Indirect Eavesdropping in Quantum Networks

Stefan Rass
Universität Klagenfurt, Department of Applied Informatics
Universitätsstrasse 65-67
9020 Klagenfurt, Austria
stefan.rass@uni-klu.ac.at

Sandra König
Universität Klagenfurt
Universitätsstrasse 65-67
9020 Klagenfurt, Austria
sakoenig@edu.uni-klu.ac.at

***Abstract*—Quantum networks are communication networks in which adjacent nodes enjoy perfectly secure channels thanks to quantum key distribution (QKD). Drawing end-to-end security from QKD-supported point-to-point security can be done by virtue of multipath transmission. This concept buys security at the cost of strongly connected networks and perfect routing. Particularly the latter is hard to ensure, since congestions or (passive) eavesdropping may cause QKD key-buffers to run empty, thus enforcing local re-routing of packets. Hence, the adversary may use eavesdropping not to extract information, but to *redirect* the information flow towards a relay-node that he controls. Such attacks can readily invalidate the stringent requirements of multipath transmission protocols and thus defeat any formal arguments for perfect secrecy. Moreover, this form of "indirect eavesdropping" seems to be unconsidered in the literature so far. We investigate whether or not unconditional security in a quantum network with non-reliable routing is possible. Using Markov-chains, we derive various sufficient criteria for retaining perfect secrecy under imperfect packet relay. In particular, we explicitly do not assume trusted relay or quantum repeaters available.**

***Keywords*-Quantum Cryptography, Markov-Chain, Secure Routing, Information-Theoretic Security**

I. Introduction

Quantum key distribution (QKD) [1] is renowned for providing unconditional security over direct channels with no intermediate nodes. Securing an entire network by means of QKD calls for additional measures, as up to now, the technology is still limited to point-to-point security. Creating end-to-end security has been subject of independent research, culminating in multipath transmission regimes. The latter can provide unconditional end-to-end security from perfectly protected links, which is exactly what QKD can do. However, most results in this area hinge on two major ingredients: sufficient graph connectivity and the sender having the routing under full control. Since the requirements for multipath transmission are stringent and therefore easily invalidated, a passively eavesdropping adversary may cause QKD key-buffers to run empty and thus enforce re-routing of packets over a set of nodes under his control. Since QKD can only protect links but not nodes, he can use eavesdropping on a link to redirect and extract information from another node. We call this *indirect eavesdropping*. Even without the adversary becoming active, local congestions may as well cause deviations from the intended routing, and consequently destroy the protection of the secret message. Our contribution in this paper is investigating the extent to which quantum networks are resilient to such incidents.

Organization of the paper: We consider networks employing QKD for point-to-point- and multipath routing for end-to-end security, referred to as *quantum networks*. For convenience of the reader, we briefly review the use of QKD with multipath transmission in Section III. In Section IV, we introduce a Markov-chain model for the path that a data packet takes from the sender to the receiver, with a particular focus to multipath transmission. Conditions under which a random routing regime can yield perfect secrecy are derived in Section V, with an example supporting the practicability of our results in Section VI. Final remarks are given in Section VII.

II. Related work

Most closely related to our work are the results in [2], who provide a stochastic routing algorithm along with probabilistic measures of secrecy in a randomly compromised network. We improve on this by taking an existing routing regime and giving conditions under which it can provide perfect secrecy under random compromission. Motivated by the physical distance limitations of practical QKD implementations (cf. [3], [4], [5] to name a few) in spite of the theoretical possibility of unlimited distance QKD transmission [6], multipath transmission over disjoint channels remains a theoretical necessity for perfect end-to-end security [7]. In particular, [8], [9], [10], [11] and references therein form the basis for our work, where our goal is investigating a hidden assumption within these results: what happens if the routing is random rather than fully controllable? Implementations of multipath transmission within the TCP protocol are currently under standardization, and many other protocols like stream control transmission protocol (SCTP [12]) as well facilitate concurrent transmission. Similarly as for a recently proposed extension of SSL by QKD [13], [14], one could imagine QKD being integrated in such protocols. Load-balancing, local congestions and most importantly (adversarial) eavesdropping can all cause re-routing of packets and therefore make otherwise disjoint

 ISBN: 978-1-61208-151-9

routes intersecting. Our work is an explicit account for security under such random distortions. To the best of our knowledge, such indirect eavesdropping attacks have not yet been considered elsewhere in the literature.

