On the security of quantum networks: a proposal framework and its capacity

Quoc-Cuong Le*, Patrick Bellot* and Akim Demaille**

(*) ENST-LTCI, Paris, France, (**) EPITA-LRDE, Paris, France

Abstract. In large Quantum Key Distribution (QKD)-based networks, intermediate nodes are necessary because of the short length of QKD links. They have tendency to be used more than classical networks. A realistic assumption is that there are eavesdropping operations in these nodes without knowledge of legitimate network participants. We develop a QKD-based network framework. We present a percolation-based approach to discuss about conditions of extremely high secret key transmission. We propose also an adaptive stochastic routing algorithm that helps on protecting keys from reasonable eavesdroppers in a dense QKD network. We show that under some assumptions, one could prevent eavesdroppers from sniffing the secrets with an arbitrarily large probability.

1 Introduction

The problem of transmitting a secret key from an origin to a destination on the network was considered for a long time, and currently solved in most of Internet applications by using Public Key Infrastructure (PKI). PKI relies on unproven assumptions about the computing power of eavesdroppers and the non-existence of effective algorithms for a certain mathematical hard problems. Thus, PKI cannot meet higher security level requirements. Quantum Key Distribution (QKD) technology is an alternative that provides unconditional security, but supports only point-to-point connections. Besides, QKD has some significant limits on throughput and range [1,2]. Moreover, QKD large networks are always vulnerable as some nodes may be controlled by eavesdroppers. That makes an open question: how to build large QKD-based networks capable of supporting extremely high secret key exchange between network participants?

This paper studies the model of a partially compromised QKD network in which two members want to establish a common key with almost-certainty that this key will not be eavesdropped. The contributions are (i) a model of partially compromised QKD networks, (ii) the use of percolation theory techniques to find where almost-certainty can be achieved, (iii) a proposal based on stochastic routing capable obtaining a given secrecy level requirement.

In 2, we introduce the context and our problem statement. In 3, we use percolation theory to show where almost-certainty can be achieved and we also present an adaptive stochastic routing algorithm. We analyze it in some attack strategies. Relations with other works is presented in 4 and we conclude in 5. The proofs of the theorems are given in Appendix.

2 A proposed quantum network framework and the problem statement

QKD-based networks, also called quantum networks, are the special purpose networks that aim to an extremely high level security of secret key transmissions between two arbitrary member pair Alice and Bob on the network. Nowadays, the most famous quantum network is DARPA quantum network that, with its specific characteristics of consisting of a few nodes, should be considered as a special model for quantum network. A general fully architecture of large quantum networks is still in discussion. However, we should consider two prominent foreseeable characteristics of quantum networks as follows: (1) Links between two adjacent nodes of the network are perfectly trusted and (2) Quantum networks need more intermediate nodes than classical ones to totally cover the same region.

Direct QKD links are proven perfectly secure by information theory. This is a perfect mean for secret key transmissions. There are also some realistic applications [1–6]. Unfortunately, QKD links are only implemented for the short distances. The current records of these links are 150 km in fiber and 23 km in free space, with a typical rate of 1 Kb/s or so. In order to overcome this limitation, we think of a chain of successive terminals such that each terminal is capable establishing a direct QKD link with the previous and another one with the next terminal. This is also called QKD data relays. Note that such a relay is not quantum repeater and data appears unencrypted for all the relays on the transmission. To ensure that data is secured in the transmission, one must ensure that all the intermediate relays are not eavesdropped. The DARPA quantum network was constructed based on this idea. This implies the key assumption that one has already protected all the DARPA network's nodes. Such an assumption can be acceptable in the context of a few node network as the DARPA network, however, this is unconvincing as we must deal with more large networks.

In this paper, as we want to solve the problem of large quantum networks, we should not use the assumption of ultimately trusted nodes as in DARPA network's model. We consider a new assumption: Eve cannot eavesdrop on all the nodes, but on some nodes without leaving any trace. Such an assumption seems to be more plausible in realistic contexts. With the new assumption, the choice of a good topology for quantum network becomes more important. Eve could prefer to eavesdrop on some nodes than others. It means that the probability of being attacked for some nodes could be more than the others. Thus, if quantum network topology presents some backbone nodes as that of Internet, then certainly Eve prefers to attack these nodes than others. The concentrated architecture may be not good for quantum network problem. It is better if we could make Eve confused in choosing the attack targets. In such a situation, the best attack strategy for Eve is to choose randomly targets according to a uniform distribution. In this paper, we restrict our attention to such an attack strategy.

