Quantum network security dependent on the connection density between trusted nodes

ANDREI GAIDASH,1,2,3,4 GEORGE MIROSNICHENKO,5,6 AND ANTON KOZUBOV1,2,3,4,*

1Department of Mathematical Methods for Quantum Technologies, Steklov Mathematical Institute of the Russian Academy of Sciences, 119991, 8 Gubkina Street, Moscow, Russia
2Laboratory of Quantum Processes and Measurements, ITMO University, 199034, 3b Kadetskaya Line, Saint Petersburg, Russia
3Leading Research Center “National Center for Quantum Internet,” ITMO University, 197101, 49 Kronverksky Prospekt, Saint Petersburg, Russia
4SMARTS-Quanttelecom LLC, 199178, 59-1-B 6th Line of Vasilievsky Island, Saint Petersburg, Russia
5Waveguide Photonics Research Center, ITMO University, 197101, 49 Kronverksky Prospekt, Saint Petersburg, Russia
6Institute “High School of Engineering,” ITMO University, 197101, 49 Kronverksky Prospekt, Saint Petersburg, Russia
*Corresponding author: avkozubov@itmo.ru

Received 3 March 2022; revised 28 September 2022; accepted 4 October 2022; published 26 October 2022

Besides true quantum repeaters, a trusted node paradigm seems to be inevitable for practical implementations (at least in the short term), and one should consider configurations of trusted nodes as the basis for global quantum networks. In this paper, we estimate how the introduction of additional connections between trusted nodes through one, two, etc., nodes (i.e., connection density) to a quantum network with serial connections of trusted nodes affects its security. We provide proper scaling of the failure probability of authentication and quantum key distribution protocols to the level of the whole quantum network. Expressions of the failure probability dependent on the total number of connected nodes between users and the connection density for the given mean failure probability of each element are derived. The result provides an explicit trade-off between an increase of key transport security and a consequent increase of spent resources. We believe that the obtained result may be useful for both the design of future networks and optimization of existing ones.

https://doi.org/10.1364/JOCN.457492

1. INTRODUCTION

Quantum key distribution (QKD) [1] is one of the most rapidly developing areas of modern science. A crucial advantage of the technology is that the security of a private message transfer by quantumly distributed keys is based on the laws of quantum physics and not on particular mathematical algorithms; the latter can be hacked in principle, while one cannot trick the fundamental laws of physics. Developing the technology of QKD can be considered as a basis for future global secure data transmission networks. The first steps towards the construction of quantum networks were presented in [2–10]. Various network topologies were proposed and analyzed recently as well as key transport schemes and their security estimation [11–21]. However, the fundamental limitation on the distance between two neighboring nodes forces the development of widespread quantum networks that cover big areas or elongated backbone networks that connect cities and countries.

Generally speaking, there are two possible types of networks: with trusted and untrusted nodes. Untrusted nodes are usually based on some kind of quantum repeater [22–25], requiring quantum memory; for both, it is hard to achieve the necessary performance due to the current state of the technology. Nevertheless, deep theoretical research in this area can be found in [26–28]. However, there are special cases when only one untrusted node is available, and one may utilize measurement-device-independent (MDI) [29–37] QKD protocols (however, we should mention that this is not the motivation for MDI). As an alternative to a single-photon approach, the first realization of twin-field (TF) QKD schemes with coherent states was proposed in [38], which makes it possible to overcome the well-known fundamental limit of repeaterless quantum communications, i.e., the secret key capacity of the lossy communication channel [39] (also known as the Pirandola–Laurenza–Ottaviani–Banchi bound) [39,40]. Moreover, several new approaches for realization of the TF QKD protocol were proposed in [41–45], as well as a multiple user variant of TF-like QKD [46]. However, even those implementations of multiple user variants of MDI or TF QKD systems (similar to star network topology with untrusted nodes in the center) are combined in a widespread network by trusted nodes, for instance, see Fig. 1 in [35]. So besides true quantum repeaters, a trusted node paradigm seems to be inevitable, and one should consider configurations of trusted nodes and connections between them to estimate how probabilistic properties
of each node are transferred to the level of the whole network, e.g., the most desired one is the security properties of networks and their key transport protocols.

The aim of this paper is to estimate how the introduction of new connections to widely used serial connections (or the increase of the connection density between trusted nodes in the global quantum network in the future) affects the security of quantum networks. In [11,12], a limited amount of compromised nodes is considered; in turn, our model may take into account any fraction of compromised nodes. Our network segment configuration (meaning that we may consider a chosen end-to-end path within a wider network) and eavesdropping model are similar to the one presented in [13]. However, in our approach, we do not monitor the presence of the eavesdropper in nodes by dropping out any of the relays. One of the purposes of the approach is to estimate the mean probability of successful key transfer considering any possible configuration of compromised nodes and intercepted QKD links. Thus in this paper, we demonstrate the appropriate key transfer technique and the general method for estimation of its successful implementation probability.

