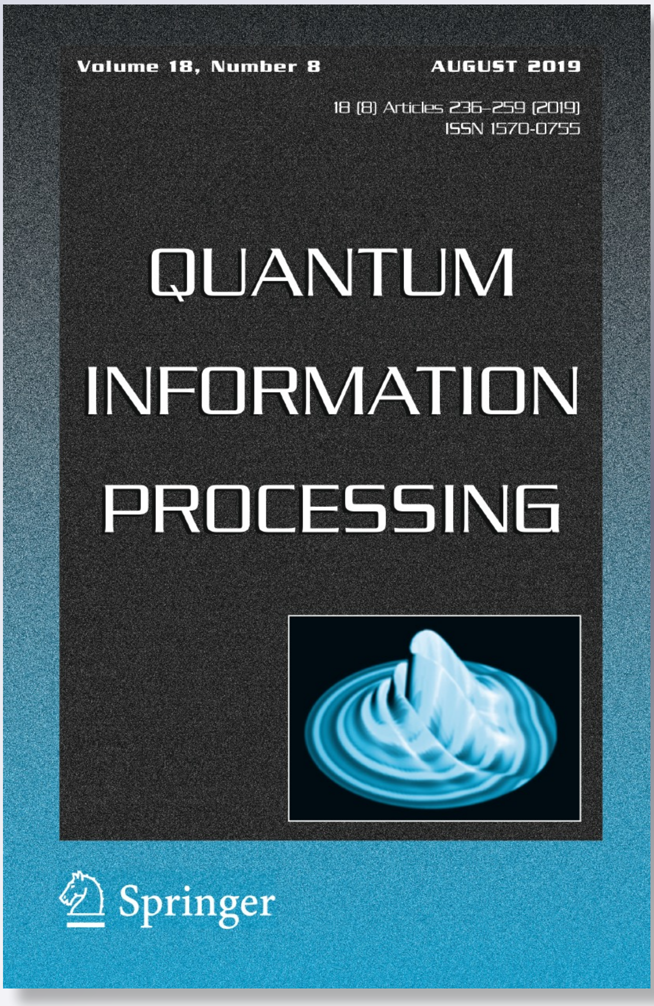
Modeling and simulation of practical quantum secure communication network

Yaxing Wang, Qiong Li, Qi Han & Yumeng Wang

Quantum Information Processing

ISSN 1570-0755
Volume 18
Number 9

Quantum Inf Process (2019) 18:1-18
DOI 10.1007/s11128-019-2394-3



Quantum Information Processing (2019) 18:278
https://doi.org/10.1007/s11128-019-2394-3

Modeling and simulation of practical quantum secure communication network

Yaxing Wang[1] · Qiong Li[1] · Qi Han[1] · Yumeng Wang[2]

Received: 4 February 2019 / Accepted: 20 July 2019

Abstract

As the quantum key distribution (QKD) technology supporting the point-to-point application matures, the need to build the quantum secure communication network (QSCN) to guarantee the security of a large scale of nodes becomes urgent. Considering the project time and expense control, it is the first choice to build the QSCN based on an existing classical network. Suitable modeling and simulation are very important to construct a QSCN successfully and efficiently. In this paper, a practical QSCN model, which can reflect the network state well, is proposed. The model considers the volatile traffic demand of the classical network and the real key generation capability of the QKD devices, which can enhance the accuracy of simulation to a great extent. In addition, two unique QSCN performance indicators, ITS (information-theoretic secure) communication capability and ITS communication efficiency, are proposed in the model, which are necessary supplements for the evaluation of a QSCN except for those traditional performance indicators of classical networks. Finally, the accuracy of the proposed QSCN model and the necessity of the proposed performance indicators are verified by plentiful simulation results.

Keywords Quantum secure communication network · Quantum key distribution · Network simulation · Performance analysis

1 Introduction

Based on the quantum key distribution (QKD) technology with the intrinsic characteristics of point-to-point (P2P) [1], building a quantum secure communication network (QSCN) [2–4] with multiple QKD devices is a prevailing solution to overcome the limits of node scale and the communication distance [5–10]. Since the state-of-the-art

✉ Qiong Li
qiongli@hit.edu.cn

[1] School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China

[2] School of International Studies, Harbin Institute of Technology, Harbin, China

Published online: 30 July 2019

QKD technology has been able to support many applications at distances of several hundred kilometers in the P2P mode, those achievements have made it possible to establish a QSCN upon an existing complex classical network. For instance, the key distribution rate of one QKD device could reach 10 Mbps [11] and 1 Mbps [12] at the distribution distance of 10 km and 100 km, respectively. Additionally, the key distribution distance of one QKD device could reach 404 km in optical fiber [13] and even reach 1200 km in free space [14]. As to the existing QSCNs, the node scale has expanded from six nodes [9,15] to 56 nodes [16], and the communication distance has extended from 19.6 km [15] to 2000 km [16]. With the growing scale and complexity of QSCNs, the aforehand modeling and simulation become crucial for the functional verification, the deployment optimization of QKD devices, the project time and cost control, the network quality assurance, etc. [17–19].

Unlike the field of classical networks, the modeling and simulation in the field of QSCN have not drawn much attention [20–25]. In order to reduce the cost of communication resources, some efforts in quantum network coding [20–22] have been made. However, the analysis of network performance was neglected in these researches. A simple trust relaying-based [26,27] QSCN simulation model was built by Yang et al. in 2017 [24] to calculate the key consumption cost. In this work, the key generation capability was set to be endless when the key consumption of a pair of partners was evaluated, which is not realistic in a practical QSCN. Taking the limited key generation capability of QKD device into account, a relatively complete QSCN model [25] was proposed and implemented by Mehic et al. based on the Network Simulator version 3 (NS-3) [28] in 2017. In the [25], the key generation and traffic generation have been simulated to estimate network performance. However, the assumptions about the key generation capability and traffic demand are unreasonable. In addition, the network performance was only measured by routing cost and packet delivery ratio (PDR), which cannot indicate the characteristics of QSCN.