A fully standard reference model for quantum network is still in discussion. What the best topology should be is an open question. As mentioned above, the

concentrated topology as that of Internet which features some backbone nodes may be not good because such a topology helps Eve choose her targets. If we assume that Eve only attacks and gains control on some proportion of all the nodes, then a distributed topology that makes Eve confused in choosing her target can improve the global security. The short distance covered by today's QKD-links also influences the topology network design. Although the maximum length of quantum links is about 150 km, because of rates and costs, 30 km-long quantum links are more likely to be used. As a first step in studying QKD networks, we restrict our attention in a simple square grid, a 4-connected lattice, see Fig. 1, large enough so that we can neglect nodes on the boundaries. This models roughly a large region meshed with QKD links.

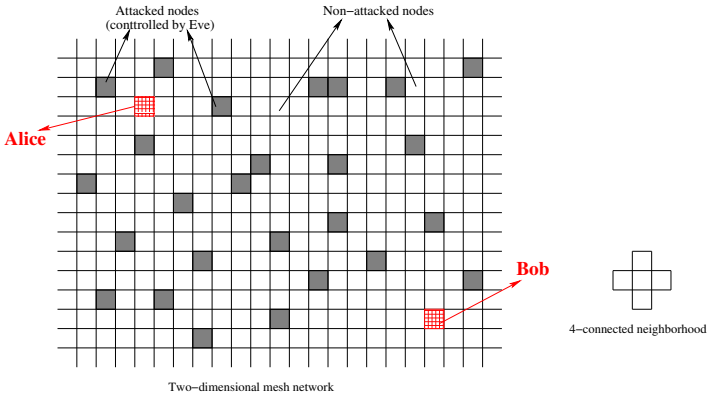

Fig. 1. Two-dimensional lattice network

2.1 Problem statement

Eve can control any node with probability $p_a \in [0, 1]$. These nodes are called by *attacked* or *unsafe* nodes; the others are *safe*. Alice and Bob can be any node. Alice wants to send securely the key K to Bob. They do not know whether a node is safe but they know the probability $p_s = 1 - p_a$ with that a node is safe. Every message that passed over one or more unsafe nodes is considered as being eavesdropped by Eve, but there is no way to verify whether a message is eavesdropped or not. We consider to a key transmission method as follows:

1. Alice uses a stochastic routing algorithm to send to Bob N blocks (or random messages) $M_1, M_2, .., M_N$; all are the same length as the key K.
2. Alice and Bob computes $K = \sum_{i=1}^{N} \oplus M_i$ where $\oplus$ is the bit-wise XOR.

According to Information Theory [7], even if Eve intercepts all the blocks M_i but one, the key K is safe.

One can ask for the reason of using stochastic routing. As is well known, almost traditional routing algorithms, e.g. those used on the Internet, are deterministic. As they are tailored to be efficient, one can guess the path that will be taken with a high probability even though there are an almost infinite number of paths connecting two points on the network. On our key transmission method above, such routing algorithms compromise security. By contrast, stochastic routing is better: each message takes independently a random path and Eve is confused in choosing the path to be attacked.

We state our problem in this framework: if Alice uses a stochastic routing algorithm to send messages, then how many messages Alice must send so that at least one message is not intercepted? More precisely: *Given an arbitrarily small real number ϵ, find N_0 such that if Alice uses a stochastic routing algorithm to send $N \geq N_0$ messages, then we have the probability $(1-\epsilon)$ that it exists at least one message not being intercepted by Eve?*

3 The proposed Solution

A *safe path* is a path that only consists of safe nodes. Otherwise, it is said *unsafe*. Obviously, if there is no safe path from Alice to Bob then there is no solution. We first find the existence condition for solution. Percolation theory helps address this question in 3.1. Then, we present our stochastic routing algorithms and its primary results in 3.2. We use our algorithm to answer to the initial question in 3.3.

3.1 Percolation theory

Suppose we immerse a large porous stone in a bucket of water. What is the probability that the center of the stone is wetted? In formulating such a situation, John M. Hammersley and Simon R. Broadbent, in 1957, gave birth to the percolation theory [8].