This paper is organized as follows. Section 2 describes the topology of considered network segments and the key transfer protocol in detail. In Section 3, we provide an explicit description of the network security and its estimation. In Section 4, we discuss the obtained results.

2. CONFIGURATION AND KEY TRANSPORT PROTOCOL

In this paper, we consider a segment of a quantum network that connects two users within it (see Fig. 1). Consider that part of a network contains $N$ nodes at least serially connected to each other and may have additional connections through one, two, and up to $c - 1$ nodes (see Fig. 2, for example); also, the total number of connections that require QKD links is $c(N - c + 1)$. We denote in the figures QKD links with dashed gray double-sided arrows (without specifying their type, e.g., see Fig. 3) and key transport links by any open classical channel (OCC) with black solid unidirectional arrows.

Keys are distributed quantumly between each pair of connected nodes. We assume that the utilized QKD protocol is $\varepsilon$-secure, e.g., [47]. Classical data encrypted by quantumly distributed keys are transferred in one direction (at least for a current session). The latter may be explicitly described by adjacency matrix $A$, which is a matrix with one at $k$-diagonals for $1 \leq k \leq c$ and zero elsewhere. This configuration describes unidirectional connections between neighboring nodes and up to $c - 1$ nodes. The considered straightforward configuration of the network implies a rather simple analysis and the presence of useful properties. Also, we believe that in principle, properties of more complicated adjacency matrix configurations may be investigated by perturbation theory or other methods. However, there is a high chance that particular segments in networks with dense node distribution can be described by adjacency matrix $A$ with symmetric properties, as noted earlier.

In particular, the total number of routes for key transport between users in a certain session is $F_N^{(c)}$, where the latter is the $N$th $c$-anacci number (see Fig. 4, for example). Thus one may apply this property to construct a key transport protocol similar to [13,15]. Each route is assigned to transfer one of the keys $K_i$, where $1 \leq i \leq F_N^{(c)}$ (see Figs. 4 and 5). Quantumly distributed keys are used to transfer several $K_i$ with routing instructions as encrypted messages between nodes. Then the final key is $K = \oplus_i K_i$, where $\oplus$ is a bitwise XOR operation. This method of key transport guarantees that compromising one node does not reveal the transferred key to an adversary (for $c > 1$). See Appendix A, where a simple example of how the key transport protocol works is considered. It should be noted that the number of routes $F_N^{(c)}$ for a large amount of nodes becomes enormous. This should be kept in mind, and one may change the routing scheme (e.g., decrease the amount of routes to a certain degree). However, it makes analysis intricate, and this discussion is beyond the scope of the paper.

Fig. 1. Visualization of a particular segment of a widespread quantum network. Circles are trusted nodes, dashed gray arrows are QKD connections between them (it should be noted that there may be untrusted nodes in between that are not shown in the figure, but are shown in Fig. 3), and black solid arrows are unidirectional key transport by any open classical channel. Key transport is organized between gray-shaded nodes for a certain session.

Fig. 2. Visualization of a quantum key distribution network segment (for a given key transport session between two gray-shaded nodes) with different amounts of additional connections, i.e., connection density. One may view the increase of connection as an increased density of nodes and connections in the global quantum network. Circles are trusted nodes, dashed gray arrows are QKD connections between them, and black solid arrows are unidirectional key transport by any OCC. A case with $N=9$ is considered as an example. (a) Typical serial connection, $c = 1$. (b) Serial connection and additional connection through one node, $c = 2$. (c) Serial connection and additional connection through one and two nodes, $c = 3$. 

Authentication protocols with failure probability $\varepsilon_{\text{auth}}$ are implemented to ensure that each node is trusted before QKD sessions; a pool of preshared keys is used for this purpose, and it is updated with a part of quantumly distributed keys. It should be noted that the authentication problem can be considered separately from the QKD problem and then combined by the composition principle [48]; thus we are eligible to assume some $\varepsilon_{\text{qkd}}$-security of the QKD protocol and do not consider it in detail. The described key transport protocol succeeds if there is at least one route from the first node to the last one that goes only through authorized trusted nodes.

### 3. KEY TRANSPORT SECURITY PROBLEM

In consideration of QKD network performance, we utilize the following assumptions.