In a practical QSCN, the most important performance depends on whether the QKD key generation capability can meet the traffic demand [29]. However, the modeling of traffic demand, key generation capability and their relationship has not been studied thoroughly in previous studies on QSCN. The main defects in the existing studies include the following. Firstly, the end-to-end (E2E) traffic demand is modeled by a constant which cannot describe the volatility of the network. Secondly, the P2P key generation capability is modeled by the performance of the QKD post-processing system without taking into account the effects of QKD optical system performance. Thirdly, there is still lack of suitable performance indicators to measure the relationship between the E2E traffic demand and P2P key generation capability. Fourthly, only one pair of terminal partners communicates in the simulation, which fails to reflect the whole status of a practical multiparty network.

In this paper, a practical QSCN model is proposed, in which the volatility of the E2E traffic demand is modeled by the Poisson stochastic process, and the P2P key generation capability is modeled by the GLLP theory. In addition, two performance indicators: ITS communication capability and ITS communication efficiency, are proposed to evaluate the special all-round performance of a QSCN. Finally, a QSCN simulation in view of the whole network is designed to verify the accuracy of the proposed QSCN model and the necessity of the proposed performance indicators.

The rest of this paper is organized as follows: Sect. 2 gives the definition and basic characteristics of QSCN. Section 3 describes the practical QSCN model by proposing traffic generation module, key generation module and two performance indicators. Section 4 designs a simulation to analyze the network performance in detail based on the QSCN model. Section 5 concludes this study and outlines the future works.

2 Definition of quantum secure communication network

In many studies, both terms of QSCN and QKD network are used to indicate the communication network based on QKD device. For the sake of better argument, QKD network is defined as a set of infrastructures for generating ITS key based on the laws of quantum mechanics [30] in this paper. The QSCN is defined as a network that provides the secure communication service utilizing the keys generated by QKD network. In order to achieve the ITS secure communication, the one-time-pad (OTP) encryption algorithm is adopted in the performance analysis in this paper. If ITS is not pursued in an application, the popular encryption algorithms, such as AES and DES, are also acceptable. The QSCN consists of two parts: QKD network and classical network [31], shown as Fig. 1.

Similar to the traditional classical network, QSCN mainly consists of terminals, switches, links and protocols [32]. The functions of each component are introduced as follows.

- The terminal is the interface between a user and a communication network, which is mainly used to transmit and receive data. In the QSCN, the terminal is abstracted as a node, which can be a source node for data transmission or a destination node for data reception.

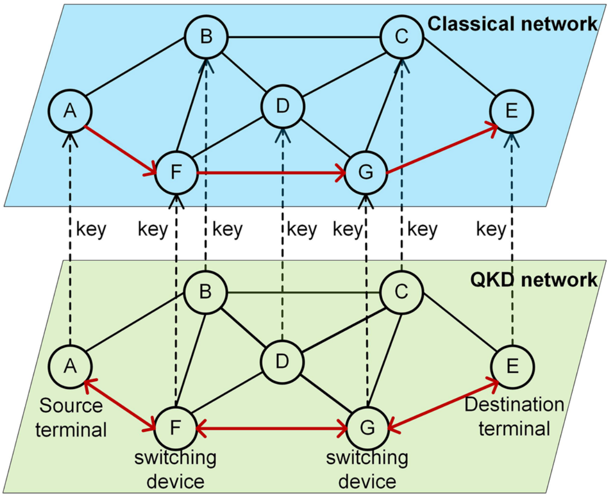


Fig. 1 Hierarchical diagram of QSCN

- The switch is the network device with the function of finding the next receiver and forwarding the data. In the QSCN, the switch needs to be completely trustable and can be abstracted as a trusted relay, which is used to forward data.
- The link refers to the medium of data communication between terminals. In fact, it includes not only a physical channel but also various communication devices, such as modulators and controllers. In the QSCN, it is abstracted as a P2P channel.
- The protocol defines the series of rules that enable the network to work properly. In the QSCN, it mainly includes packet protocol and routing protocol.

3 Quantum secure communication network model

The biggest difference between the QSCN and classical network is that the classical communication of QSCN consumes the keys generated by QKD layer. This leads to the performance of the QSCN ia closely limited by the matching degree between the traffic demand and key generation capability. In fact, the traffic demand in the QSCN is from E2E partners, while the key generation capability is decided by P2P links. In order to describe the network performance more accurately, this paper proposes a practical QSCN model, shown as Fig. 2.

In the QSCN model, the function of traffic generation module is to model the E2E traffic demand of classical network, and the function of key generation module is to model the P2P key generation capability of the QKD network. In addition, the relationship between these two functions will be measured by two proposed performance indicators. The schemes of other modules such as routing protocols and data encryption/decryption can be borrowed from the traditional classical network model.

3.1 Traffic generation module

Due to the neglect of the relationship between key generation and key consumption, the traffic demand of the classical communication [33–37] has not attracted enough attention in the field of QSCN. A reasonable traffic demand model of the classical network is designed in this section.

The packet transmission process can be assumed to satisfy the following three conditions [33]:

(1) In the non-overlapping time period, the numbers of transmitted packets are independent variables.
(2) In an arbitrarily short time Δt, the probability of transmitting a packet is independent of the starting time and only proportional to the length of the time period.
(3) In an arbitrarily short time Δt, the number of transmitted packets is either 1 or 0.