In 2 dimensions, percolation model can be described as follows. We focus on a regular graph $G = \mathbb{Z}^2$, with vertex set V and edge set E. Let the vertices be independently *open* with probability $p \in [0, 1]$. All the edges are assumed open. Consider a path π in G as a sequence $\pi = v_1, v_2, \ldots$ of adjacent vertices. A path *open* iff all the vertices v_i are open. Obviously, the central vertex of the stone is wetted iff there is a open path from it to a vertex on the boundary.

The goal of percolation theory is to describe the transition phase from non-existence to existence of a infinite wetted vertex cluster. The existence of an infinite wetted cluster is equivalent to having an unbounded open path starting from the origin. We denote by $u \leftrightarrow v$ the existence of an open path between two vertices $u, v \in V$. The *wetted cluster* or *open cluster* $C(v)$ of the vertex v is defined as $C(v) = \{u \in V : u \leftrightarrow v\}$.

The central quantity studied in percolation model is the probability that the cardinality of $C(v)$ is infinite for a vertex v, also called the *percolation probability* $\theta(p) = \{\Pr\Big(|C(v)| = \infty\Big)\}$.

Perhaps, the most important result of percolation theory is to well define a critical value of p, also called percolation threshold or critical probability p_c, that separates the globally disconnected and globally connected states for the unbounded lattice (see Fig. 2).It is defined by $p_c = \max\{p : \theta(p) = 0\}$.

Nowadays, there are many variant of the basic percolation model. One studied the percolation in a number of various structures and dimensions. Results were presented as a mixture of rigorous results, numerical estimates and conjectures. However, its polyvalence and efficiency in characterizing non-linear phenomena led the scientific community to use this theory to model complex systems such as biological systems, social networks and economic systems.

In this paper, we focus on the 2-dimensional site percolation as sketched above. Note that if we restrict our attention only on the existence of a safe path from Alice and Bob, then there is no difference between our framework and percolation model: safe nodes and safe paths are equivalent with open nodes and open paths, respectively. Thus, we could use some important properties that have been proven in percolation [9]:

1. The probability that a node belongs to the infinite wetted or open cluster, or percolation probability $\theta(p)$, is a non-decreasing and continuous function with respect to p, except possibly at the percolation threshold p_c, where it is at least non-decreasing and continuous from the right (see Fig. 2).
2. The number of infinite wetted or open clusters k_0 must take no other value than 0 or 1: $k_0 = 1$ if $\theta(p) > 0$, 0 otherwise.

The fundamental goal of quantum network is to find a more higher security level. Situations that lead to a small probability of having at least one safe path should be taken out of interest. We should focus only on the values of p in the region where $\theta(p)$ is equal or almost equal to 1 (see Fig. 2). For such p, Alice and Bob belong almost certainly to the infinite safe cluster. This implies there exists almost certainly at least a safe path between them. The probability τ(Alice,Bob) that Alice and Bob can be safely connected is $\tau(\text{Alice,Bob}) = (\theta(p))^2$.

We have the following idea on the lower bound p_0 for the interesting region of p : $p_0 = \inf\{p : (\theta(p))^2 \geq (1 - \epsilon)\}$. As $\epsilon \to 0$, we have $p_0 \to p_0'$ where $p_0' = \inf\{p : \theta(p) = 1\}$. The threshold $p_c \sim 0.6$ for 2-dimensional site square lattice percolation is obtained by numerical estimates. Motivated by this idea, we did simulations [10] that show some critical threshold in our quantum network problem. In this paper, we want to re-use one of them, this is $p_0 = p_0' \sim 0.91$.

3.2 Stochastic routing algorithms

Introduction to stochastic routing algorithms Traditional routing algorithms, such as those used on the Internet, are mostly deterministic. As they are tailored to be efficient, they are guessable. This is not good in our framework. The basic idea of stochastic routings is sending randomly a packet to one of possible paths. When a node needs to forward a packet, it randomly chooses one of its neighbors, not necessarily the most "efficient" one. This makes the emergence

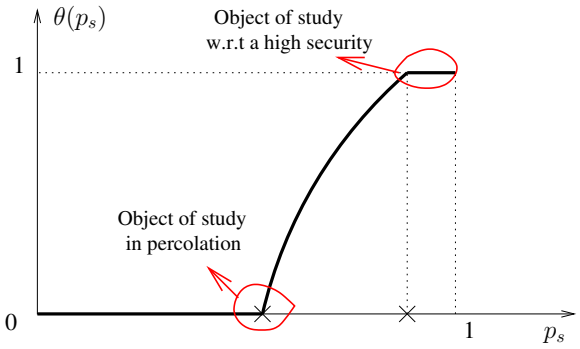

Fig. 2. Two different objects of study

of a new concept called next-hop probability distribution: the next-hop choice is random, but according to the next-hop probability distribution. The main challenge in stochastic routing is how to determine the next-hop probabilities that could maximize a given specific goal. In quantum networks, the top priority is the security and the other metrics for performance evaluation of routing algorithms are less considered.

