Networks Based on QKD and Weakly Trusted Repeaters

David Elkouss, Jesus Martinez-Mateo, Alex Ciurana, Vicente Martin

I. Introduction

We study how to use quantum key distribution (QKD) in common optical network infrastructures and propose a method to overcome its distance limitations. QKD is the first technology offering information theoretic secret-key distribution that relies only on the fundamental principles of quantum physics. Point-to-point QKD devices have reached a mature industrial state; however, these devices are severely limited in distance, since signals at the quantum level (e.g. single photons) are highly affected by the losses in the communication channel and intermediate devices. To overcome this limitation, intermediate nodes (i.e. repeaters) are used. Both, quantum-regime and trusted, classical, repeaters have been proposed in the QKD literature, but only the latter can be implemented in practice. As a novelty, we propose here a new QKD network model based on the use of not fully trusted intermediate nodes, referred as *weakly trusted repeaters*. This approach forces the attacker to simultaneously break several paths to get access to the exchanged key, thus improving significantly the security of the network. We formalize the model using network codes and provide real scenarios that allow users to exchange secure keys over metropolitan optical networks using only passive components [1].

II. Weakly trusted repeaters

Network coding is a paradigm where the intermediate nodes, instead of simply forwarding the incoming flows through the outgoing paths (according to some routing algorithm), distribute a function of the inputs through each outgoing path.

We will consider every link in a QKD network to be a private link between its neighboring nodes. This restricts eavesdropping to the intermediate network nodes; only a curious router can gain access to network messages. This ability to extend the traditional security perimeter to also cover the communication channel between two QKD nodes is the consequence of the laws of quantum physics and is the key attribute of QKD. However, this property cannot be extended to classical repeaters. In essence, any classical repeater node in a chain of quantum links gets meaningful information [2]. In order to prevent the curious routers from accessing information, we can create extended source messages by adding randomness to the source messages. Formally, the messages are drawn from the direct product of the source alphabet $\mathcal{M}$, and a random key alphabet $\mathcal{K}$.

Let us consider a set of $|\mathcal{W}|$ independent eavesdroppers. Every $w \in \mathcal{W}$ may receive the messages traversing a fixed collection of nodes, or eavesdropping pattern B_w, in order to recover a subset of the source message M_w. In consequence an eavesdropper has access to $Y_{B_w} = \{Y_e : e \in \mathcal{A}(v), v \in B_w\}$, the messages traversing B_w. Note that the elements in $\mathcal{W}$, i.e. eavesdroppers, are elements of the power set of V and in consequence potentially overlapping. We say that the intermediate nodes in the network graph are weakly trusted repeaters (WTR) to reflect the assumption that no further cooperation with the eavesdroppers is performed.

Following [2], a network code is admissible over this *eavesdrop network* model if every user node u can recover M_u and the information that every eavesdropper w holds about M_w does not reduce its entropy:

$$H(M_w|Y_u) = 0$$

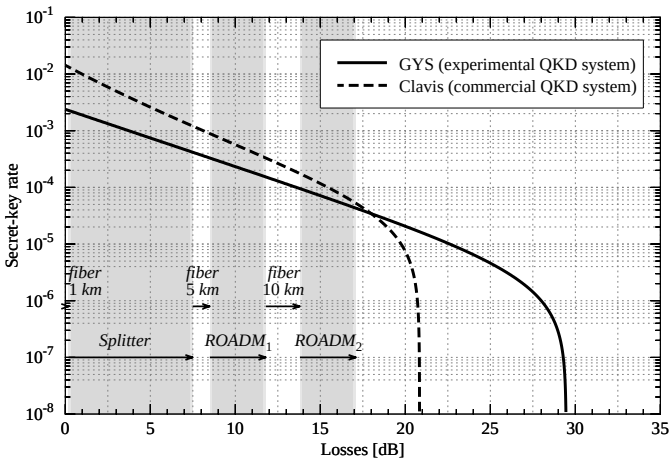

Fig. 1. Secret-key rate, in bits per qubit sent, of two different QKD systems, GYS and Clavis, using the BB84 protocol with decoy states as a function of the absorptions in the network. Losses due to network devices are depicted using a shadowed region.

and $\forall w \in \mathcal{W}$:

$$H(M_w|Y_{B_w}) = H(M_w)$$

These two conditions are called the secure and decodable conditions.

III. Network design

To secure a metropolitan optical network, a quantum channel has to be created among any two nodes of the access networks. Therefore, first we connect an emitter to the end of an access network. Losses, due to fiber and network components, do not allow to directly plug the receiver in a different access network (see Fig. 1). Intermediate nodes are needed. Possible locations are the immediate backbone node or its closest neighbors. If we follow this idea we obtain a bipartite graph with emitters placed at the end of the access network and receivers at the backbone nodes. Each emitter has several outgoing links: to the receiver in its own backbone node and the neighboring ones. The type of QKD device selected for each node is not arbitrary. Receivers are more expensive and difficult to maintain due to the single-photon detectors, hence they are kept at the telco installations.

This shows that telecom networks not only suit QKD, but they are flexible enough to provide several alternative paths among two nodes (at least in metro areas). Therefore, the network coding approach described in Section II can be used. This implies that a commercial optical network with improved security and resilience, as compared to the traditional scheme, can be designed using QKD and WTR.

References

[1] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *J. Opt. Commun. Netw.*, vol. 5, no. 4, pp. 316–328, Apr 2013.

[2] N. Cai and T. Chan, "Theory of Secure Network Coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 421–437, 2011.