It can be proved that the packet transmission process follows a Poisson stochastic process [38]. Let λ be the average number of transmitted packets per second and $p_k(t)$ denote the probability of transmitting k packets within the time period t. According to the conditions as above, in an arbitrarily short time Δt, the average number of transmitted packets is $\lambda \Delta t$. Dividing the finite time period t into n small time slices Δt, i.e., $t = n\Delta t$, then the k packets transmitted in the time period t can be divided

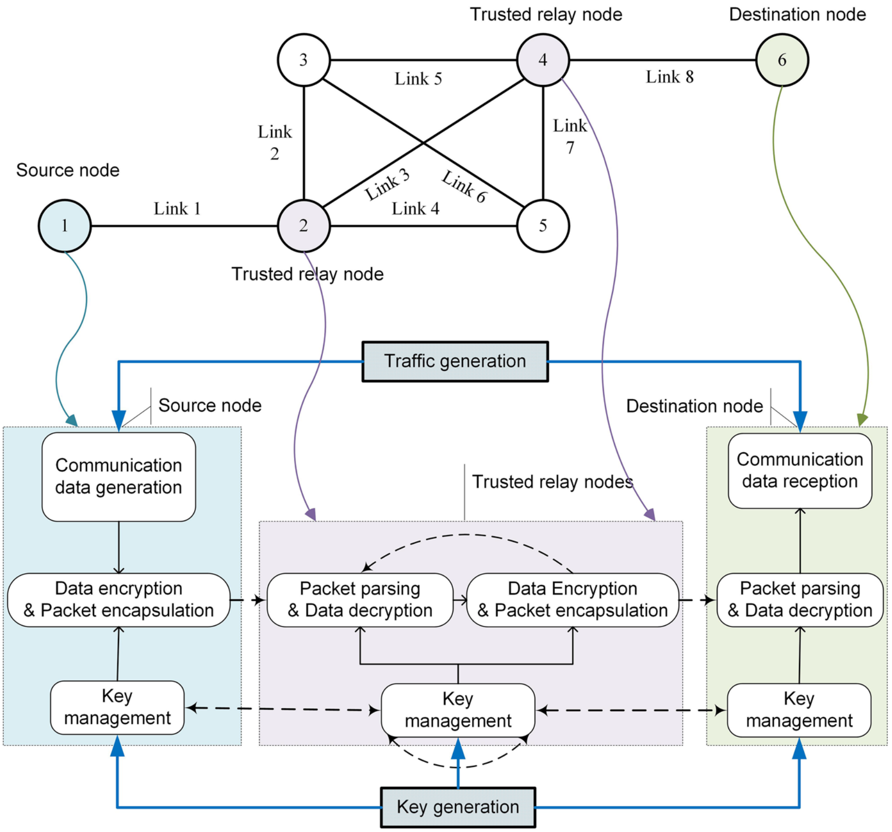


Fig. 2 QSCN model

into n parts. Let $n \to \infty$, then the probability of transmitting k packets in time period t is

$$p_k(t) = \frac{e^{-\lambda t}(\lambda t)^k}{k!}, k = 0, 1, 2, \ldots \tag{1}$$

Equation 1 states that the probability $p_k(t)$ of transmitting k packets in time period t obeys the Poisson distribution under the above three conditions [38]. According to the basic properties of probability theory, it can be derived that:

(1) The probability density function of the packet transmission interval is $\lambda e^{-\lambda t}$. In other words, the packet transmission interval is subject to the exponential distribution.

(2) The average number of transmitted packets during the time period t is $E(k, t) = \sum_{k=0}^{\infty} k p_k(t) = \lambda t$. Therefore, the average number of transmitted packets per second is $E(k, 1) = \lambda$, and the average transmitted packets interval is $1/\lambda$. Setting the packet size to κ, the average communication rate is $R_f = \lambda\kappa$.

(3) Let η denote a random number sequence of multiple packet transmission intervals, which satisfies the exponential distribution with a mean of $1/\lambda$. Therefore, its cumulative distribution function is $F(\eta) = 1 - e^{-\lambda\eta}$. Suppose ξ is a random number sequence with uniformly distributed in [0, 1], η can be produced as follows:

$$\eta = \frac{1}{\lambda} \ln(1 - \xi) \tag{2}$$

According to the analysis above, if the average number of transmitted packets per second is λ, the packet transmission process can be simulated into an exponential distribution with the average transmission interval of $1/\lambda$. Therefore, the traffic generation module is constructed by the exponential distribution-based packet transmission interval.

3.2 Key generation module

A QKD system consists of the optical sub-system and the post-processing sub-system. The key generation capability is determined by performance of the two sub-systems [39]. Therefore, it is not convincing to characterize the key generation capability only by the performance of the post-processing procedure as in the literature [25].

In 2004, Gottesman et al. proposed the GLLP theory to calculate the secure key generation rate of QKD system with imperfect devices [40]. This method has been adopted in most practical QKD systems [9,41–51]. Therefore, we use the GLLP theory to model the key generation module. The formula to calculate the secure key generation rate is as follows:

$$R = \max\left\{-qQ_\mu f_{ec} H\left(E_\mu\right) + qQ_1\left[1 - H\left(e_1\right)\right], 0\right\}. \tag{3}$$

In Eq. 3, q is the sifting coefficient, the subscript μ denotes the intensity of signal state, Q_μ is the overall gain of signal state, E_μ is the overall quantum bit error rate (QBER), Q_1 is the gain of single-photon state, e_1 is the error rate of single-photon state, f_{ec} is the error correction efficiency and $H(x)$ is the binary Shannon information function, given by $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