A constant-length stochastic routing algorithm. Called L-SRA(l), it is a stochastic routing algorithm that takes l as input and tries to transmit a message using random path of length l. If l is less than the distance d between Alice and Bob then L-SRA(l) returns no path. For $l \geq d$,there can be different paths $\pi_1, \ldots, \pi_m$. In such cases, for each message, L-SRA(l) will choose randomly a path π_i among $\pi_1, \ldots, \pi_m$ according to a probability distribution that holds:

1. $\forall i, 1 \leq i \leq m, 0 \leq Pr(\text{L-SRA(l) takes } \pi_i) \leq 1$
2. $\sum_{i=1}^{m} Pr(\text{L-SRA(l) takes } \pi_i) = 1$

Theorem 1. The probability that L-SRA(l) chooses successfully a safe path to send one message depends only on the safe probability p and the length l, not on the distance d between Alice and Bob:

$$Pr(1, p, d, \text{L-SRA(l)}) = p^l \tag{1}$$

A proposed routing algorithm. Called K-SRA(k), it is built based on L-SRA(l). K-SRA(k) receives an input value $k \geq 2$, and considers only the paths with lengths $d, (d+1), \ldots, (k * d - 1)$. For each message, K-SRA(k) chooses randomly a value l among $d, (d+1), \ldots, (k * d - 1)$ according to a uniform distribution. Once l was chosen, K-SRA(k) uses L-SRA(l) to send the message.

Theorem 2. The probability that K-SRA(k) chooses successfully a safe path to send one message depends on the safe probability p, the input parameter k and the distance d between Alice and Bob:

$$\beta = Pr(1, p, d, \text{K-SRA(k)}) = \frac{p^d * (1 - p^{(k-1)*d})}{(k-1) * d * (1-p)} \tag{2}$$

3.3 Some attack strategies of Eve

We consider 2 strategies of Eve:

1. *Dynamic attack*. Frequently, Eve re-chooses the set of attacked nodes.
2. *Static attack*. Eve chooses once for all the set of attacked nodes.

Theorem 3. If Eve does a dynamic attack, then the probability that there is at least one safe path in N routings of K-SRA(k) depends on N, the safe probability p, the input parameter k, and the distance d between Alice and Bob:

$$Pr(N, p, d, \text{K-SRA(k)}) = 1 - (1 - \beta)^N \tag{3}$$

where β is evaluated in the formula 2.

Lemma 1. If Eve executes a dynamic attack, given ϵ and K-SRA(k), then we have the threshold N_0 responding for the initial question:

$$N_0 = \lg(\epsilon)/(1 - \lg(\beta)) \tag{4}$$

where β is evaluated in the formula 2.

Theorem 4: If Eve does a static attack, then the upper bound of the probability that there is at least one safe path in N routings of K-SRA(k) depends on N, the safe probability p, the input parameter k, and the distance d between Alice and Bob:

$$Pr(N, p, d, \text{K-SRA(k)}) \leq 1 - (1 - \beta)^N \tag{5}$$

where β is evaluated in the formula 2. And the equality is possible when $N \leq 4$.

Lemma 2: If Eve executes a static attack, given ϵ and K-SRA(k), we have the threshold N_0 responding for the initial question:

$$N \geq \lg(\epsilon)/(1 - \lg(\beta)) \tag{6}$$

where β is evaluated in the formula 2. And the equality is possible when $N \leq 4$.

4 Other work

Percolation theory. The context of percolation theory has many similarities with our problem context. The significant method used to solve percolation problems is simulations and statistics that report the percolation probability and an approximate formula that describes the system state at the phase transition. In this paper, our ambition is not to find approximate formulas that describe the evolution of a certain process. In contrast, it is to feature a quantum network framework based percolation, and beyond it to find solutions for security problem. The rigorous thresholds, formulas featuring the region of interest for p (see Fig. 2) is one of our future works.