III. QKD-Based Multipath Transmission

Our adversary model will be a computationally unbounded passive threshold adversary Eve. That is, given a network $G = (V, E)$, with a sender s and receiver r (both in V), the adversary can compromise up to $k \leq |V \setminus \{s, r\}|$ *nodes* in G (thanks to QKD, an activity on any of the links would be detected anyway). Moreover, Eve knows all relevant protocol specification and the network topology, but sticks to the protocol in a merely passive attempt to extract secret content flowing over the network.

For a string $M \in \{0,1\}^*$, let $|M|$ be its length (in bits), and let H be the Shannon-entropy. We will use the following security model (similarly to the model given in [7]):

Definition III.1. *Let $\varepsilon > 0$, and let Π be a message transmission protocol. Suppose that for conveyance of a message $M \in \{0,1\}^*$, the packets $C_1, \ldots, C_n \in \{0,1\}^*$ are transmitted over the network (constituting the protocol's* transcript*). The adversary's* view *on the transmission of M is adv$(M) \subseteq \{C_1, \ldots, C_n\}$. We call a protocol ε-secure, if $H(M|\text{adv}(M)) \in \{0, H(M)\}$ and $Pr[H(M|\text{adv}(M)) = 0] \leq \varepsilon$, i.e., the adversary can disclose M with a chance of at most ε. We call the protocol Π* efficient*, if the size of the transcript, i.e., $\sum_{i=1}^{n} |C_i|$, is polynomial in the size of the message M, the size of underlying network (in terms of nodes), and $\log \frac{1}{\varepsilon}$. A protocol that is ε-secure for any $\varepsilon > 0$ is said to enjoy* perfect secrecy.

It is easy to see that if a protocol is ε-secure with $\varepsilon < 2^{-|M|}$, then simply guessing the message is more likely than breaking the protocol itself.

Multipath transmission pursues a simple idea: having t paths from s to r that are node-disjoint, the sender can transmit a message m by first putting it through a (t', t)-secret sharing (Shamir's for instance), giving the shares $s_1, \ldots, s_t$ and sending each share over its own (distinct) path to r. The adversary is successful if and only if he catches at least t' shares. Obviously, the scheme is unconditionally secure if $t' > k$ (where k is the adversary's threshold), but in addition, we require full knowledge of the topology, and assured delivery over the chosen disjoint paths. The general interplay between network connectivity and unconditional security has been studied extensively, and our goal in the next section is finding out whether or not unconditional security can be retained if the paths are not fully under the sender's control (i.e., what happens if the adversary indirectly fiddles with the routing).

IV. A Markov-Chain Routing Model

Assume a quantum network modeled as a graph $G = (V, E)$ with $|V|$ nodes and nb(v) denoting the set of v's neighbors. Formally, we put nb$(v) := \{u \in V | (v, u) \in E\}$. For each $v \in V$, it is trivial to (empirically) estimate the probability distribution supported on nb(v), indicating the chances for a packet to leave towards the j-th neighbor. If the transition from u to v is denoted as $u \to v$, then this (local) distribution comprises the probabilities $\Pr[u \to v_i]$ where $v_i \in \text{nb}(u)$. The whole process can be considered as a Markov chain, with the transition matrix P describing the hops along which a data packet travels. In other words, the "chain" is the list of intermediate nodes that a packet comes across, with the *state* of the chain being the node that currently hosts the message before forwarding it. As outlined in Section III, it is reasonable to assume a multipath transmission regime in the absence of infinitely long quantum channels. Hence, we will look at an ensemble of t independently traveling packets with corresponding trajectories (traces) starting off the nodes $v_1, v_2, \ldots, v_t$. Without loss of generality, and to ease notation in the sequel, call the starting nodes $1, 2, \ldots, t$, with the sender's node being number "0", having the neighborhood nb$(0) = \{1, 2, \ldots, t\}$. The receiver's node has number r. So, $|V| = r + 1$ and $V = \{0, 1, 2, \ldots, r\}$.

To simplify technicalities, let us assume a *synchronous* forwarding regime, i.e., the nodes simultaneously forward their packets at fixed times. Despite this assumption appearing restrictive, it does in no way affect the validity of the obtained results, as will become evident soon. In particular, the derived formulas equally perfectly apply to a setting in which nodes independently forward their data.

