Universidade de Aveiro
2017-2018

Real-time shot-noise measurement

Diamantino Silva
(diamantinosilva@ua.pt)

Department of Electronics, Telecommunications and Informatics,
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações, Aveiro, Portugal

Real-time quantum noise measurement

T. Wang, P. Huang, Y. Zhou, W. Liu, G. Zeng

Practical performance of real-time shot-noise measurement in continuous-variable quantum key distribution

Quantum Inf Processing **17.1**, 11 (2018)

RTSNM - the problem

For any QKD system, some statistics about the transmitted data are used to evaluate the amount of information that may be in possession of an attacker.

The estimation of the eavesdropper information depends on the **excess noise** which is the difference between the observed noise and the shot noise, and also on the **observed correlation** between the emitter and the receiver.

The historical method to estimate the shot noise is to calibrate once and for all the slope of the local oscillator to shot noise linear relation on the homodyne detection, and then to measure in real time the power of the local oscillator.

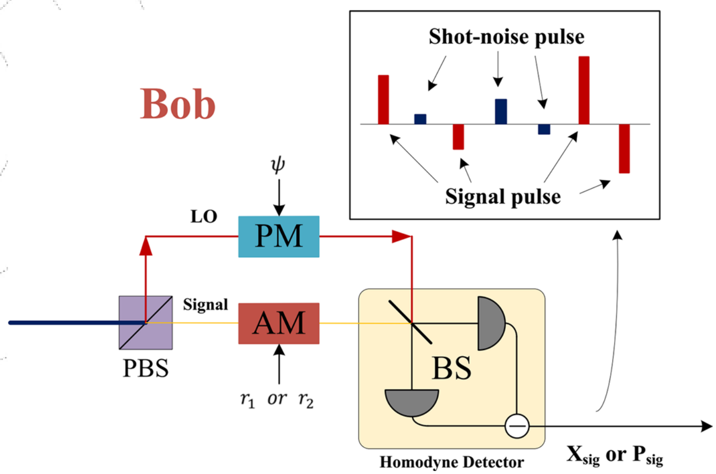
It was shown that this relationship is **prone to change over time**, especially under the influence of an attacker.

RTSNM - a solution

In order to defend practical attacks, real-time monitoring technologies are extensively adopted to prevent both attack and signal disturbance.

RTSNM is proposed as a "procedure for preventing the eavesdropper exploiting the practical security loopholes" of CVQKD, such as fluctuations of local oscillator intensity.

RTSNM - Implementation



??? ESTE TEXTO ESTA ESTUPIDO ???
This procedure adds a modification to the standard CVQKD protocol, which consists on a amplitude modulator (AM) introduced in Bob's signal path. This will allow to choose between two extintion ratios ($r_1 = 1$ or $r_2 = 0$), of the AM to measure the signal pulse or the shot-noise pulse.

RTSNM - Implementation

After a quantum transmission, Alice and Bob share two correlated vectors $P = \{(x_i, y_i)|i = 1, 2, \ldots N\}$, where N is the total number of received data when the extintion ratio was r_1. Meanwhile, Bob also acquires a single vector $Q = \{(y_{0i})|i = 1, 2, \ldots, N'\}$, where N' is the total number when the ratio ir r_2.

RTSNM - Channel model

The quantum channel of CVQKD is a normal linear model with the following relations between Alice and Bob

$$y = tx + z, \quad y_0 = z_0$$

in which $t = \sqrt{\eta T}$, z is the total noise term and z_0 is the partial noisel, both gaussian random variables.

η	efficiency of the homodyne detection
T	transmission of the quantum channel
N_0	variance of shot noise
ε	excess noise (in SN units)
V_{el}	detector's electronic noise

RTSNM - Channel Model

Variable	Mean	Variance
x	0	V_A
y	0	$\eta T V_A + \eta T \varepsilon N_0 + N_0 + V_{el}$
z	0	$\eta T \varepsilon N_0 + N_0 + V_{el}$
y_0	0	$N_0 + V_{el}$
z_0	0	$N_0 + V_{el}$

Variance term	Description
V_A	Variance of the parameters of the coherent state
N_0	Shot noise variance
V_{el}	Detector's electronic noise
$\eta T V_A$	V_A after the channel transmission and detection
$\eta T \varepsilon N_0$	"The noise in Bob's state in excess compared to the shot noise"?

RTSNM - Estimators

Parameteres that need to be estimated

Parameter	Description
T	transmission of the quantum channel
N_0	variance of shot noise
ε	excess noise (in SN units)

From the P vector, m pairs $(m < N)$ of correlated data are randomly selected to use in the parameter estimation. Bob uses $m' = N'$ data samples from the vector Q to perform the shot-noise estimation procedure.

Correlation of Alice and Bob values $\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2}$

Estimator of the variance of z $\hat{\sigma}^2 = \frac{1}{m} \sum_{i=1}^{m} (y_i - \hat{t} x_i)^2$

Estimator of the variance of z_0 $\hat{\sigma_0}^2 = \frac{1}{m'} \sum_{i=1}^{m'} (y_{0i})^2$

RTSNM - Estimators

The real values of the threes quantities should be in the interval

$$t \in \left[\hat{t} - \Delta t, \hat{t} + \Delta t\right],$$

$$\sigma^2 \in \left[\hat{\sigma}^2 - \Delta\sigma^2, \hat{\sigma}^2 + \Delta\sigma^2\right], \quad \sigma_0^2 \in \left[\hat{\sigma}_0{}^2 - \Delta\sigma_0^2, \hat{\sigma}_0{}^2 + \Delta\sigma_0^2\right]$$

The estimators should obtain the most pessimist estimation for the quantity of information obtained by an eavesdropper. We end up with the following estimatives

$$T_{min} = (\hat{t} - \Delta t)^2/\eta, \quad \varepsilon_{max} = \frac{\left(\hat{\sigma}^2 + \Delta\hat{\sigma}^2 - \hat{\sigma}_0{}^2\right)}{\hat{t}^2\left(\hat{\sigma}_0{}^2 - V_{el}\right)}$$

in which

$$\Delta t = z_{\varepsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}^2}{mV_A}}, \quad \Delta\sigma^2 = z_{\varepsilon_{PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \quad \Delta\sigma_0^2 = z_{\varepsilon_{PE}/2}\frac{\hat{\sigma}_0{}^2\sqrt{2}}{\sqrt{m'}}$$

RTSNM - Problems of the Solution

Small size effects
Given the size of the blocks (N) and the size of the analysed pulses for estimating the parameters, noise is introduced in the system.

Imperfect amplitude modulation
Because there are no perfect modulators,..

"In short, using this RTSNM scheme, although the pratical security and stability of the system are improved, we may sacrifice the transmission distance and the final key rate."

E-mail: diamantinosilva@ua.pt