Stochastic routing. The main challenge in stochastic routings is how to compute the next-hop probabilities that maximize a given goal. In literature [11,12], stochastic routing can be re-formalized as an abstract game between two players: the designer of the routing algorithm and the attacker that attempts to intercept packets. It is assumed that the attacker has a finite resource, i.e. she only intercepts packets at some nodes on the network. This is a zero-sum game in which a designer seeks a strategy to minimize the cost that he has to pay for a packet being safely transmitted and the attacker wants to maximize this cost. Such a problem was studied in [12].

Previous works on stochastic routing focus on performance metrics (latency, throughput, acceptance rate, etc.), which are not of major importance to quantum networks. What matters is sensitivity to eavesdropping and security. As the main goal of our works is to investigate the possibility of achieving an extremely high security level, the object of study is also different: this is the overall state of a set N paths. One grid 4-connected topology as proposed in this paper can suit to quantum network, but also makes previous works on stochastic routing become useless.

Quantum network. The first quantum network, DARPA Quantum Network, was built to test the strength of such systems in the real-world applications. It consists of three sites (Cambridge, Harvard, and Boston University) and became fully operational in October 2003 [13]. It relies on trusted relays: one must trust the security of all the participants, and be sure that eavesdroppers cannot sniff any information on any of the nodes. In realistic contexts, nobody can be sure that he does not reveal any information for eavesdroppers. Moreover, in a larger quantum network, the assumption that one can trust all the nodes becomes unacceptable. In this paper, we studied large quantum networks in a more realistic context: nodes are not totally trustworthy, there is a probability that nodes are controlled by eavesdroppers.

5 Conclusions

We investigated the constraints of quantum networks and the ineluctable probability that some nodes are attacked. The existence condition of an extreme high security level for key transmission was analyzed using percolation-theory based methods. We proposed also an adaptive stochastic routing and gave the idea about the number of messages necessary to be sent for obtaining a given coefficient security ϵ.

Much remains to be done. Studying more general topologies is of primary importance: grids are only the first stab. The node safety-probability might also vary between regions. Finding formulas (explicit or implicit via equations) is also of interest, as they usually provide more revealing results than simulations do. Finally, we will also work to improve our stochastic routing proposal.

6 Appendix

Proof of theorem 1.

$$\begin{aligned}
Pr\big(1,p,d,\text{L-SRA(l)}\big) &= \sum_{i=1}^{k} \Big(Pr\big(\text{L-SRA(l) takes } \pi_i\big) \times Pr(\pi_i \text{ is safe}|\pi_i \text{ was taken})\Big) \\
&= \sum_{i=1}^{k} \Big(Pr\big(\text{L-SRA(l) takes } \pi_i\big) * Pr(\pi_i \text{ is safe})\Big) \\
&= \sum_{i=1}^{k} \Big(Pr\big(\text{L-SRA(l) takes } \pi_i\big) * (p^l)\Big) \\
&= \Big(\sum_{i=1}^{k} \Big(Pr\big(\text{L-SRA(l) takes } \pi_i\big)\Big)\Big) * (p^l) \\
&= 1 * (p^l) = p^l
\end{aligned}$$

Proof of theorem 2.

$$\begin{aligned}
\beta = Pr\big(1,p,d,\text{K-SRA(k)}\big) = \sum_{l=d}^{k*d-1} \Big(&Pr\big(\text{K-SRA(k) takes } l\big) \times \\
&Pr\big(\text{L-SRA(l) takes a safe path}\big)\Big) \\
= \sum_{l=d}^{k*d-1} &\Big(\frac{1}{(k-1)*d} * \Big(Pr\big(1,p,d,\text{L-SRA(l)}\big)\Big)\Big) \\
= \frac{1}{(k-1)*d} * &\Big(\sum_{l=d}^{k*d-1} \Big(Pr\big(1,p,d,\text{L-SRA(l)}\big)\Big)\Big) \\
= \frac{1}{(k-1)*d} * &\Big(\sum_{l=d}^{k*d-1} \big(p^{(l)}\big)\Big) \\
= \frac{1}{(k-1)*d} * &\big((p^d) * (1 + p + \ldots + p^{(k-1)*d-1})\big) \\
= \frac{1}{(k-1)*d} * &\ p^d * \big(\frac{1-p^{(k-1)*d}}{(1-p)}\big) = \frac{p^d * (1-p^{(k-1)*d})}{(k-1)*d*(1-p)}
\end{aligned}$$

