Physics Letters A 382 (2018) 3253–3261

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

A denial-of-service attack on fiber-based continuous-variable quantum key distribution

Yuan Li [a], Peng Huang [a,*], Shiyu Wang [a], Tao Wang [a], Dengwen Li [a], Guihua Zeng [a,b,**]

[a] State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, China
[b] College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China

ARTICLE INFO

Article history:
Received 1 June 2018
Received in revised form 19 September 2018
Accepted 20 September 2018
Available online 25 September 2018
Communicated by M.G.A. Paris

Keywords:
Quantum key distribution
Continuous variable
Parameter estimation
Practical security

ABSTRACT

In a fiber-based continuous-variable quantum key distribution (CVQKD) system, to perform the channel estimation, the channel transmittance is usually assumed to be a constant. Subsequently, when the channel parameters are intentionally manipulated, the employed parameter estimation method will lead to deviations of channel parameters and ultimately impacting the evaluation of the secret key rate. In this paper, we propose a denial-of-service attack strategy based on Eve's manipulation of the channel parameters. In particular, we analyze in detail the impact of this attack when the channel transmittance is attacked and obeys two-point distribution and uniform distribution. The result shows that in both cases, Eve's slight manipulation on the quantum channel will lead to large underestimation of the secure transmission distance by using the previous parameter estimation, which will lead to intentional terminations of the communication. To prevent this attack, a simple data post-selection should be added before parameter estimation.

1. Introduction

Quantum key distribution (QKD) has developed immensely over the past decade [1–3] and is certainly one of the most advanced applications of the quantum technology. It allows two distant partners share secure secret keys through an untrusted quantum channel controlled by an eavesdropper Eve [4], and its unconditional security is guaranteed by the basic laws of the quantum mechanics. In contrast to discrete-variable quantum key distribution (DVQKD) [5], the continuous-variable quantum key distribution (CVQKD) [6–10] encode information on the two quadratures of the weak coherent states [11,12]. And it is easy to implement and compatible with the existing networks. In theory, the continuous-variable quantum key distribution has been proved secure against arbitrary collective attacks, and the Gaussian-modulated coherent-state (GMCS) CVQKD protocol has been fully proven against arbitrary attacks [13–16].

However, in actual implementation, the imperfection of key devices and algorithms in CVQKD system can lead to serious loopholes that can be attacked by eavesdropper Eve. A lot of related research work [17–25] has been done on practical security issues introduced by imperfect system hardware, e.g., the wavelength attack, the calibration attack, and the LO fluctuation attack. But few studies have been done on the practical security analysis of the software algorithms. Currently, only the reconciliation [26] has been considered.

Actually, as a key step in CVQKD, parameter estimation which helps us to evaluate the security of the communication and obtain parameters for further post-processing procedure, can also be attacked by Eve. In the practical implementation of the fiber-based CVQKD system, the parameter estimation method usually assume that the channel transmittance is a constant. However, in actual implementation, this assumption is difficult to satisfy. Therefore, the impact of this parameter estimation method in practical systems needs further investigation.

In this paper, we analyze the problems that may be caused by the existing parameter estimation method in the fluctuated channel. And we find that although the traditional parameter estimation method can guarantee the security of the system, it introduces a large estimated deviation when the channel transmittance fluctuates. This estimated deviation causes the estimated channel transmittance to be lower than the true value, while the channel excess

* Corresponding author.
** Corresponding author at: State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, China.
E-mail addresses: huang.peng@sjtu.edu.cn (P. Huang), ghzeng@sjtu.edu.cn (G. Zeng).

https://doi.org/10.1016/j.physleta.2018.09.027
0375-9601/

noise to be higher than the true value. As a result, the secure secret key rate will be underestimated, and the secure transmission distance will be drastically reduced. And the communication that was originally considered secure will then become insecure.

Furthermore, we propose a kind of denial-of-service attack aimed at the vulnerability of the parameter estimation algorithm in a fiber-based CVQKD system. Under this attack Eve manipulates the channel and slightly changes the channel transmittance, resulting in large errors in parameter evaluation, and thus lead to the interruption of the communication. This attack is relatively covert and not easy to be detected by both parties. And it gives us a direction of the attempt to troubleshoot the problem when the system is interrupted for no reason. In performance, this attack is similar to the blinding attack in DVQKD or the denial-of-service attack in classical communication. They can all lead to communication interruptions and make the legitimate parties unable to communicate during Eve's attack.

Finally, a simple countermeasure based on post-selection is proposed to defend against this attack at the end of the paper. Also, it provides us a reference for developing more perfect parameter estimation algorithms.