1. Nodes are assumed to be trusted. The authentication protocol is assumed to work properly and fail with at most $\varepsilon_{\text{auth}}$ probabilities for each node. All nodes are attacked separately and simultaneously every key transport session.
2. QKD links are assumed to be of any kind (via optical fiber, free space, point-to-point connection, or with untrusted nodes in between, e.g., see Fig. 3) and to work properly between all nodes, and each link independently should be $\varepsilon_{\text{qkd}}$-secure (for the sake of simplicity, we consider them to be the same for each link.). All QKD links are attacked separately and simultaneously every key transport session.
3. The distance between two neighboring nodes is less than the limiting one. The distance between the most distant directly connected (through $c - 1$) nodes should be considered as the limiting one.

The problems one faces in QKD network security estimation are similar to the problems in point-to-point QKD links. Thus one has to deal with both attacks on authentication of nodes and the QKD protocol for every link. Basically, failure probabilities of an authentication protocol ($\varepsilon_{\text{auth}}$) and a QKD protocol ($\varepsilon_{\text{qkd}}$) can be considered separately according to the composition principle [48]. However, regarding network implementation, we should correctly scale both notations considering certain restrictions.

Moreover, we should clarify one more feasible concern. Since we transmit via the open channel the same encrypted quantum key $k_{pq}$ messages $K_i$ several times in the case of improper realization, it may lead to potential vulnerability. It is well known that for natural languages using a constant repeating key (in our case, the message), a simple XOR cipher can trivially be broken using frequency analysis. However, there can be two possible solutions for this problem. The first and the simplest is to utilize a hash function to our message $K_i$ to shuffle the bits before XOR ciphering. The second one is more discussable. Since we are free to construct messages according to our will, let us introduce some basic rules. To remove any correlations inherent in natural languages, bit strings corresponding to the messages $K_i$ should be constructed using random numbers and hold the uniform distribution property.
A. Authentication Scaling Problem

There is a possibility of a “man-in-the-middle” attack, basically, an attack on the authentication protocol, when an eavesdropper fully duplicates one of the nodes and acts like it, and neighboring nodes do not suspect anything. Then, after QKD between each pair of nodes (including compromised nodes), at the moment when key transport with trusted nodes is performed, the compromised node can obtain transfer through its information. Basically, it is the attack on a classical key transport (with quantumly distributed keys) scheme and not on the QKD “part” of the network. To maximize the amount of compromised nodes, an eavesdropper should attack simultaneously all trusted nodes in a certain segment. The condition of the successful attack is to compromise at least \( c \) nodes in a row (by the order of nodes in the longest path). This condition follows from the topology of a network, since if \( c \) nodes in a row are compromised, there is no possible route between the first and last nodes that can be constructed. Then all \( K_i \) can be known by the eavesdropper. It also should be mentioned that the eavesdropper cannot keep the compromised node because knowledge of the preshared key is required. The eavesdropper may attempt a new attack at the beginning of each session.

One may consider the full problem as solved in Appendices B–D. Alternatively, another way is consideration of an approximated solution (i.e., the lowest order term, which works well with low probabilities) as follows: the lowest amount of compromised nodes for a successful attack is \( c \), and there are \( N - c - 1 \) possible configurations to be located in a row within \( N - 2 \) nodes (we do not consider compromising the first and last nodes). Here and further, we assume that \( N \) and \( c \) can take any value with only the condition \( c \leq N - 2 \). Then it is straightforward that the overall probability of a successful attack on the authentication protocol is as follows:

\[
e_{a} \approx (N - c - 1) (e_{auth})^c.
\]

The latter approximation is reasonable for small \( e_{auth} \leq \left( \frac{1}{N-c-1} \right)^2 \), which can be easily satisfied.

B. QKD Security Scaling Problem

To estimate network security, one should also consider simultaneous attacks on all QKD links that may provide transferred keys to an adversary. In some sense, this problem is closely related to the min-cut problem [49] in graph theory. The general idea of the considered problem is to find the minimum number of links that need to be cut to divide the graph into two parts. The method basis is quite similar to the one utilized in the previous subsection. To provide a successful attack, one should intercept all incoming or outgoing links from \( c \) nodes in a row. However, in the case of link interception, this amount, \( a \), can be optimized. Figure 6(c) illustrates non-degenerate min-cut for the case of \( c = 3 \). However, in the case of security notation, this amount is not the optimal one. The main reason is the chosen key transport protocol, which leads to the degeneration of the necessary amount when approaching the extreme nodes as shown in Fig. 6. Thus the amount of links for min-cut lies inside the following interval:

\[
e \leq a \leq \left( \frac{c + 1}{2} \right).
\]