Proof of theorem 3. Once time a message has been sent, Eve re-chooses the set of attacked nodes. This makes the context become a memoryless system. Consider each time SRA(k) sends a message as a trial. Such a trial is called success if the message sent is not intercepted by Eve. We are interested in the probability that it exists at least a trial success in a chain of N trials. Because the system is memoryless, and by Equation 2, we have:

$$Pr(\text{All the N trials are failed}) = \Big(1 - Pr(\text{A trial is successful})\Big)^N = (1-\beta)^N$$

Clearly:

$$\begin{aligned} Pr(N, p, d, \text{K-SRA(k)}) &= Pr(\text{At least one of N trials is successful}) \\ &= 1 - Pr(\text{All the N trials are failed}) \\ &= 1 - (1-\beta)^N \end{aligned}$$

Proof of theorem 4. In the case that Eve keeps the set of attacked nodes until all the N messages have been sent, we must take into account relation between the paths taken by N messages sent. We first consider to the probability that K-SRA(k) takes an unsafe path for each trial:

$$\begin{aligned} \overline{Pr(1, p, d, \text{K-SRA(k)})} = &\sum_{l=d}^{k*d-1} \Big(Pr\big(\text{K-SRA(k) takes } l\big) \times \\ &\qquad Pr\big(\text{L-SRA(l) takes an unsafe path}\big)\Big) \\ = &\ 1 - \beta \end{aligned} \tag{7}$$

Now, we consider to the probability that all the N messages are intercepted.

$$\begin{aligned} &\overline{Pr(N, p, d, \text{K-SRA(k)})} \\ &= \sum_{\substack{d \le l_1 < k*d \\ \cdots \\ d \le l_N < k*d)}} \Bigg(Pr\big(\text{K-SRA(k) takes } (l_1, \ldots, l_N)\big) \times \\ &\qquad \Bigg(\sum_{\substack{l_{\pi_1} = l_1, \\ \cdots \\ l_{\pi_N} = l_N}} \Big(Pr(l\text{-SRA takes } \pi_1 \ldots \pi_N) \times \\ &\qquad\qquad \big(Pr(\pi_1 \ldots \pi_N \text{ are failed})\big)\Big)\Bigg)\Bigg) \end{aligned} \tag{8}$$

Note that with a given set $(\pi_1, \ldots, \pi_N)$, we have the following inequation:

$$Pr(\pi_1, \ldots, \pi_N \text{ are failed}) \ge \prod_{i=1}^{N} Pr(\pi_i \text{ is failed}) \tag{9}$$

The equality holds iif $(\pi_1, \ldots, \pi_N)$ are independents. We first prove with $N = 2$. Assume that π_1, π_2 have the length l_1, l_2 respectively, and have l common node $(0 \le l \le \min(l_1, l_2))$. We have:

$$
\begin{aligned}
Pr(\pi_1, \pi_2 \text{ are failed}) &= p^l * (1 - p^{(l_1 - l)}) * (1 - p^{(l_2 - l)}) + (1 - p^l) \\
&= (1 - p^{(l_1)} - p^{(l_2)} + p^{(l_1 + l_2)}) + (p^{(l_1 + l_2 - l)} - p^{(l_1 + l_2)}) \\
&= (1 - p^{(l_1)}) * (1 - p^{(l_2)}) + (p^{(l_1 + l_2 - l)} - p^{(l_1 + l_2)}) \\
&\geq (1 - p^{(l_1)}) * (1 - p^{(l_2)}) \text{ (equality iif } l = 0)
\end{aligned}
$$

On the other hand:

$$
Pr(\pi_1 \text{ is failed}) * Pr(\pi_2 \text{ is failed}) = (1 - p^{(l_1)}) * (1 - p^{(l_2)})
$$