Let the distribution $\pi_i(n, v) : \mathbb{N} \times V \to [0, 1]$ describe the chance that the i-th trajectory ($i = 1, 2, \ldots, t$) is within node v at time $n \in \mathbb{N}$. The whole distribution is denoted as $\pi_i(n)$, and the whole ensemble of t trajectories is denoted as $\pi(n) = (\pi_1(n), \ldots, \pi_t(n))$. The particular state of the i-th trajectory at time n is written as $X_i(n)$. Consider an arbitrary but fixed trajectory i in the following. It is well known from the theory of Markov chains that the state of the i-th chain is governed by $\pi_i(n) = P^n \cdot p_i(0)$, where P is the transition matrix. Our chain has only a *single absorbing state*, which is the receiver's state r (the receiver will surely not pass on his message any further). Furthermore, it can be assumed irreducible, because if it were not, then there would be at least two nodes u, v in the network whose chance of getting a packet from u to v is zero, so they could never communicate.

We write H_{jA} for the time (measured in *hops*) that it takes a trajectory to get from j to a set of $A \subseteq V$ target nodes,

$$H_{jA} = \min \{n \geq 0 : X_i(n) \in A | X(0) = j\}.$$

The probability h_{jA} of the chain ever reaching A from j is therefore $h_{jA} = \Pr[H_{jA} < \infty]$, and the family $(h_{jA}; j \in V)$ is the smallest non-negative solution of the equation system

$$h_{jA} = \sum_{i \in V} p_{ji} h_{iA}, \tag{1}$$

where $h_{jA} = 1$ for all $j \in A$ and p_{ji} is the probability of passing from node j onwards to node i (see [15, p.123] for details). Writing down this system for, say $n = 5$ equations with $A = \{1, 3\}$, we get (after some minor algebra),

$$\begin{array}{rcccc} -p_{21} - p_{23} & = & (p_{22} - 1)h_{2A} & + & p_{24}h_{4A} \\ -p_{41} - p_{43} & = & p_{42}h_{2A} & + & (p_{44} - 1)h_{4A}, \end{array}$$

where we additionally substituted $h_{rA} = 0$, as r is the only absorbing state of our chains. Let us write (in a slight abuse of notation) $P_{-R,-C}$ to denote the matrix P with all rows in R and all columns in C *deleted*. Similarly, we use the notation $P_{R,C}$ to denote the matrix P only with the rows in R and columns in C retained. To ease notation, let us put $Q := P_{-r,-r}$, i.e., Q is P without the r-th row and column. If I is the identity matrix, and $\mathbf{1}$ is the vector of all 1's, then the above equation system takes the compact form

$$-Q_{-A,A} \cdot \mathbf{1} = (Q_{-A,-A} - I)h_A, \tag{2}$$

where h_A is the family $(h_{1A}, h_{2A}, \ldots, h_{rA})$, excluding $h_{rA} = 0$ and $h_{jA} = 1$ for all $j \in A$. In order to have the values h_j for $j \neq r$ and $j \notin A$ well-defined, we ought to show that $(Q_{-A,-A} - I)$ is invertible. This is our first

Lemma IV.1. *Let P be a stochastic matrix of an irreducible Markov-chain with the state space V and exactly one absorbing state $r \in V$. Select any set of states $A \subset V$ with $r \in A$, and let $Q = P_{-A,-A}$ be the submatrix of P that describes transitions between states outside of A. Then $Q - I$ is invertible.*

Proof: Partition the state set V into $V_1 = A$ and $V_2 = V \setminus A$, then $r \in V_1$ and Q describes transitions *within* V_2. For each $v \in V_2$, write $\pi_{V_2}(n, v)$ for the chance of the chain being in state v after n steps. From the theory of Markov-chains, we know that the vector $\pi_{V_2}(n) = (\pi_{V_2}(n, v))_{v \in V_2}$ is given by $\pi_{V_2}(n) = Q^n \pi_{V_2}(0)$. As the chain is irreducible, we will eventually reach r from *any* state in V_2, and since r is absorbing, this means that $Q^n \to 0$ as $n \to \infty$. Now, put $(Q - I)x = 0$. Then $Qx = x$ and on iterating $Q^n x = x$. As $n \to \infty$, $Q^n x = x \to 0$, so $Q - I$ is invertible. ∎

