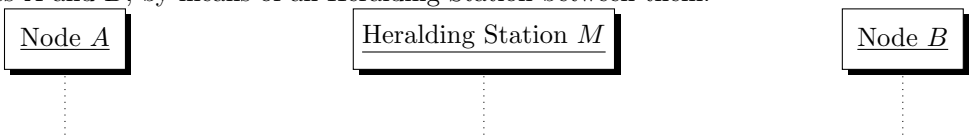
Notes on Link+Physical Layer

Stephanie

March 27, 2018

The objective of this document is to describe a link and physical layer protocol for a quantum network, based on an existing implementation of the physical layer with certain properties. Specifically, it will describe the desired service, interface as well as logical protocol given a means for classical message delivery as well as entanglement generation as a given. The protocol is geared towards producing entanglement between two nodes A and B, by means of an Heralding Station between them.



As a high level summary (see details in section **??**), the desired services provided by the combined link+physical layer protocol is as follows:

- Confirmed (heralded) generation of entanglement with minimum fidelity F between A and B upon request.
- Reliability: "reasonable" assurances that fidelity F is indeed supplied.
- Performance: If the number of generation requests is below a maximum threshold, then requests are honored w.h.p. within some time $t_{\max}$. Many other demands can be made, still TBD (eg on latency or throughput, depending on priorities, see Section **??**)
- Total order: A and B will agree on a total ordering of the entangled pairs without requiring further communication.
- Authenticity: If desired, control communication is authenticated.

This document is structured as follows: In Section 1, assumptions about the delivery of classical messages is described, as well as a short summary of well known classical methods that can turn these relatively weak assumptions into a higher quality assumptions that will be used in the final protocol at the end. In Section 2 an abstract version of a heralded entanglement generation protocol is described, along with the assumptions made about this protocol. This protocol forms the basis of the quantum part of the physical layer. As in the case of sending classical messages, we will lift this basic protocol using standard methods into one that satisfies slightly stronger assumptions which will be used in our overall protocol at the end. In Section **??** an elementary distributed task queue is described that will be used in the final protocol. Finally, Section **??** describes the overall protocol using the components developed in the earlier sections.

1 Sending classical messages

1.1 Starting situation

It will be assumed that there exists a means to transmit classical data between A, B and M. How this is realized is not the objective of this document, and it could be achieved both by a dedicated fiber (possibly

using two wavelength for bidirectional communication), or interspersed with quantum signals on the same fiber. Of interest are merely standard numbers:

- Classical channels are bidirectional, meaning data could in principle be sent in both direction at the same time (and, as a relevant consequence, messages can cross and are not ordered in both directions)
- Likelihood of losses: p_{loss} probability of loss (e.g. following standard fiber loss plus electronics if applicable).
- Likelihood of errors: p_{err} probability of error - where we remark that as in other classical communication burst errors are probably dominant.
- Standard delays of interest: propagation delay (over the fiber), transmission delay (incl. delays of the electronics in putting the packets on the fiber), and processing delay, if known. We will assume that given the highly sophisticated electronics and the fact that the rate of classical communication is low due the relatively low repetition rate of entanglement generation attempts , the transmission and processing delay are essentially negligible.

1.2 Enhanced situation

Two standard methods exist to enhance this situation to the following, whose exact form and choice depends on the parameters above:

- Error dectection: This can be achieved using standard methods, where probably a simple CRC depending on the length of the headers is most appropriate. This will add a number of bits to the messages headers below if employed. For example, for a standard CRC-32 as used in Ethernet, the CRC is computed over the message and stored in a 32 bit header field.
- Message authentication: In this case, this refers to the fact that A knows the messages originate with B (and vice versa). Similarly, M can authenticate messages if desired. Such authentication can be realized using a message authentication code (MAC) (see eg **?**). These can be realize with varying levels of security. If A and B share consumable key (such as for example generated by QKD), they can afford to use one-time MAC which - similar to a one-time pad - offers information-theoretic security. Such MACS, for example based on two-universal hashing, can in principle be fast (see e.g. **?** needing however various levels of key), although it is a question whether they are fast enough to be useful in this context. Steph: Note that this does not automatically imply the entanglement is authenticated: this would only be the case if the midpoint is trusted which is evidently against all principles here. Given the local nodes take actions, like initiating entanglement generation for example, based on classical messages received - it strikes me as highly desirable to do this in order to ensure some form of robustness, given that this can even affect the quality of the qubits already stored etc

2 Entanglement Generation

2.1 Starting situation

In the following, I will highly abstract away from the present entanglement generation protocols in order to highlight some assumptions, and focus only on the relevant elements for the final protocol, namely what information is available where and at what time and who can make decisions (such as choice of fidelity). The following model, also applies to the memory-assisted scheme based on entanglement distillation with minor modifications, but for simplicity I will assume that it is single click or BK.

General assumptions are:

- An association between the classical control messages m below, and the entanglement generation. For this reason, I will write classical message transmission as simply m, and q for arbitrary quantum signal q.

To make it clear, how I will use this abstract description later, I will always take $m = (req, pass)$ where req is request information only for the mid point and later protocol specific, and $pass$ is something that will by default always be passed onto the other side (also protocol specific). Midpoint will provide a response $resp$, for example, success or failure.

- Variables $v_1, \ldots, v_k$, where v_j specifies the number of pairs yet to be created of quality choice j (for example, forming an agregate of a particular choice of bright state population α, or other parameters). It is assumed (see Section **??**) that A, and B agree on the values of these variables. For now simply take $k = 1$.

Very abstractly, a generation protocol thus takes the following form,