Since we are talking about a worst case scenario, we utilize the lowest order term approximation. An adversary needs to intercept a quantum key at certain links in a way that all \( K_i \) are transferred by those links, e.g., see Fig. 5. It is obvious that the least amount of links that transfer all \( K_i \) are those connected to the first or last node; in either case, there are \( c \) links (higher terms are at least of order \( c + 1 \)). Hence a successful attack on QKD links can be performed with the following probability:

\[
e_{2} \approx 2(e_{qkd})^c.
\]

This approximation is reasonable for \( c > 1 \) and \( e_{qkd} \leq \left( \frac{1}{2} \right)^{\frac{1}{c}} \), which can be easily satisfied. It should be noted that specifically in the case of \( c = 1 \), the latter expression is \( e_{2} = (N - 1) \cdot e_{qkd} \).

In general, for every \( c \) and \( N > c + 2 \), there will be only two options to eavesdrop all \( K_i \): intercept all links outgoing from the first node or all links incoming to the last node. However, it should be mentioned that there is only one exception to this consideration. It is related to the limiting case of the minimal necessary amount of nodes, \( N = c + 2 \), for every number of serial connections \( c \), i.e., \( c = 2 \), \( N = 4 \). The explanation is pretty simple. In the limiting case, there is always a direct connection between the second and last nodes, which leads to additional eavesdropping possibilities. This increases the number of combinations for successful interception of \( c \) links, and thus the failure probability should be considered as \( e \approx (c + 1)(e_{qkd})^c \).

C. Quantum Network Security

The main result of our paper is the security notation for arbitrary configurations of quantum networks utilizing the described key transport protocol. Following the composition principle, we should bound the failure probability of a quantum network \( (e_{qu}) \) by the scaled failure probabilities of authentication \( (e_{a}) \) and QKD protocols \( (e_{2}) \) using the following expression:

\[
e_{qu} = e_{a} + e_{2} \approx (N - c - 1)(e_{auth})^c + 2(e_{qkd})^c.
\]
4. RESULTS AND DISCUSSION

Obtained results can be applied to two different scenarios. On one hand, one may consider obtained results regarding the current state of the art. Quantum networks are in the early stages of development, so one can design their configurations dependent on different purposes. As shown in Eqs. (1) and (3), introduction of additional connections reduces the probabilities of attacks as the power function \( \varepsilon_{\text{auth}} \rightarrow (\varepsilon_{\text{auth}})^{\gamma} \) and \( \varepsilon_{\text{eqd}} \rightarrow (\varepsilon_{\text{eqd}})^{\gamma} \). However, at the same time, requirements for the maximal allowed QKD losses in the quantum channel are increased \( (\eta \rightarrow \eta^\gamma) \) or a number of nodes per maximal allowed distance is increased \( \epsilon \) times (the cost of \( N \) nodes \( \rightarrow \) the cost of \( N \cdot \epsilon \) nodes), and the total number of edges \( (\text{i.e., number of QKD connections}) \) is increased as well \( (N - 1 \rightarrow \epsilon (N - \frac{\epsilon + 1}{2})) \). At the same time, one should avoid an enormous number of routes in the key transport scheme or be able to provide fast enough data transfer rates. The security of the quantum network is a priority; however, one should make the decision about the latter multivariable trade-off. The result provides simple dependencies on the \( \epsilon \) parameter (where it can be considered as the density of connections in the network) to make analysis of the trade-off as easy as possible. Thus one can set the topology (and optimize the cost) of the network at the stage of its design to achieve necessary security.

On the other hand, we may consider obtained results regarding a future global quantum network where there is already dense trusted node distribution within it. In this case, one may utilize obtained results to adjust parameters of particular key transport sessions considering the necessary security provided by minimal spent resources. More specifically, if universal hash functions \([50]\) are used to authenticate users, then the probability of nodes to be compromised is of the order of hash function collision, i.e., \( 2^{-n/2} \), where \( n \) is the length of the hash output (and in the case of a permutation-only hash, it is also the length of the input). Then according to Eq. (1), the hash output (or input) length may be reduced by a factor of \( \epsilon \log_{N-2}(N - \epsilon - 1) \), while we preserve overall security. The optimal value of \( \epsilon \) that reduces the hash output the most can be obtained numerically by solving the following equation:

\[
(N - \epsilon - 1) \log(N - \epsilon - 1) = \epsilon, \tag{5}
\]

where one should keep in mind that \( 1 \leq \epsilon < N - 2 \), and it is an integer. The approximate solution for the latter equation can be found as \( \epsilon \approx \frac{(N-1) \log(N-1)}{\log(N-1)-2} \). We believe this may be useful in the context of a key recycling paradigm \([51]\).