Lemma IV.1 helps constructing a formula giving us the chance that exactly l trajectories pass through a given area $A \subseteq V$ that is under the adversary's control. We can solve the system (2) for any given set A and see whether it is passed with certainty. Similarly as for the binomial distribution, we can ask for the probability of a subset of l trajectories hitting A within finite time, with the remaining ones never reaching A. The probability we are after is the sum over all subsets of size l. Formally, we have

Proposition IV.2. *Let a graph $G = (V, E)$ be given, and assume a random walk of t trajectories starting at nodes $1, 2, \ldots, t$. For a given $A \subseteq V$, the chance of l trajectories passing through A is given by*

$$p(A, l) = \sum_{\substack{M \subseteq [1:t] \\ |M| = l}} \left[\prod_{i \in M} h_{iA} \prod_{i \in ([1:t] \setminus M)} (1 - h_{iA}) \right],$$

where the vector $h_k = (h_{iA})_{i \in V}$ is calculated as described above (i.e., put $h_{rA} = 0, h_{jA} = 1$ for all $j \in A$, and calculate the remaining probabilities by solving (2)*). Here, $[1 : t]$ is a shorthand notation for the set $\{1, 2, \ldots, t\}$.*

V. Perfect Secrecy under Random Routing

According to Proposition IV.2, the adversary will not learn anything unless he conquers some set A that is passed by sufficiently many, say l, trajectories. Consequently, his best strategy is attacking the set with maximum likelihood of seeing sufficiently many trajectories. It follows that the most vulnerable subset of nodes in the network is

$$A^* = \operatorname*{argmax}_{A \subseteq V} \Pr[l \text{ trajectories traverse } A] = \operatorname*{argmax}_{A \subseteq V} p(A, l). \tag{3}$$

The following result is an immediate consequence of the above discussion:

Theorem V.1. *A network with a routing regime described by a transition matrix P can provide perfect secrecy if and only if for some integer $l \geq 1$, we have $p(A, l) < 1$ for all $A \subseteq V$ that the adversary can compromise.*

Despite this maximum likelihood optimization problem being sound, it is yet infeasible to evaluate as the number of subsets to test is exponential (in the adversary's threshold). We shall therefore set out to find sufficient criteria that are easier to test.

For a 1-passive adversary, we have the following criterion:

Theorem V.2. *Let $t = |nb(s)| \geq 1$ count the sender s's neighbors. If, for each $v \in V$, we have $\sum_{i=1}^{t} h_{iv} < t$, then the network provides perfect secrecy against a 1-passive adversary.*

Proof: Put the secret message through a (t, t)-secret sharing and let each share take its own individual path through the network (i.e., do a random walk according to the transition matrix P). With the random indicator variable

$$\mathbb{I}_{i,j} := \begin{cases} 1, & \text{if } h_{ij} > 0 \\ 0, & \text{otherwise,} \end{cases}$$

the number of trajectories passing through a node $v \in V$ is given by $N_v := \sum_{i=1}^{t} \mathbb{I}_{i,v}$, and its expected value is $\mathsf{E}(N_v) = \mathsf{E}(\sum_{i=1}^{t} \mathbb{I}_{i,v}) = \sum_{i=1}^{t} h_{iv}$. The assertion now directly follows from Markov's inequality, since

$$\Pr[N_v \geq t] \leq \frac{\mathsf{E}(N_v)}{t} < \frac{t}{t} = 1,$$

which holds for all $v \in V$. The network thus provides perfect secrecy by Theorem V.1. ∎

 ISBN: 978-1-61208-151-9

Theorem V.3. *Let $G = (V, E)$ be a graph, and let the sender and receiver be $s, r \in V$. Let the adversary be k-passive, i.e., up to k nodes in G can be compromised. For perfect secrecy, it is necessary that $|nb(s)| > k$. In that case, with $V^* := V \setminus \{s, r\}$, if*

$$\forall i \in nb(s) : h_{ij} \leq \frac{1}{ek} \ \ \forall j \in V^* \setminus \{i\},$$

then the network provides perfect secrecy.

Proof: Without loss of generality, assume s's neighbors to be the nodes $\{1, 2, \ldots, t\}$, and put the secret message m through a (t, t)-secret-sharing scheme, transmitting the i-th share over the i-th neighbor of s (the remaining path of each is individual and determined by the network's transition matrix P). Observe that the adversary will not learn anything unless he gathers all t shares.