Four key variables, Q_μ, E_μ, Q_1 and e_1, are required to calculate R. The first two can be measured directly by the experiment; however, the last two can only be estimated by decoy state method. Let η_{Bob} denote the transmittance of Bob, including the internal transmittance of optical components and detector efficiency. Note that Y_0 is the background rate and e_0 is the error rate of the background. Assuming that Alice and Bob choose the vacuum + weak decoy state method, with expected photon numbers ν and ϕ, which satisfy $\nu < \mu$ and $\phi = 0$. Thus, Alice and Bob can estimate the background rate,

$$Q_\phi = Y_0, \tag{4}$$

$$E_\phi = e_0. \tag{5}$$

The overall gain and QBER of the signal state are given by

$$Q_\mu = 1 - e^{-\eta\mu} + Y_0, \tag{6}$$

$$Q_\mu E_\mu = e_0 Y_0 + e_{det}\left(1 - e^{-\eta\mu}\right). \tag{7}$$

The overall gain and QBER of the weak decoy state are given by

$$Q_\nu = 1 - e^{-\eta\nu} + Y_0, \tag{8}$$

$$Q_\nu E_\nu = e_0 Y_0 + e_{det}\left(1 - e^{-\eta\nu}\right). \tag{9}$$

Considering the statistical fluctuations of finite dataset size [52,53] in real-life experiments on the estimation process of Q_1 and e_1, the Chernoff bound [54] is used to provide good bounds [55]. Let X_1, X_2,..., X_n be a set of independent Bernoulli random variables that satisfy $P\left(X_i = 1\right) = p_i$, and let $X = \sum_{i=1}^{n} X_i$ and $\overline{X} = E\left(X\right)$. With the security bound of $\varsigma = 2\varepsilon$, we can draw the following inequalities [55]:

$$P\left(X - \overline{X} > \sqrt{2X\ln\left(\varepsilon^{-3/2}\right)}\right) \le \varepsilon, \tag{10}$$

$$P\left(\overline{X} - X > \sqrt{2X\ln\left(16\varepsilon^{-4}\right)}\right) \le \varepsilon. \tag{11}$$

Denote the number of pluses sent by Alice for signal as N_μ, for weak as N_ν and for vacuum as N_ϕ. Let X denote the response count of signal state, then $X = N_\mu Q_\mu$. According to Eqs.10 and 11, we can draw that

$$P\left(N_\mu Q_\mu - \sqrt{2N_\mu Q_\mu \ln\left(\varepsilon^{-3/2}\right)} \le N_\mu \overline{Q}_\mu \le N_\mu Q_\mu + \sqrt{2N_\mu Q_\mu \ln\left(16\varepsilon^{-4}\right)}\right) \ge 1 - \varsigma$$

Therefore, the lower bound and upper bound of $\overline{Q}_\mu$ are given by

$$\overline{Q}_\mu^L = Q_\mu - \sqrt{\frac{2Q_\mu \ln\left(\varepsilon^{-3/2}\right)}{N_\mu}}, \tag{12}$$

$$\overline{Q}_\mu^U = Q_\mu + \sqrt{\frac{2Q_\mu \ln\left(16\varepsilon^{-4}\right)}{N_\mu}}. \tag{13}$$

And so on, for the $\overline{Q}_\nu^L$, $\overline{Q}_\nu^U$, $\overline{Q}_\phi^L$ and $\overline{Q}_\phi^U$.

Let X denote the error count of weak decoy state, then $X = N_\nu Q_\nu E_\nu$. According to Eqs.10 and 11, the lower bound and upper bound of $\overline{E}_\mu$ are given by

$$\overline{E}_\nu^L = E_\nu - \sqrt{\frac{2E_\nu \ln\left(\varepsilon^{-3/2}\right)}{N_\nu Q_\nu}}, \tag{14}$$

$$\overline{E}_\nu^U = E_\nu + \sqrt{\frac{2E_\nu \ln\left(16\varepsilon^{-4}\right)}{N_\nu Q_\nu}}. \tag{15}$$

The $\overline{E}_{\phi}^{L}$ and $\overline{E}_{\phi}^{U}$ can be deduced by analogy.

Combining Eqs.6 and 8, the lower bound of Y_1 is given by

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(\overline{Q}_{\nu}^{L}e^{\nu} - \frac{\nu^2}{\mu^2}\overline{Q}_{\mu}^{U}e^{\mu} - \frac{\mu^2-\nu^2}{\mu^2}Y_0\right). \tag{16}$$

Under the condition of Eqs.4 and 5, the lower bound of Q_1 and upper bound of e_1 are given by

$$Q_1 \geq Q_{_1}^{L} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(\overline{Q}_{\nu}^{L}e^{\nu} - \frac{\nu^2}{\mu^2}\overline{Q}_{\mu}^{U}e^{\mu} - \frac{\mu^2-\nu^2}{\mu^2}\overline{Q}_{\phi}^{U}\right), \tag{17}$$

$$e_1 \leq e_1^U = \frac{\mu\nu - \nu^2}{\mu\nu}\frac{\overline{Q}_{\nu}^{U}\overline{E}_{\nu}^{U}e^{\nu} - \overline{Q}_{\phi}^{L}\overline{E}_{\phi}^{L}}{\overline{Q}_{\nu}^{L}e^{\nu} - \frac{\nu^2}{\mu^2}\overline{Q}_{\mu}^{U}e^{\mu} - \frac{\mu^2-\nu^2}{\mu^2}\overline{Q}_{\phi}^{U}}. \tag{18}$$

Substituting these parameter estimations into Eq. 3, we can calculate the lower bound of the secure key generation rate of one QKD device

$$R \geq \max\left\{R_L = -qQ_{\mu}f_{ec}H\left(E_{\mu}\right) + qQ_{_1}^{L}\left[1 - H\left(e_{_1}^{U}\right)\right], 0\right\}. \tag{19}$$

Then, the key generation capability of a P2P link is given by

$$R_k = \max\left\{f_{req}R_L, 0\right\}, \tag{20}$$

where f_{req} is the repetition rate.

