Decoy-State Quantum Key Distribution Using Homodyne detection
S. H. Shams Mousavi\textsuperscript{1}, and P. Gallion\textsuperscript{2}

\textsuperscript{1}. Ecole Supérieure d'Électricité (Supélec), Photonics and Communication Systems, 2 rue Edouard Belin, 57070 Metz, France
\textsuperscript{2}. TELECOM ParisTech, Ecole Nationale Supérieure des Télécommunications, CNRS LTCI UMR 5141, 46 rue Barrault, 75013 Paris, France
email: hamed.mousavi@supelec.fr

Summary
Photon number splitting (PNS) is a powerful attack against the quantum key distribution (QKD) systems. This attack significantly limits the secure transmission range of the QKD systems. In this article, we show how we can improve the transmission range of the QKD systems based on balanced homodyne detection (BHD) using the decoy-state technique.

Introduction

In theory, a secure QKD system should use only single photon states for the transmission of the key bits [1]. However, since the single photon sources are still out of reach, most practical QKD systems use the coherent laser sources which produce weak coherent pulses (WCP) with the Poissonian distribution on the number of photons. The non-single photon pulses that come out of a coherent source are vulnerable against the PNS attack.

In a strong version of the PNS attack, the eavesdropper (Eve) blocks all the single photon pulses and steals one or several photons from each pulse carrying multiple photons. Clearly, this attack changes the quantum bit error rate (QBER) of the signal as well as the photon number distribution (PND) at the receiver’s side (Bob). We assume that Eve can compensate the decrease in QBER by changing the transmission medium with a superior channel and also adapts its strategy in order to maintain the PND.

It has been shown that the PNS attack is feasible whenever the channel length is above a limit which only depends on the average photon number per pulse ($\mu$) [2]. On the other hand, the secure transmission range of a practical QKD system is also limited by the attenuation of the channel ($\alpha$) and efficiency of the detector. This limit is particularly tight for the systems based on WCP’s and even more for the systems based on (BHD) [3].

The decoy state technique is proposed in order to improve the secure transmission range of the QKD system. The idea behind the decoy state technique is to use several coherent states randomly. These coherent states are indistinguishable by the eavesdropper and each one yields a different QBER. Then, at the end of the transmission, the used states for all bits will be publicly announced and by checking the different QBERs, the legitimate parties can detect the PNS attack [4].

Discussion

In general, the transmission rate of a QKD system can be written as $R = qp_D\eta_{pp}$, where $q = 0.5$ for standard BB84 protocol and $p_D = 1 - \exp(-\eta\mu)$ for the coherent light. $\mu$ is the average photon number and $\eta$ is the transparency of the channel; $\eta = 10^{-\alpha l}$. The third factor $\eta_{pp}$, the post processing efficiency, is the key factor. Most of these systems
use the photon counting for detection because of the low level of the receiving signal. We use however BHD [5].

![Graph](image1)

*Fig 1. R vs. channel length, l, for a) \( x = 0.9 \) b) \( x = 2 \)*

![Graph](image2)

*Fig 2. Minimum and maximum channel lengths, \( l_{\text{min}} \) and \( l_{\text{max}} \), for different values of threshold (x).*

Using the GLLP analysis of the performance of the QKD systems [3], we can write the performance of the system for the case that a single coherent is state used for the transmission of data as:

\[
\eta_{\text{pp}} = (1 - 2a)[-f(e)H(e) + (1 - \Delta)[1 - H(e)]]
\]

(1)

In this equation \( e \) and \( a \) are the bit error rate (BER) and the bit abandonment rate (BAR), respectively. For the BHD system with phase encoding, \( e = 0.5 \text{erfc}\sqrt{2\eta\mu(1 + x)} \) and \( a = 0.5 \text{erfc}\sqrt{2\eta\mu(1 - x)} - e \), where \( x \) is the detection threshold.

As we can see in fig. 1.a & 1.b, for the values of threshold less than one, we have a maximum channel length \( (l_{\text{max}}) \). Furthermore, for the larger values of threshold, we have a minimum \( (l_{\text{min}}) \) and a maximum \( (l_{\text{max}}) \) channel length between which we have an acceptable data rate. In Fig. 2, we have drawn \( l_{\text{min}} \) and \( l_{\text{max}} \) as a function of \( x \).

In conclusion, the value of \( x \) should be chosen according to the curves of \( l_{\text{min}} \) and \( l_{\text{max}} \), so that the actual channel length will lie between these two bounds and for any particular channel length, we can find an optimum value of \( x \) by simulation.

**References**