So, the inequation (9) is proven with $N = 2$. We iterate this to obtain the inequation (9) for $\forall N$. Note that the equality holds iif $\pi_1 \dots \pi_N$ are separated, and in the square 4-connected lattice, there are maximum 4 separated paths between Alice and Bob. Thus, if $N > 4$, the equality for the inequation (9) cannot appear. Applying Inequation (9) to Equation (8), we have:

$$
\begin{aligned}
&\overline{Pr(N, p, d, \text{K-SRA(k)})} \\
&> \sum_{\substack{d \leq l_1 < k*d \\ \cdots \\ d \leq l_N < k*d)}} \Big(\Big(\prod_{i=1}^{N} Pr\big(\text{K-SRA(k) takes } l_i\big) \Big) \times \\
&\qquad \Big(\sum_{\substack{l_{\pi_1} = l_1, \\ \cdots \\ l_{\pi_N} = l_N}} \big(\prod_{i=1}^{N} Pr(l\text{-SRA takes } \pi_i) \big) \times \\
&\qquad\qquad \big(\prod_{i=1}^{N} Pr(\pi_i \text{ is failed}) \big) \Big) \Big) \\
&= \sum_{\substack{d \leq l_1 < k*d \\ \cdots \\ d \leq l_N < k*d)}} \Big(\Big(\prod_{i=1}^{N} Pr\big(\text{K-SRA(k) takes } l_i\big) \Big) \times \\
&\quad \Big(\prod_{l_j = l_1}^{l_N} \Big(\sum_{l_{\pi_i} = l_j} \big(Pr(l\text{-SRA takes } \pi_i) * Pr(\pi_i \text{ is failed}) \big) \Big) \Big) \Big) \\
&= \sum_{\substack{d \leq l_1 < k*d \\ \cdots \\ d \leq l_N < k*d)}} \Big(\Big(\prod_{i=1}^{N} Pr\big(\text{K-SRA(k) takes } l_i\big) \Big) \times \\
&\quad \Big(\prod_{l_j = l_1}^{l_N} Pr\big(l\text{-SRA}(l_j) \text{ takes an unsafe path}\big) \Big) \Big) \\
&= \sum_{\substack{d \leq l_1 < k*d \\ \cdots \\ d \leq l_N < k*d)}} \Big(\Big(\prod_{i=1}^{N} Pr\big(\text{K-SRA(k) takes } l_i\big) \times \\
&\quad Pr\big(l\text{-SRA}(l_j) \text{ takes an unsafe path}\big) \Big) \Big) \\
&= \prod_{i=1}^{N} \Big(\Big(\sum_{d \leq l_i < k*d} Pr\big(\text{K-SRA(k) takes } l_i\big) \times \\
&\quad Pr\big(l\text{-SRA}(l_i) \text{ takes an unsafe path}\big) \Big) \Big) \\
&= \prod_{i=1}^{N} \Big(Pr\big(\text{K-SRA(k) takes an unsafe path}\big) \Big) \\
&= (1 - \beta)^N \text{ (from Equation 7)}
\end{aligned}
$$

Thus:

$$Pr(N, p, d, \text{K-SRA(k)}) = 1 - \overline{Pr(N, p, d, \text{K-SRA(k)})} = 1 - (1 - \beta)^N$$

References

1. Elliott, C., Pearson, D., Troxel, G.: Quantum cryptography in practice. In: Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany (2003)
2. Kimura, T., Nambu, Y., Hatanaka, T., Tomita, A., Kosaka, H., Nakamura, K.: Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography criterion. Jap. J. of Appl. Phy. **43** (2004)
3. HQNET: High bit-rate and versatile quantum-secured networks. In: http://hqnet.enst.fr, Paris, France (2007)
4. Bellot, P., Gallion, P., Guilley, S., Danger, J.L.: Visq, voice on ip with quantum safety. In: http://visq.enst.fr, Paris, France (2006)
5. Bennett, C., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proc. of IEEE Int. Conf. on Computers, Systems, and Signal, Bangalore, India (1984)
6. Shor, P., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85** (2000)
7. Shannon, C.: Communication theory of secrecy of systems. Bell System Technical Journal (1949)
8. Grimmett, G.: Percolation. Second edn. Springer-Verlag (1999)
9. Hughes, B.D.: Random walks and random environments. Volume 2. Oxford University Press (1995)
10. Le, Q.C., Bellot, P., Demaille, A.: Stochastic Routing in Large Grid Shaped Quantum Networks. In: Proc. of the 5th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Futur, Vietnam (2007)
11. Bohacek, S., Hespanha, J.P., Obraczka, K.: Saddle policies for secure routing in communication networks. In: Proc. of the 41st IEEE Conf. on Decision and Control. (2002)
12. Bohacek, S., Hespanha, J.P., Obraczka, K., Lee, J., Lim, C.: Enhancing security via stochastic routing. In: Proc. 11th Int. Conf. on Computer Communication and Networks. (2002)
13. Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., Yeh, H.: Current status of the DARPA quantum network. (2005)