The paper is organized as follows. In Section 1, we briefly review the parameter estimation method of the GMCS CVQKD protocol. In Section 2, we propose a denial-of-service attack strategy on fiber based CVQKD protocols. Then the impact of this attack on GMCS CVQKD systems is analyzed in Section 3. And last, we conclude the paper.

2. Parameter estimation methods of the GMCS CVQKD protocol

In the GMCS CVQKD protocol, Alice modulates the Gaussian random numbers on his quantum signal and sends it to Bob through the quantum channel [27,28]. The quantum channel is assumed to be controlled by Eve and is characterized by transmission efficiency T and excess noise ε. After receiving the state, Bob takes homodyne detection and informs Alice which observable he obtained. And then, Alice and Bob will share two correlated Gaussian variables which can be further used to estimate the channel parameters and extract the shared secret keys.

In this scenario, in order to evaluate the security of the communication and obtain parameters for further post-processing procedure, we need to know the detailed channel and device parameters, the channel transmittance T, the channel excess noise ε, the detector efficiency η, the electrical noise V_{el}, and the shot noisy N_0.

Usually, during the parameter estimation process, some parameters are measured in advance and others must be evaluated in real time. The detector efficiency η and the electrical noise V_{el} are determined by the Homodyne detector in Bob's end, and their changes in repeated experiments are relatively stable. In general, we measure them before our communication. The shot noise can be expressed as follows

$$N_0 = K_{N_0} E_{LO}, \tag{1}$$

where K_{N_0} is a parameter that needs to be calibrated in advance, and E_{LO} is the power of the local oscillator. We can find that the shot noise is positively related to the intensity of our local oscillator and we can use the intensity of the local oscillator to calibrate it in communication. Also, Eve's attack on shot noise estimation may also cause serious security problems, but we will not discuss it in this paper.

In this article, we mainly focus on the estimation of the channel transmittance T and channel excess noise ε, also analyze the estimation deviations that may be caused by the attacker Eve. And for simplicity, we study the parameters estimation procedure for

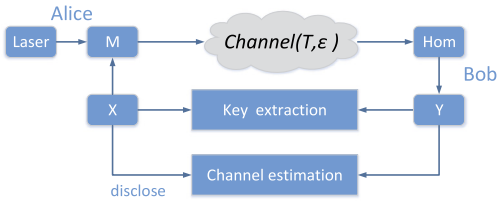

Fig. 1. In a GMCS CVQKD protocol, Alice encode Gaussian random numbers on the coherent state, and then send it to Bob through the quantum channel, which is controlled by the Eavesdropper Eve. In Bob's end, a homodyne detector is used to acquire the transmitted information. And then, before they extract keys from the shared Gaussian variables, they disclose part of the variables and use them to evaluate the channel parameters.

GMCS CVQKD protocols, without postselection. Under normal conditions, the transmittance in optical fiber is relatively stable. In a fiber based CVQKD protocol, we always use statistical methods to estimate its channel parameters. As shown above in Fig. 1, blocks of shared Gaussian variables should be disclosed and used to estimate the channel transmittance and the channel excess noise, and the other is used for key extraction.

In the previous parameter estimation method, Alice and Bob's data are linked through the following relation

$$y = tx + z, \tag{2}$$

which is a normal linear model parametrized by $t = \sqrt{T} \in \mathbb{R}$ and z follows a centered normal distribution with unknown variance $\sigma^2 = 1 + T\varepsilon$. According to the above equation and using the maximum likelihood estimation method, we can get the estimated value of the channel transmittance and channel excess noise as follows

$$\begin{aligned} \hat{t} &= \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2} \\ \hat{\sigma}^2 &= \frac{1}{m}\sum_{i=1}^{m}(y_i - \hat{t}x_i)^2, \end{aligned} \tag{3}$$

where $\hat{t}$ is the estimated value of parameter $\sqrt{T}$, and $\hat{\sigma}^2$ is the estimated value of $1 + T\varepsilon$.

Moreover, the two estimators $\hat{t}$ and $\hat{\sigma}^2$ obey the normal distribution and chi-square distribution respectively

$$\begin{aligned} &\hat{t} \sim \mathcal{N}(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_i^2}) \\ &\frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \end{aligned} \tag{4}$$

where t and σ^2 are the true value of the parameter $\sqrt{T}$ and $1+T\varepsilon$ respectively.

Using Eq. (3), we can fully estimate the value of the channel transmittance T and channel excess noise ε, without considering the finite-size effect of the estimated data blocks. However, the finite-size effect in practical implementations is inevitable, which will add excess statistical noise to our estimate. The variance of this statistical noise is related to the length of our estimated data blocks. And in [15], the bias caused by the finite-size effect on parameter estimation is fully demonstrated. The range of the estimates can be expressed as follows