Another point of view on the problem is that one may estimate the network failure probability considering \( \varepsilon_{\text{auth}} \) as the mean nodes’ failure probability. Then obtained result in Eq. (1) shows the probability that there will be no working routes that connect the first and last nodes, i.e., overall denial of service probability.

To conclude, the obtained expression in Eq. (4) may be useful for both the design of future quantum networks and optimization of existing ones.

APPENDIX A: KEY TRANSPORT PROTOCOL EXAMPLE

Let us consider a simple example of how the key transport protocol works for \( N = 6 \) and one additional connection, i.e., \( \epsilon = 2 \). The task is to securely transfer message \( M \) from the first node to the last one (no direct QKD connection between them) following the algorithm described below.

1. Each node authenticates in the network.
2. Between each pair of nodes, QKD is performed, key \( k_{12} \) is shared between the first and second nodes, key \( k_{13} \) is shared between the first and third nodes, and so on, i.e., key \( k_{ij} \) is shared between the \( i \)th and \( j \)th nodes if there is a QKD link between them.
3. The network defines [can be done by software defined network (SDN) principles, e.g., \([52–55]\)] the total number of routes for key transport \( P_N^{(c)} \); in our case, it is \( P_6^{(2)} = 8 \), as can be observed in Fig. 4.
4. For each route, the first node generates \( K_i \) with \( 1 \leq i \leq 8 \). Then the first node (or network itself by SDN principles) develops a routing scheme \( R \) as shown in Fig. 5 and sends it to other nodes.
5. The first node transfers the encrypted messages \( (K_1K_2K_3K_5K_7)\oplus_{k_{12}} \) and \( (K_4K_6K_8)\oplus_{k_{13}} \) to the second and the third nodes correspondingly in accordance with the routing scheme \( R \) by any OCC, where by \( K_{ij} \), we assume concatenated bit strings \( K_i \) and \( K_j; \oplus \) is a bitwise XOR.
6. The second node decrypts the obtained message by applying a known quantum key as \( K_1K_2K_3K_5K_7 = (K_1K_2K_3K_5K_7)\oplus_{k_{12}} \oplus_{k_{13}} \) and splits it according to the routing scheme \( R \) by \( K_1K_3K_5 \) and \( K_2K_7 \).
7. The second node sends \( (K_1K_3K_5)\oplus_{k_{23}} \) and \( (K_2K_7)\oplus_{k_{24}} \) to the third and fourth nodes correspondingly by OCC.
8. The following eight messages are sent by OCC during the session:

\[
\begin{align*}
(K_1K_2K_3K_5K_7)\oplus_{k_{12}}, \\
(K_4K_6K_8)\oplus_{k_{13}}, \\
(K_1K_3K_5)\oplus_{k_{23}}, \\
(K_2K_7)\oplus_{k_{24}}, \\
(K_1K_4K_6)\oplus_{k_{34}}, \\
(K_3K_8)\oplus_{k_{35}}, \\
(K_1K_4K_7)\oplus_{k_{45}}, \\
(K_2K_5K_6)\oplus_{k_{46}}, \\
(K_1K_3K_4K_7K_8)\oplus_{k_{46}}.
\end{align*}
\]

9. By doing so, the last node obtains all \( K_1, \ldots, K_8 \). Then the first and last nodes obtain an encryption key \( K = \oplus_{K_i} \) known only to them.
10. The first node encrypts the message \( M \) as \( M\oplus_{K} \) and transfers it by OCC to the last node where one decrypts the message by \( M = M \oplus_{K} \oplus_{K} \).

APPENDIX B: STRICT DERIVATION

To estimate the probability of the successful attack, one should calculate the ratio between the number of all possible combinations of compromised nodes leading to the complete key eavesdropping and the number of all possible combinations of compromised nodes.
Let us consider the estimation algorithm in more detail.

1. An eavesdropper attacks every trusted node (in particular segments) with the mean success probability $p$.

2. According to the Bernoulli scheme, the probability of compromising $m$ nodes is as follows:

   \[ p_m = \binom{N-2}{m} p^m (1-p)^{N-m-2}, \tag{B1} \]

   where \( \binom{a}{b} = \frac{a!}{b!(a-b)!} \) is the corresponding binomial coefficient. We consider \( N-2 \) nodes since the first and last nodes are assumed to be not under attack.