If $t \leq k$, then the adversary can "cut off" s from the rest of the network, thus reading all information conveyed by s, and perfect secrecy is impossible by Theorem V.1.

Assume $t > k$ henceforth, so there exists at least one honest neighbor of s in every attack scenario. Let $A \subseteq V$ with $A = \{j_1, \ldots, j_k\}$ be a set of compromised nodes. The (mutually dependent) events $T_l^{j_i}$ for $i = 1, 2, \ldots, k$ occur when the trajectory starting off the node l reaches node j_i. For each (starting node) $l = 1, 2, \ldots, t$, we have

$$\Pr\left[T_l^{j_i}\right] = h_{lj_i} \leq \max\{h_{lv} | v \in V \setminus \{l, s, r\}\} \leq \frac{1}{ek}, \quad (4)$$

where the last inequality follows from our hypothesis. Since $\Pr\left[T_l^{j_i}\right] \leq \frac{1}{e \cdot k}$, then Lovász local lemma (symmetric version) implies

$$\Pr\left[\bigcap_{\nu=1}^{k} \overline{T_i^{j_\nu}}\right] > 0. \quad (5)$$

In other words, the l-th trajectory has a positive chance of *evading* the set $\{j_1, \ldots, j_k\}$. Since inequality (4) holds independently of the particular j_i's, (5) is true for all these sets. If condition (4) holds for all $l = 1, 2, \ldots, t$, then in every attack scenario there is at least one trajectory with a positive chance of *not* passing through the compromised area in the graph. So, for every $A \subset V$ with $|A| \leq k$, it holds that $p(A, t) < 1$ and the network can provide perfect security. ∎

Efficiency

Regarding the bandwidth demand, we require the overall network traffic (bit complexity) and round complexity to be polynomial in $\log \frac{1}{\varepsilon}$ for any chosen $\varepsilon > 0$. Assume the network satisfies the condition for perfect secrecy in Theorem V.1.

Fix some $\varepsilon > 0$. We will prove the following transmission regime to enjoy efficient bit- and round-complexity, i.e., polynomial efforts in $\log \frac{1}{\varepsilon}$. Let the secret message transmitted from s to r be m:

1) put m through a (n, n)-secret sharing, giving the shares $s_1, \ldots, s_n$ (the number n will be determined below).
2) for $i = 1, 2, \ldots, n$ do the following: put the i-th share s_i through a (t, t)-secret sharing, where $t = |\mathrm{nb}(s)|$, and transmit the j-th share of s_i over the j-th neighbor of s.

Obviously, the attacker will not learn anything unless he gets all the information flowing over the network (due to the (n, n)- and (t, t)-sharings). Our task is proving n to be polynomial in $\log \frac{1}{\varepsilon}$ and the size of the network. For the proof, define an indicator variable for each round $i = 1, 2, \ldots, n$ via

$$\mathbb{I}_i = \begin{cases} 1, & \text{if the share } s_i \text{ was disclosed;} \\ 0, & \text{otherwise,} \end{cases}$$

so that $\mathbb{I}_i$ measures the adversary's success (in a binary scale) in the i-th round. By our hypothesis, Theorem V.1 implies $\Pr[\mathbb{I}_i = 1] < 1$ for all rounds i and all sets of nodes that the adversary could have conquered (recall that the adversary is k-passive). Put $\rho := \max_{i=1,2,\ldots,n} \Pr[\mathbb{I}_i = 1]$, then $\rho < 1$. Since $0 \leq \mathbb{I}_i \leq 1$ for all i, the first moment $\mathsf{E}(\mathbb{I}_i)$ exists and $\mathbb{I}_i$'s deviation from its mean is bounded by $-1 \leq \mathbb{I}_i - \mathsf{E}(\mathbb{I}_i) \leq 1$ for all i. Define $S := \sum_{i=1}^{n} \mathbb{I}_i$, then since $\mathsf{E}(\mathbb{I}_i) \leq \rho$, we get $\mathsf{E}(S) = \sum_{i=1}^{n} \mathsf{E}(\mathbb{I}_i) \leq n\rho$. Moreover, $S - \mathsf{E}(S) \geq S - n\rho \geq \tau$ for some τ to be fixed later. Application of a variant of Hoeffding's inequality (with relaxed independence constraints; see [16]) gives

$$\Pr[S - n\rho \geq \tau] \leq \Pr[S - \mathsf{E}(S) \geq \tau] \leq \exp\left(-\frac{\tau^2}{2n}\right)$$