3.3 Performance indicators

To meet the requirement of ITS, it is necessary to utilize the OTP algorithm in the QSCN for data encryption and decryption. The key generation capability of the network is based on the P2P links; however, the traffic demand is based on the E2E partners. Under this condition, if the key generation capability cannot meet the traffic demand, i.e., if the QSCN will paralyze at some point, it directly affects the performance of a QSCN. However, there is no counterpart in classical network, and there is no appropriate indicator in classical network to measure such performance of QSCN either. In this paper, two performance indicators are proposed: ITS communication capability and ITS communication efficiency, as necessary supplements to evaluate a QSCN except for those traditional performance indicators of classical networks.

3.3.1 ITS communication capability

For a given topology $G = (V, E)$, let R_k^m $(m \in E)$ be the key generation capability of the link m which is time independent and can be calculated according to GLLP theory. R_f indicates the total traffic demand of all pairs of partners, and

$R_f \cdot \overline{P}^{i,j}$ $(i \in V, j \in V)$ means the average traffic demand of node i and node j, which can be modeled by a Poisson stochastic process and can be calculated according to the average packet interval. $\overline{\varpi}^{i,j,m} \in \{0, 1\}$ indicates whether the communication of node i and node j requires link m. In addition, $\overline{O}^m$ represents the average number of keys consumed by routing data on the link m.

To guarantee the stable operation of the network, the key consumption of each link needs to be less than or equal to its key generation. The key consumption mainly includes communication data consumption and routing data consumption. When the OTP algorithm is used, the key consumption of communication data is equal to the traffic:

$$\forall m \in E,\ R_k^m \geqslant \sum_{i \in V} \sum_{j \in V} R_f \cdot \overline{P}^{i,j} \overline{\varpi}^{i,j,m} + \overline{O}^m \tag{21}$$

The ITS communication capability of the QSCN is defined as the maximum traffic demand that enables all links to work stably. It is represented by a symbol C:

$$C = \max \left\{ R_f \mid \forall m \in E,\ \sum_{i \in V} \sum_{j \in V} R_f \cdot \overline{P}^{i,j} \overline{\varpi}^{i,j,m} + \overline{O}^m - R_k^m \leqslant 0 \right\} \tag{22}$$

It can be seen from the formula that the ITS communication capability is mainly related to the traffic demand, key generation capability and routing protocol.

3.3.2 ITS communication efficiency

When the traffic demand is higher than the ITS communication capability, the QSCN will inevitably paralyze after running for a certain period of time. The time span before the QSCN paralyzes is defined as ITS operation time, represented by the symbol T_o. Let D be the initial number of keys on each link in the network and $R_f \cdot P^{i,j}(t)$ $(i \in V, j \in V)$ be the traffic demand of node i and node j at the time of t. In addition, $\omega^{i,j,m}(t) \in \{0, 1\}$ indicates whether the communication of node i and node j requires link m at the time of t and $O^m(t)$ indicates the number of keys consumed by routing data on the link m at the time of t. Then, the network ITS operation time must meet the following requirement:

$$T_o = \max \left\{ T \mid \forall m \in E,\ \int_0^T \left(\sum_{i \in V} \sum_{j \in V} R_f \cdot P^{i,j}(t)\, \omega^{i,j,m}(t) + O^m(t) \right) dt - T \cdot R_k^m \leqslant D \right\} \tag{23}$$

When the network paralyzes, the number of remaining keys on the link m is:

$$D_m = \int_0^{T_o} \left(\sum_{i \in V} \sum_{j \in V} R_f \cdot P^{i,j}(t)\, \omega^{i,j,m}(t) + O^m(t) \right) dt - T_o \cdot R_k^m \tag{24}$$

The ITS recovery time is defined as the length of time required for the numbers of keys on all links to recover to D, represented by the symbol T_r:

$$T_r = \min \left\{ T \mid \forall m \in E, T \geqslant \frac{D - D_m}{R_k^m} \right\} \tag{25}$$

In order to ensure stable operation based on the OTP algorithm in any traffic demand environment, the ITS operation time and ITS recovery time of the QSCN must meet the preset requirement. The ratio of the ITS operation time to the sum of ITS operation time and ITS recovery time is defined as ITS communication efficiency Q as in Eq. 26:

$$Q = \frac{T_o}{T_o + T_r} \tag{26}$$

The ITS communication efficiency, which is mainly related to the traffic demand, key generation capability and routing protocol, can be used to guide the actual working policy of the QSCN.

It can be seen from the formulas that when the network scale becomes large, it is quite difficult to theoretically analyze the QSCN performance. In this case, the network simulation becomes the most important, convenient and economical solution for the performance analysis of the QSCN.

4 Simulation and results analysis

In this section, a QSCN simulation using Network Simulator version 3 (NS-3) [28] is designed to analyze the network performance.

4.1 Simulation design

The simulation design mainly includes the traffic generation, key generation, topology and routing protocol, which can directly affect the performance of a QSCN.

4.1.1 Traffic generation

To simplify the analysis, the traffic demand between any two partners in our simulation is assumed to be the same scale. Based on the analysis in Sect. 3.1, the packet transmission intervals follow an exponential distribution. In order to find out the performance bottleneck of QSCN , two comparison simulations are conducted with communication rates of 100 Kbps and 10 Kbps. In the case where the packet size is set to 500 bytes, the average packet transmission intervals are set to 40 ms and 400 ms.