3. Since the probability of compromising \( m \) nodes is known, one should finally estimate the amount of compromised node combinations leading to a successful attack. Necessary combinations are where at least \( c \) in a row nodes (by their order) are compromised; it is as follows:

   \[ f(N, m, c) = \binom{N-2}{m} - \left\lfloor \frac{c-1}{m-c} \right\rfloor \left( \sum_{k=0}^{\lfloor \frac{c-1}{m-c} \rfloor} x^k \right)^{N-m-1}, \tag{B2} \]

   where \( \left\lfloor \cdot \right\rfloor_m \) is the corresponding coefficient of the \( x^m \) summand. The latter expression is obtained heuristically by observation of the result of numerical simulations. However, alternatively, the expression can be derived in a different way as follows:

   \[ f(N, m, c) = \sum_{j=1}^{\left\lfloor \frac{N-2}{m-c} \right\rfloor} (-1)^{j+1} \binom{N-m-1}{j} \times \binom{N-2-c\cdot j}{m-c\cdot j}, \tag{B3} \]

   where \( \lfloor \cdot \rfloor \) is a floor function. More details on the derivation of Eq. (B3) as well as its equivalence to Eq. (B2) are shown in the following appendices. A visualization example of \( f(N, m, c) \) is shown in Fig. 7. Relation

   \[ p(s|m) = \frac{f(N, m, c)}{\binom{N-2}{m}} \tag{B4} \]

   is the conditional probability of a successful attack when \( m \) nodes are compromised.

4. Then the probability of a successful attack is defined as follows:

   \[ p_s = \sum_{m=0}^{N-2} p(s|m) \cdot p_m, \tag{B5} \]

   \[ p_s \approx (N-c-1)p^c, \tag{B6} \]

   and the latter approximation is reasonable for small mean success probabilities \( p \leq \left( \frac{1}{N-2-c-1} \right)^{\frac{1}{2}} \). For \( p \geq \left( \frac{1}{N-2-c-1} \right)^{\frac{1}{2}} \), the probability of a successful attack \( p_s \) is close to one. The behavior of the found precise and approximate expressions can be observed in Fig. 8. As one may observe, the approximated result is the same as in the main body of the paper.

**APPENDIX C: DERIVATION OF THE \( f(N, m, c) \) EXPRESSION**

The problem is to define the number of combinations where \( m \) entities (compromised nodes) are randomly distributed between \( N-2 \) positions (total number of trusted nodes in considered segments), and at least \( c \) of them are located in neighboring positions (at least \( c \) in a row). Obviously, when \( m < c \), there are no described combinations. A reasonable approach is to fix some \( k \geq c \) neighboring positions and observe the number of combinations of the rest of \( m-k \) located in the rest of \( N-2-k \) positions. However, in that case, one should avoid counting the same configurations...
multiple times for different values of considered $k$. Thus it is necessary to follow the algorithm described below.

1. Consider $c \leq m < 2c$. Step $i = 0$. The total number of outcomes when $m$ occupied positions are neighboring is $V(i = 0) = N - m - 1$, as shown in Fig. 9(a).

2. Step $i = 1$. Consider $m - 1$ neighboring positions. Also, we want to prohibit occupation of the closest two positions (to avoid multiple counting of the same pattern), highlighted in Fig. 9(b) with light gray. Then there are $(m - 1) + 2$ “occupied” (i.e., occupied and prohibited) positions that may “touch” the left and right edges, and $N - 2 - (m - 1) - 2$ vacant positions. The total number of outcomes is

$$V(i = 1) = (N - 2 - (m - 1) - 2 + 1)\times\left(\frac{N - 2 - (m - 1) - 2}{1}\right). \quad (C1)$$

3. Step $i \leq m - c$. Consider $m - i$ neighboring positions. We prohibit occupation of the closest two positions as well. Then there are $(m - i) + 2$ “occupied” (i.e., occupied and prohibited) positions that may “touch” the left and right edges, and $N - 2 - (m - i) - 2$ vacant positions. The total number of outcomes is

$$V(i) = (N - 2 - (m - i) - 2 + 1)\times\left(\frac{N - 2 - (m - i) - 2}{i}\right). \quad (C2)$$

4. The total number of combinations is as follows:

$$\sum_{i=1}^{m-c} V(i) = \sum_{i=1}^{m-c} (N - m - 3 + i)\left(\frac{N - 4 - m + i}{i}\right). \quad (C3)$$

It should be noted that summation here starts with $i = 1$ since when $i = 0$, occupied positions touch edges. This case is considered further separately.

5. Consider edges as shown in Fig. 9(c). Step $i \leq m - c$. Then $m - i$ occupied positions touch one of the edges. We prohibit occupation of the closest position as well. Then the number of “occupied” positions is $(m - i) + 1$, and the number of vacant positions is $N - 2 - (m - i) - 1$; the number of combinations for the considered $m$ is as follows:

$$W(i) = \left(\frac{N - 2 - (m - i) - 1}{i}\right). \quad (C4)$$

6. The total number of “edge” combinations is as follows:

$$2 \sum_{i=1}^{m-c} W(i) = 2 \sum_{i=1}^{m-c} \left(\frac{N - 3 - m + i}{i}\right), \quad (C5)$$

where a factor of two is due to two edges.