Since $\frac{1}{n} S \geq \min_i \mathbb{I}_i$, we can choose τ to satisfy $\frac{\tau}{n} \leq \min_i \mathbb{I}_i - \rho \leq \frac{1}{n} S - \rho$. So we can continue the chain of inequalities on the left-side as

$$\Pr\left[\min_i \mathbb{I}_i - \rho \geq \frac{\tau}{n}\right] \leq \Pr[S - n\rho \geq \tau] \leq \exp\left(-\frac{\tau^2}{2n}\right),$$

and by taking $\delta := \frac{\tau}{n}$ we conclude that

$$p := \Pr\left[\min_i \mathbb{I}_i \geq \rho + \delta\right] \leq \exp\left(-\frac{n\delta^2}{2}\right)$$

for all $\delta \geq 0$. By construction, the adversary is successful if and only if $\mathbb{I}_i = 1$ for all rounds $i = 1, 2, \ldots, n$, or equivalently, $\min_i \mathbb{I}_i = 1$. Choosing $\delta := 1 - \rho > 0$, the number n of rounds until $\Pr[\min_i \mathbb{I}_i \geq \rho + \delta = 1] < \varepsilon$ is achieved comes to $n \in \mathcal{O}\left(\log \frac{1}{\varepsilon}\right)$. The bit-complexity is $n \cdot t \cdot |m|$, where $|m|$ is the length of the message, and as such in $\mathcal{O}\left(|m| \cdot |\mathrm{nb}(s)| \cdot \log \frac{1}{\varepsilon}\right)$, i.e., polynomial in the network size and $\log \frac{1}{\varepsilon}$. Summarizing the discussion, we have proved

Theorem V.4. *If a given network provides perfect secrecy according to Theorems V.1, V.2 or V.3, then there is an efficient protocol achieving this.*

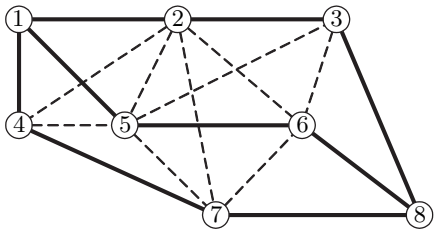

Figure 1. Example multipath transmission from 1 to 8

VI. Application to Quantum Networks

It is important to emphasize that Theorems V.1, V.2 and V.3 *should not* directly be applied to the communication network at hand. Instead, we are interested in estimating the harm that any deviation from a prescribed routing strategy causes. Going back to multipath transmission, our goal is using the results from the previous section to classify a given network as (in)secure under the assumption of random detours that a packet takes upon local congestions or empty local quantum-key-buffers.

We illustrate the application of Theorem V.3 using a simple example, which we hope demonstrates the general line of reasoning. Take the network shown in Figure 1, with each link secured by means of QKD. Alice (node 1) performs a multipath communication over three disjoint channels $\rho_1 = (1 \to 2 \to 3 \to 8), \rho_2 = (1 \to 5 \to 6 \to 8), \rho_3 = (1 \to 4 \to 7 \to 8)$ (shown bold) to Bob's node 8. Assume that each node does the packet forwarding reliably, up to some chance of α for the packet to deflect from the prescribed route. Thus, assuming stochastic independence for the sake of simplicity, with probability $1 - \alpha^{\text{length}(\rho_i)-2}$, the packet will travel over ρ_i as desired. Notice that any path is accessible from any other, and that an adversary will surely not waste resources by attacking anywhere else than on the chosen paths. Hence, we can create an abstract model for such a multipath transmission by restricting the focus on whether the packets travel as desired (likelihood determined by the reliability of routing, i.e., the probability of the packet not deviating from its prescribed route), or whether they take detours (should happen with a small chance only) that could yield to intersecting paths and disclosure of the secret message.