In a practical network, a classical link often needs to serve multiple partners, which will lead to two kinds of problems. Firstly, when the traffic demand of a pair of terminal partners is met, it may reduce the communication performance of another pair of terminal parties. Secondly, the change of paths for a certain pair of terminal partners may improve the communication performance of others. Therefore, it is not reasonable to only analyze the traffic demand of one pair of terminal partners as in the literature [25]. Therefore, we should consider the traffic demand of all pairs of partners at the same time, as shown in Algorithm 1.

Algorithm 1 End-to-end traffic generation of whole network

```
Input: a given topology $G = (V, E)$ with the node size of $n$ and the edge size of $m$, traffic generation
    module with the average packet interval of $1/\lambda$, packet size of $\kappa$, routing protocol of $\omega$, total duration
    of simulation $T$
Output: The key consumptions of all links $comCnt$ (an array of size $m$)
$comCnt \leftarrow 0$
while $t < T$ do
    for each vertex $v_i, v_j (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n, i \neq j) \in G, V$ do
        for each edge $e_k (1 \leqslant k \leqslant m) \in G, E$ do
            $comCnt(k) \leftarrow comCnt(k) + \omega^{i,j,m}(t) \cdot \kappa$    ▷ Calculate the key consumption of the link $e_k$
            $\xi = Rnd(0, 1)$    ▷ Let $\xi$ as a random number in the [0, 1]
            $\eta = \frac{1}{\lambda} \ln(1 - \xi)$    ▷ Calculate the packet interval
            $t \leftarrow t + \eta$    ▷ Send next packet after the packet interval
        end for
    end for
end while
```

4.1.2 Key generation

To simplify the analysis, we assume that only one QKD device is configured on each link and the parameters of all QKD devices are the same. The parameters of QKD device in our simulation are shown in Table 1, referring to the literature [11]. It should be noted that the QSCN model supports the configuration of multiple QKD devices for each link and the different parameter setting for each QKD device.

According to the parameters given in Table 1, the key generation rate of each link can be calculated. In order to find out the performance bottleneck of the whole network, we make all QKD devices with different distribution distances start generating keys at the same time and simulate the process of key generation, as shown in Algorithm 2:

4.1.3 Topology

To the best of our knowledge, the most comprehensive study on QSCN performance appears in the literature [25]. For comparison, the topology of SECOQC network [30] is used in [25], as shown in Fig. 3. Besides, the trusted relays adopted in our simulation work on the basis of the hop-by-hop [30]. Each node in the topology is a communication user and acts as a trusted relay. In other words, each node should be configured with the

Table 1 Parameters of QKD devices

$freq$	q	α	η_{Bob}	e_{det}	μ	ν	ϕ	Y_0	e_0	f_{ec}	N_μ	N_ν	N_ϕ	ς
1 GHz	0.9	0.2 db/km	0.1	0.01	0.4	0.1	0	2.1E-5	0.5	1.15	1.6E10	2E9	2E9	5.73E-7

Algorithm 2 Point-to-point key generation of whole network

```
Input: a given topology $G = (V, E)$ with the node size of $n$ and the edge size of $m$, key generation module
    with $(f_{rep}, q, Q_\mu, E_\mu, f_c, Q_1, e_1)$, total duration of simulation $T$
Output: The key generations of all links $genCnt$ (an array of size $m$)
$genCnt \leftarrow 0$
for each link $e_k (1 \leqslant k \leqslant m) \in G, E$ do
    $R_k \leftarrow \max\left\{-f_{req} q Q_\mu f_{ec} H\left(E_\mu\right) + f_{req} q Q_1^L \left[1 - H\left(e_1^U\right)\right], 0\right\}$    ▷ Calculate the key generation rate
    $genCnt\,(k) \leftarrow genCnt\,(k) + R_k \cdot T$
end for
```

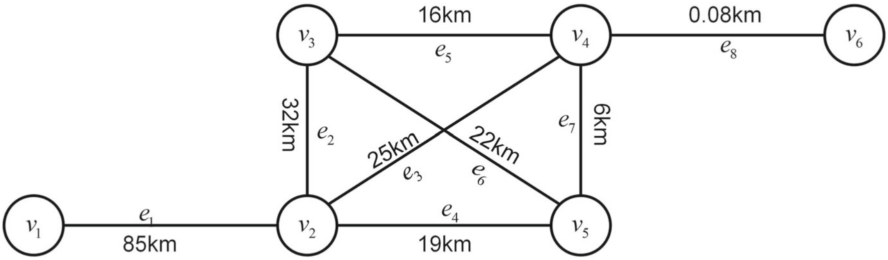


Fig. 3 Topology of the QSCN

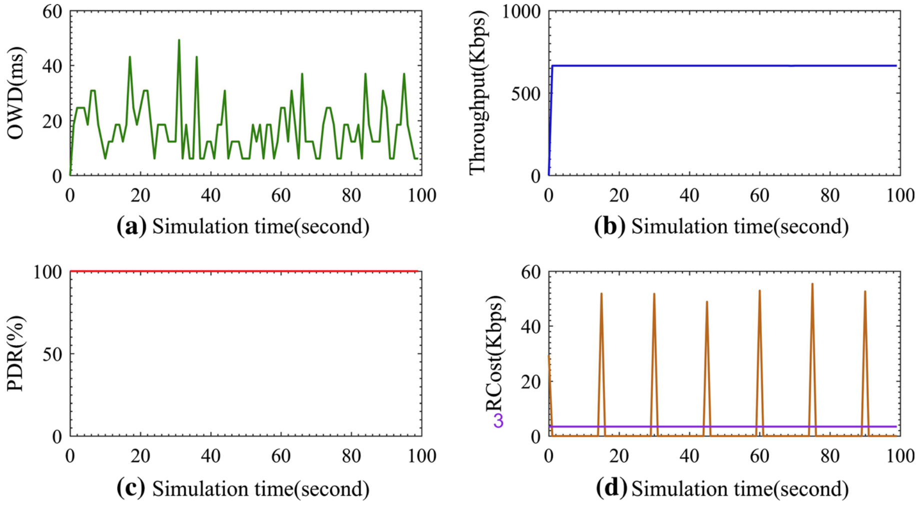
classical communication equipment, the QKD device, encryption/decryption module, key management module, traffic monitoring module.

