Thus, we must detect out the potential key consuming attacks rapidly.

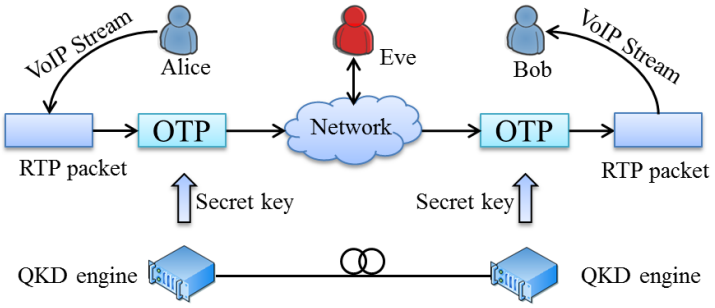

Fig. 2. The Framework of QKD-VoIP Systems

3 Dynamic Key Consuming Detection Scheme in QKD-VoIP Systems

In QKD-VoIP systems, eve can gain nothing by eavesdropping data packets. But eve can modify the transmitted data to consume the security keys generated by QKD systems. When the amount of security keys is not enough to encrypt the VoIP stream, Alice and Bob can't to exchange security messages any more. In this paper, we propose a Dynamic Key Consuming Detection scheme (DKode) in QKD-VoIP systems.

3.1 Detection Principles

In order to provide a numerical indication of perceived quality of received audio stream after transmission and compression, we introduce the Mean Opinion Score (MOS) model defined by ITU-T [12]. The MOS value is expressed from 1 to 5, as it shown in Tab. 1. Values dropping below 3.5 are termed unacceptable by many network users. In order to prevent the audio communication between Alice and Bob, the attacking actions must drop the MOS value of transmitted VoIP stream below 3.5 or even lower [13]. We can use PESQ algorithm which based on MOS model to estimate the stream quality quickly to detect out the potential attacks [14].

Table 1. The MOS Values

MOS	5	4	3	2	1
Quality	Perfect	Fair	Annoying	Very annoying	Impossible to communicate

3.2 The proposed DKode Scheme

By adjusting the detecting timer dynamically, our proposed Dkode scheme can estimate the link state effectively to find the potential key consuming attacks. Dkode includes the following five steps.

Step 1. Initialization. Set up the detecting timer of Dkode $T_{cur} = T_{init}$, the threshold of MOS value $M_t = M_{init}$. Measure the MOS value of initial voice quality M_{ptr}.

Step 2. Sampling and measuring the MOS value of VoIP stream per T_{cur}. If $M_{cur} \geq M_{ptr}$, go to Step 3. If $M_{cur} \leq M_t$, go to Step 4. Else, go to Step 5.

Step 3. If $2T_{cur} < T_{init}$, set $T_{cur} = 2T_{cur}$. If not, set $T_{cur} = T_{init}$. Go to Step 2.

Step 4. Sampling and measuring the MOS value of VoIP stream M_{cur} again immediately. If $M_{cur} \leq M_t$, the VoIP communication between Alice and Bob is suffering the key consuming attacks. Abort.

Step 5. $M_{cur} = M_{ptr}$, $T_{cur} = T_{cur} / 2$. Go to Step 2.

4 Acknowledgment

The work described in this paper is partially supported by the project of National Science Foundation of China under grant No. 61202488, 61272482; the National High Technology Research and Development Program of China (863 Program) No. 2011AA01A103, 2012AA01A506, 2013AA013505.

References

1. Liu, B., Zhao, B.K., Wei, Z.L., Wu, C.Q., Su, J.S., Yu, W.R., Wang, F., Sun, S.H.: Qphone: A Quantum Security VoIP Phone. ACM SIGCOMM Comp. Commun. Rev. 43, 477-478 (2013).
2. Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., Yeh, H.: Current status of the DARPA quantum network. In: Quantum Information and Computation III, March 29, 2005 - March 30, 2005, pp. 138-149.
3. IDQuantique, http://www.idquantique.com/network-encryption/products/network-encryption-overview.html, 2014.
4. MagiQ, http://www.magiqtech.com/Products.html, 2014.
5. Peev, M., Poppe, A., Maurhart, O., Lorunser, T., Langer, T., Pacher, C.: The SECOQC quantum key distribution network in Vienna. In: 35th European Conference on Optical Communication, ECOC 2009.
6. Chen, T.-Y., Liang, H., Liu, Y., Cai, W.-Q., Ju, L., Liu, W.-Y., Jianwang, Yin, H., Chen, K., Chen, Z.-B., Peng, C.-Z., Pan, J.-W.: Field test of a practical secure

communication network with decoy-state quantum cryptography. Optics Express 17, 6540-6549 (2009).
7. Liu, B., Zhao, B., Zou, D., Wu, C., Yu, W., You, I.: A real-time privacy amplification scheme in quantum key distribution. Information and Communication Technology, pp. 453-458. Springer (2013).
8. Liu, B., Zhao, B., Liu, B., Wu, C.: A Security Real-time Privacy Amplification Scheme in QKD System. Journal Of Universal Computer Science 19, 2420-2436 (2013).
9. Xu, E., Liu, B., Xu, L., Wei, Z., Zhao, B., Su, J.: Adaptive VoIP steganography for information hiding within Network Audio Streams. In: 2011 International Conference on Network-Based Information Systems, NBiS 2011, September 7, 2011.
10. Wei, Z., Zhao, B., Liu, B., Su, J., Xu, L., Xu, E.: A novel steganography approach for voice over IP. J Ambient Intell Human Comput 1-10 (2013).
11. Tanaka, A., Fujiwara, M., Yoshino, K.-I., Takahashi, S., Nambu, Y., Tomita, A., Miki, S., Yamashita, T., Wang, Z., Sasaki, M., Tajima, A.: High-speed quantum key distribution system for 1-mbps real-time key generation. IEEE Journal of Quantum Electronics 48, 542-550 (2012).
12. Wu, Z., Yang, W.: G.711-Based adaptive speech information hiding approach. In: International Conference on Intelligent Computing, ICIC 2006, August 16, 2006 - August 19, 2006, pp. 1139-1144.
13. Mean Opinion Score (MOS) - A Measure Of Voice Quality, http://voip.about.com/od/voipbasics/a/MOS.htm, 2014.
14. Rix, A.W., Beerends, J.G., Hollier, M.P., Hekstra, A.P.: Perceptual evaluation of speech quality (PESQ)-a new method for speech quality assessment of telephone networks and codecs. In: Acoustics, Speech, and Signal Processing, 2001. pp. 749-752 vol.742.