For the analysis of a general network $G = (V, E)$ under a multipath transmission scenario, we therefore consider the auxiliary graph $G' = (V', E')$: let $\rho_1, \ldots, \rho_t$ be paths in G, then each of these becomes a node in G', which is connected to the sender and receiver, so put $V' := \{\rho_1, \ldots, \rho_t\} \cup \{s, r\}$. Attacking elsewhere than on the paths $\rho_1, \ldots, \rho_t$ is less paying for the adversary than compromising the paths themselves, so we may safely disregard any nodes in the network that are not on a chosen path. Also, assume that a packet can jump from any path to any other, so the nodes $\rho_1, \ldots, \rho_t$ form a clique. Finally, each path ρ_i is connected to the receiver r in a one-way manner, as the receiver is absorbing and will not pass anything further. Similarly, the sender is (one-way-)connected to all his chosen paths, though these transitions are of no further interest, since an accidental jump from a path back to the sender can trivially be corrected by the sender putting the packet back on its correct path. The set of edges therefore comes to $E' = \{\rho_1, \ldots, \rho_t\}^2 \cup \{(\rho_i, r), (s, \rho_i) | i = 1, 2, \ldots, t\}$. The resulting transition graph for the example is depicted in Figure 2, with arrows indicating possible state transitions.

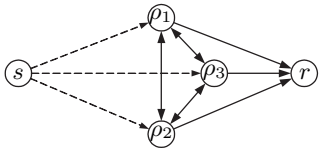

Figure 2. Auxiliary graph G' describing state transitions

The topology of the auxiliary graph G', excluding the transitions from s to each ρ_i (for obvious reasons) defines the Markov-chain on which we can invoke the results from Section V. For the analysis, it remains to specify the following likelihoods:

- $\Pr[\rho_i \to r]$: with the parameter α as above, this is $\Pr[\rho_i \to r] = 1 - \alpha^{\text{length}(\rho_i)-2}$. Notice that several events of node failure are not necessarily independent, and correlations among these must be considered in a more accurate (perhaps more realistic) model.
- $\Pr[\rho_i \to \rho_j]$: this quantity depends on the particular chances of jumping from a node on ρ_i to any node on ρ_j, and must be worked out individually for the network at hand. For the sake of simplicity and illustration, we assume an equal likelihood of jumping on any other path once ρ_i is left. For the example, we take $\Pr[\rho_i \to \rho_j] = \frac{1}{t-1}(1 - \Pr[\rho_i \to r])$.

Since the jumps from the sender to each of his chosen paths are uninteresting, we do not need to model the corresponding transition probabilities, nor must these appear in the transition matrix of the Markov-chain. These links are merely included to have G' consistent with our criteria, and are therefore shown dashed.

With $\alpha = 0.01$, we end up finding the transition matrix:

$$P = \begin{array}{c} \\ \rho_1 \\ \rho_2 \\ \rho_3 \\ r \end{array} \begin{array}{c} \begin{array}{cccc} \rho_1 & \rho_2 & \rho_3 & r \end{array} \\ \begin{pmatrix} 0 & 0.01 & 0.01 & 0.98 \\ 0.01 & 0 & 0.01 & 0.98 \\ 0.01 & 0.01 & 0 & 0.98 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Now, we can use Theorem V.3 on this matrix to see that the network is indeed secure against a 2-passive adversary: with $V^* = \{1, 2, 3\}$ and by solving (2) for $A = \{1\}, \{2\}, \{3\}$, we find $h_{ij} = \frac{1}{99} < \frac{1}{2e} \approx 0.184$, for each $i, j \in V^*, j \neq j$. It follows that the network remains secure even under

much less reliable routing. Indeed, we can tolerate up to $\alpha \approx 0.155$, i.e., a more than 15% chance of the packets becoming re-routed via indirect eavesdropping or congestion control. Finally, Theorem V.4 tells that resilience against such incidents can be retained efficiently.

VII. Conclusion

We have obtained simple criteria for protection against passive adversaries. Carrying over our results for active (Byzantine) adversaries, one needs a slightly different transmission technique. In fact, (k, n)-secret sharing is resilient against an active adversary compromising up to $\lfloor (n-k)/2 \rfloor$ shares [17]. Future work will include refining and adapting our criteria for Byzantine adversaries, as well as investigating transmission efficiency (notice that the proof of Theorem V.4 no longer holds for active adversaries. Still, QKD enhanced multipath routing can indeed bring perfect secrecy to future networks, even without much change to the existing routing regimes apart from using QKD. More detailed examples are subject to ongoing research in the context of a project where this framework is going to be tested empirically. We will report on this in future papers.