7. Finally, the total number of allocation combinations is as follows:

$$V(0) + \sum_{i=1}^{m-c} (V(i) + 2W(i)) = (N - m - 1)\times\left(\frac{N - 2 - c}{m - c}\right), \quad (C6)$$
where we utilize the following property:
\[ \sum_{k=0}^{a} \binom{b+k}{k} = \binom{b+a+1}{a} \].
\[ \text{(C7)} \]

8. One should consider similar to previous steps for $2c \leq m < 3c$, $3c \leq m < 4c$, and so on. However, at these steps, one should be aware of possible double counting of some combinations (this can explain the obtained further change of signs at summation). The presence of heuristic Eq. (B2) as the reference helps us to consider intricate avoidance of double counting at these steps in the right way. We obtain a final expression for the estimation of the number of combinations where $m$ entities (promised nodes) are randomly distributed between $N - 2$ positions (total number of trusted nodes), and at least $c$ of them are located in neighboring positions (at least $c$ in a row) as follows:
\[
f(N, m, c) = \sum_{j=1}^{\lfloor \frac{N}{2} \rfloor} (-1)^{j+1} \binom{N - m - 1}{j} \times \binom{N - 2 - c \cdot j}{m - c \cdot j}.
\]
\[ \text{(C8)} \]

APPENDIX D: EQUIVALENCE OF APPROACHES

In this section, we consider the equivalence of a heuristically obtained expression involving the generating function in Eq. (B2) and the alternative expression in Eq. (B3). To do so, let us consider the following steps.

1. The generating function from Eq. (B2) is
\[
\sum_{i=0}^{c-1} x^i = \frac{1 - x^c}{1 - x}.
\]
\[ \text{(D1)} \]

2. The next step is to raise it to the power $K = n - m - 1$ and expand as follows:
\[
(1 - x^c)^K \cdot (1 - x)^{-K}.
\]
\[ \text{(D2)} \]

3. Let us differentiate the expression:
\[
(U(x) \cdot V(x))^{[m]} = \sum_{r=0}^{m} \binom{m}{r} U(x)^{[r]} V(x)^{[m-r]},
\]
\[ \text{(D5)} \]

\[
\left. ((1 - x^c)^K \cdot (1 - x)^{-K}) \right|_{x=0} = \binom{K + m - r - 1}{m - r} \cdot (m - r)!
\]
\[ \text{(D6)} \]

4. Let us substitute $r = j \cdot c$ and $K = N - m - 1$:
\[
\left. \left( \sum_{i=0}^{c-1} x^i \right)^{N-m-1} \right|_{x=0} = m! \cdot \sum_{j=1}^{\lfloor \frac{N}{2} \rfloor} (-1)^{j+1} \binom{N - m - 1}{j} \cdot \binom{N - 2 - c \cdot j}{m - c \cdot j}.
\]
\[ \text{(D8)} \]

5. The final step is as follows:
\[
\left( \frac{N - 2}{m} \right) - cf \left[ \sum_{i=0}^{c-1} x^i \right]^{N-m-1} = m! \cdot \sum_{j=1}^{\lfloor \frac{N}{2} \rfloor} (-1)^{j+1} \binom{N - m - 1}{j} \cdot \binom{N - 2 - c \cdot j}{m - c \cdot j}.
\]
\[ \text{(D9)} \]

REFERENCES

1. S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaffer, M. Tomamichel, V. G. Ussenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” arXiv:1906.01645 (2019).
2. C. Elliott, “Building the quantum network,” New J. Phys. 4, 46 (2002).
3. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafner, and H. Yeh, “Current status of the DARPA quantum network,” Proc. SPIE 5815, 138–149 (2005).
4. C. Elliott and H. Yeh, “DARPA quantum network testbed,” Tech. Rep. (BBN Technologies, 2007).
5. A. Poppe, M. Peev, and O. Maehurst, “Outline of the SECOQC quantum-key-distribution network in Vienna,” Int. J. Quantum Inf. 6, 209–218 (2008).
6. J. Dynes, A. Wonfor, W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plevy, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, “Cambridge quantum network,” NPJ Quantum Inf. 5, 101 (2019).
7. M. Peev, C. Pacher, R. Alléaume, et al., “The SECOQC quantum key distribution network in Vienna,” New J. Phys. 11, 075001 (2009).
8. F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, “Field experiment on a robust
hierarchical metropolitan quantum cryptography network,” Chin. Sci. Bull. 54, 2991–2997 (2009).