4.1.4 Routing protocol

The traffic demand that the network needs to meet is E2E based; however, the key consumption is P2P based. Through the design of better routing protocol, it is expected to maximize the utilization of the P2P key generation capability to satisfy the E2E traffic demand, thereby improving network performance. Due to the frequent changes of the number of keys during the simulation process, the connected/broken state of a link may change as well, which leads to frequent changes of the network topology. It means that the selected routing protocol should be able to perceive the network topology changes in time. Therefore, the DSDV routing protocol [56], which is commonly used in the wireless ad hoc network, is adopted. The DSDV protocol updates routing table regularly.

4.2 Performance of traditional indicators

In this section, four most important performance indicators of classical network are evaluate to analyze the QSCN performance, which are one-way delay (OWD) [57], throughput [58], packet delivery rate (PDR) [25] and routing cost (RCost) [59]. OWD is the required time of data packet transmission across the network, which may be affected by any component of the related links. Throughput is defined as the rate of successful message delivery over a communication channel. PDR refers to the ratio of



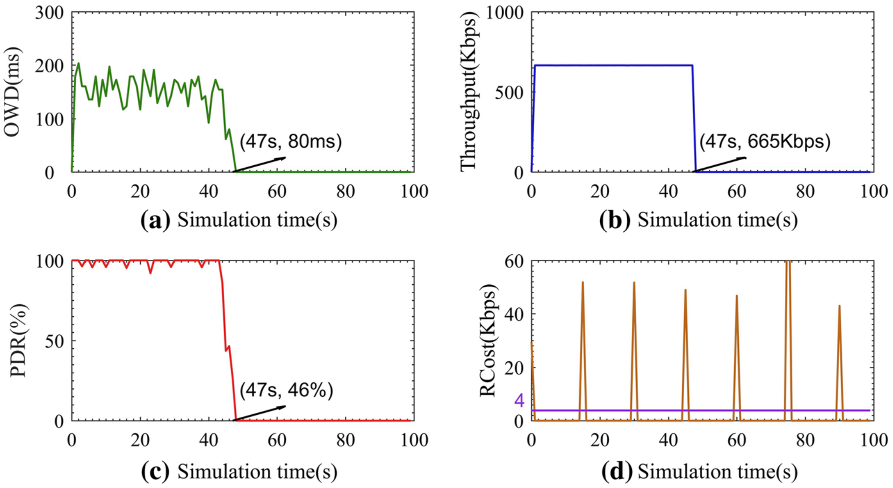
(a) Simulation time(second)

(b) Simulation time(second)

(c) Simulation time(second)

(d) Simulation time(second)

Fig. 4 Network performance with 10 Kbps communication rate



(a) Simulation time(s)

(b) Simulation time(s)

(c) Simulation time(s)

(d) Simulation time(s)

Fig. 5 Network performance with 100 Kbps communication rate

the received packets by the destination to the generated packets by the source. RCost refers to the amount of routing data generated during network operation.

Based on the QSCN model and the foregoing parameters, the simulation results of OWD ($v_1 \rightarrow v_6$), throughput ($v_1 \rightarrow v_6$), PDR ($v_1 \rightarrow v_6$) and RCost of whole network with the average packet intervals of 400 ms (communication rates of 10 Kbps) and 40 ms (100 Kbps) are shown in Figs. 4 and 5, respectively.

From Figs. 4 and 5, it can be seen that there is almost no difference in OWD, throughput and PDR between the two communication rates before the 47th second. However, after the 47th second, the performance in Fig. 4 remains stable. Conversely, the sharp rise of OWD, sharp drop of throughput and PDR in Fig. 5 indicate that the

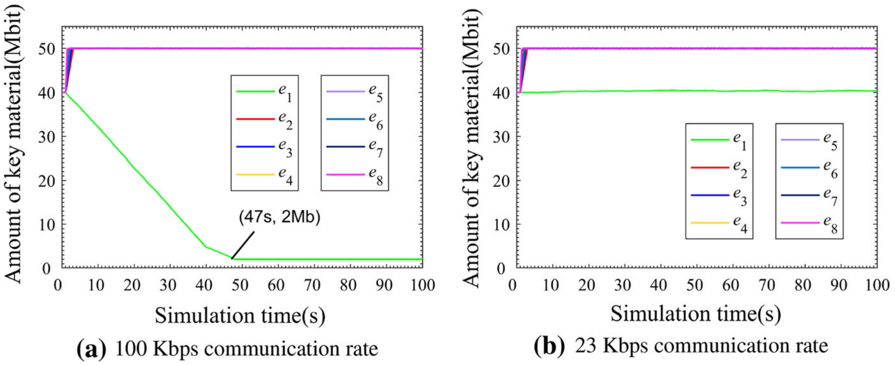


Fig. 6 Key consumption in the SECOQC topology

node v_6 cannot accept any packet from the node v_1. In other words, the network is paralyzed at the 47th second.