Our results are only indirectly dependent on the quantum nature of the network, as the attack targets the multipath transmission regime only by *exploiting* general QKD properties. These are, moreover, independent of the particular QKD-implementation, and equally well apply to discrete or continuous quantum information encodings. In general, any successful denial-of-service attack, regardless of whether on a conventional or quantum line, can be used for indirect eavesdropping in the described form, as soon as secure multipath transmission is used.

This work is an explicit account for an adversary who turns the QKD eavesdropping detection against the network. If end-to-end security is set up by means of multipath transmission, then "disconnecting" (by eavesdropping) otherwise adjacent nodes may enforce local re-routing of packets and in turn direct the information flow right into the adversary's hands. We presented various sufficient criteria for this kind of "indirect eavesdropping attacks" to be repealable. In general, our criteria can be used to decide whether or not a network retains perfect secrecy under randomly compromised nodes and routes.

References

[1] C. Bennett and G. Brassard, "Public key distribution and coin tossing," in *IEEE Int. Conf. on Computers, Systems, and Signal Processing*. IEEE Press, 1984, pp. 175–179.

[2] H. Wen, Z. Han, Y. Zhao, G. Guo, and P. Hong, "Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network," *Science in China Series F: Information Sciences*, vol. 52, no. 1, pp. 18–22, 2009.

[3] T. Schmitt-Manderbach, "Long distance free-space quantum key distribution," Ph.D. dissertation, Ludwig–Maximilians–University Munich, Faculty of Physics, 2007.

[4] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-conversion detectors," *Opt. Express*, vol. 15, pp. 15 920–15 927, 2007.

[5] H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, "1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm," *Optics Express*, vol. 15, pp. 7247–7260, Jun. 2007.

[6] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, pp. 2050–2056, 1999, arXiv:quant-ph/9803006.

[7] M. Franklin and R. Wright, "Secure communication in minimal connectivity models," *J. of Cryptology*, vol. 13, no. 1, pp. 9–30, 2000.

[8] M. Franklin and M. Yung, "Secure hypergraphs: privacy from partial broadcast," in *Proc. of the 27th annual ACM Symp. on Theory of computing*, ser. STOC '95. New York, NY, USA: ACM, 1995, pp. 36–44.

[9] Y. Wang and Y. Desmedt, "Perfectly secure message transmission revisited," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2582–2595, 2008.

[10] M. Fitzi, M. K. Franklin, J. Garay, and S. H. Vardhan, "Towards optimal and efficient perfectly secure message transmission," in *Proc. of 4th Theory of Cryptography Conf. (TCC)*, ser. LNCS 4392. Springer, 2007, pp. 311–322.

[11] M. Ashwin Kumar, P. R. Goundan, K. Srinathan, and C. Pandu Rangan, "On perfectly secure communication over arbitrary networks," in *PODC '02: Proc. of the 21st annual Symp. on Principles of distributed computing*. New York, NY, USA: ACM, 2002, pp. 193–202, last access: 05/17/2011.

[12] R. Stewart, "RFC4960: Stream Control Transmission Protocol," http://tools.ietf.org/html/rfc4960, September 2007, last access: 05/17/2011.

[13] M. Pivk, C. Kollmitzer, and S. Rass, "SSL/TLS with quantum cryptography," in *Proc. of the 3rd Int. Conf. on Quantum, Nano and Micro Technologies*. IEEE Computer Society, February 2009, pp. 96–101.

[14] A. Mink, S. Frankel, and R. Perlner, "Quantum key distribution (qkd) and commodity security protocols: Introduction and integration," *Int. J. of Network Security & Its Applications (IJNSA)*, vol. 1, no. 2, pp. 101–112, July 2009.

[15] D. Stirzaker, *Stochastic Processes & Models*. Oxford University Press, 2005.

[16] W. D. Smith, "Tail bound for sums of bounded random variables," URL: http://www.math.temple.edu/∼wds/homepage/works.html, April 2005, last access: 05/17/2011.

[17] R. McElice and D. Sarwate, "On sharing secrets and Reed-Solomon codes," *Communications of the ACM*, vol. 24, no. 9, pp. 583–584, 1981.

 ISBN: 978-1-61208-151-9