9. M. Sasaki, M. Fujiwara, H. Ishizuka, et al., “Field test of quantum key distribution in the Tokyo QKD network,” Opt. Express 19, 10387–10409 (2011).

10. S. Wang, W. Chen, Z.-Q. Yin, et al., “Field and long-term demonstration of a wide area quantum key distribution network,” Opt. Express 22, 21739–21756 (2014).

11. T. R. Beals and B. C. Sanders, “Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network,” in International Conference on Information Theoretic Security (Springer, 2008), pp. 29–39.

12. L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” J. Comput. Secur. 18, 61–87 (2010).

13. S. M. Barnett and J. S. Phoehnix, “Securing a quantum key distribution relay network using secret sharing,” in IEEE GCC Conference and Exhibition (GCC) (IEEE, 2011), pp. 143–145.

14. S. J. Phoenix and S. M. Barnett, “Relay QKD networks & bit transport,” arXiv:1502.06319 (2015).

15. C. Ma, Y. Guo, and J. Su, “A multiple paths scheme with labels for key distribution on quantum key distribution network,” Commun. Phys. 2, 118 (2019).

16. H. Zhou, K. Lv, L. Huang, and X. Ma, “Quantum network: security assessment and key management,” IEE/ACM Trans. Netw. 30, 1328–1339 (2022).

17. S. Zhao, A. Wiegela, and P. Scharnter, “Building a quantum network: how to optimize security and expenses,” J. Netw. Syst. Manag. 18, 283–299 (2020).

18. N. R. Solomons, A. I. Fletcher, D. Aktas, N. Venkatachalam, S. Wengrowersky, M. Lončarić, S. P. Neumann, B. Liu, Ž. Samec, M. Stipčević, R. Ursin, S. Pirandola, J. G. Rarity, and S. K. Joshi, “Scalable authentication and optimal flooding in a quantum network,” arXiv:2011.12225 (2021).

19. M. Pattaranantakul, A. Janthong, K. Sanguanan, P. Sangwongnam, and K. Sripimanwat, “Secure and efficient key management test using secret sharing,” in 4th International Conference on Ubiquitous and Future Networks (iCUFN) (IEEE, 2012), pp. 280–285.

20. S. Das, S. Bäuml, W. Czyszczowicz, and K. Horodecki, “Universal limitations on quantum key distribution over a network,” Phys. Rev. X 11, 041016 (2021).

21. S. Pirandola, “End-to-end capacities of a quantum communication network,” Commun. Phys. 2, 51 (2019).

22. L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, “Quantum repeater with encoding,” Phys. Rev. A 79, 032326 (2009).

23. Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, “Experimental realization of entanglement concentration and a quantum repeater,” Phys. Rev. Lett. 90, 207901 (2003).

24. T.-J. Wang, S.-Y. Song, and G. L. Long, “Quantum repeater based on spatial entanglement of photons and quantum-dot spins in optical microcavities,” Phys. Rev. A 85, 062311 (2012).

25. M. Ghalaii and S. Pirandola, “Capacity-approaching quantum repeaters for quantum communications,” Phys. Rev. A 102, 062412 (2020).

26. A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, “Quantum Internet: networking challenges in distributed quantum computing,” IEEE Netw. 34, 137–143 (2019).

27. A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, “When entanglement meets classical communications: quantum teleportation for the Quantum Internet,” IEEE Trans. Commun. 68, 3808–3838 (2020).

28. J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, “Quantum Internet protocol stack: a comprehensive survey,” arXiv:2202.10894 (2022).

29. H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” Phys. Rev. Lett. 108, 130503 (2012).

30. S. L. Braunstein and S. Pirandola, “Side-channel-free quantum key distribution,” Phys. Rev. Lett. 108, 130502 (2012).
53. V. Martin, A. Aguado, J. Brito, A. Sanz, P. Salas, D. R. López, V. López, A. Pastor-Perales, A. Poppe, and M. Peev, “Quantum aware SDN nodes in the Madrid quantum network,” in 21st International Conference on Transparent Optical Networks (ICTON) (IEEE, 2019).

54. A. Aguado, V. Martin, D. Lopez, M. Peev, J. Martinez-Mateo, J. Rosales, F. de la Iglesia, M. Gomez, E. Hugues-Salas, A. Lord, R. Nejabati, and D. Simeonidou, “Quantum-aware software defined networks,” in International Conference on Quantum Cryptography (QCrypt) (2016).

55. E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, “Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks,” J. Opt. Commun. Netw. 11, A209–A218 (2019).