4.3 Performance of proposed indicators

4.3.1 ITS communication capability

The simulation results of traditional evaluation indicators show that when the traffic demand exceeds a certain value, the network will paralyze after a certain period of continuous operation. To find out the maximum traffic demand that the QSCN can support stably is very important for the QSCN designer and manager. Therefore, ITS communication capability is proposed and simulated.

In order to explore the reasons for paralysis, the key consumption at the communication rate of 100 Kbps is simulated, as shown in Fig. 6a. Each curve in the figure reflects the key consumption process of a link. Meanwhile, the slope of the curve represents the consumption rate. The initial number of keys of each key pool is set to be 40 Mb. The partners need a small number of pre-shared keys before a new key generation process is established [60,61]. The pre-shared keys are used to guarantee the integrity of the protocol in the first transaction, and it should not be used for any other purposes except to establish a new key generation process. In our simulation, the minimal threshold is set to 2 Mb. From Fig. 6a, it can be concluded that the link with the fastest key consumption rate is e_1. At the 47th second, because the remaining number of keys is below the minimum threshold, this link is "broken".

DSDV routing protocol finds the optimal path based on the principle of minimum hop count. Therefore, the key generation of link e_1 needs to satisfy the communication traffic demand of five pairs of communication partners (v_1, v_2), (v_1, v_3), (v_1, v_4), (v_1, v_5) and (v_1, v_6). Considering that the communication process is bidirectional, the link e_1 will load $5 \times 2 = 10$ times of the one-way traffic demand of one pair of communication partners. According to the topology in Fig. 3, the length of link e_1 is 85 km. By substituting the length into the GLLP theory, the calculated key generation rate is about 233 Kbps. From Fig. 5, the consumption rate of DSDV protocol routing data of whole network is about 4 Kbps. There are eight links in the network, and we can deduce that the routing data consumption of link e_1 is about $4/8 \approx 0.5$ Kbps. Therefore, in order to implement ITS transmission in the QSCN directly, the traffic demand that link e_1 can afford is only about $(233 - 0.5)/(5 \times 2) \approx 23$ Kbps.

Figure 6b shows the key consumption when the communication rate is 23 Kbps. It can be seen that the number of keys of link e_1 maintains the original amount basically. The results demonstrate that the key consumption and key generation on the link e_1 are balanced, which is consistent with the theoretical analysis as above.

4.3.2 ITS communication efficiency

ITS communication capability can indicate the maximal traffic demand that the QSCN is able to support stably. However, when the traffic demand exceeds the ITS communication capability, the QSCN must need a certain recovery time after it operates for some time to maintain a stable communication. The less proportion of recovery time means higher performance. Therefore, the ITS communication efficiency is proposed and simulated, which is the ratio of the ITS operation time to the sum of ITS operation time and ITS recovery time.

The simulation results previously show that, due to the insufficient key generation capability of the QSCN, the communication process can only last 47 s at the communication rate of 100 Kbps. It needs to make clear that the 47 s is the network ITS operation time at the communication rate of 100 Kbps:

$$T_o \approx 47\ s \tag{27}$$

The simulation results previously show that the first paralyzed link is the link e_1. The key generation rate of the link e_1 can be seen from the topology. Therefore, in this simulation, the ITS recovery time of the network depends on the ITS recovery time of the link e_1, which can be calculated as Eq. 28:

$$T_r = \frac{40\,\mathrm{Mb} - 2\,\mathrm{Mb}}{233\,\mathrm{Kbps}} \approx 163\,\mathrm{s} \tag{28}$$

According to Eq. 26, the ITS communication efficiency can be calculated as Eq. 29:

$$Q = \frac{T_o}{T_o + T_r} = \frac{47\,\mathrm{s}}{47\ \ \mathrm{s} + 163\,\mathrm{s}} \approx 22\% \tag{29}$$

From the analysis above, the ITS communication capability and ITS communication efficiency of this QSCN are 23 Kbps and 22%, respectively. Therefore, the QSCN can work stably when the traffic demand is lower than 23 Kbps, such as short message and audio communication. In addition, when the traffic demand is higher than the ITS communication capability, such as real-time video communication, suitable key management mechanism or QKD network improvement needs to be designed accordingly.

5 Conclusion

In this paper, a practical QSCN model is proposed and the three major improvements include (I) the volatility of traffic demand of classical network is modeled by the Poisson stochastic process; (II) the capability of key generation in QKD network is calculated by the GLLP theory; and (III) two performance indicators are proposed, which are ITS communication capability and ITS communication efficiency. In addition, the simulation is designed based on the QSCN model with the topology of the SECOQC network and the DSDV routing protocol. The plentiful simulation results verified the accuracy of the proposed QSCN model and the necessity of the proposed performance indicators. In the further, we plan to design better QKD device deployment and routing protocols to improve the ITS communication capability and the ITS communication efficiency.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant Numbers 61771168, 61702224), Space Science and Technology Advance Research Joint Funds (6141B061 10105).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**(12), 7–11 (2014)
2. Chen, X.B., Tang, X., Xu, G., Dou, Z., Chen, Y.L., Yang, Y.X.: Cryptanalysis of secret sharing with a single d-level quantum system. Quantum Inf. Process. **17**(9), 225 (2018)
3. Xu, G., Chen, X.B., Dou, Z., Yang, Y.X., Li, Z.: A novel protocol for multiparty quantum key management. Quantum Inf. Process. **14**(8), 2959–2980 (2015)
4. Chen, X.B., Sun, Y.R., Xu, G., Jia, H.Y., Qu, Z., Yang, Y.X.: Controlled bidirectional remote preparation of three-qubit state. Quantum Inf. Process. **16**(10), 244 (2017)
5. Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., Yeh, H.: Current status of the DARPA quantum network. In: Donkor, E.J., Pirich, A.R., Brandt, H.E. (eds.) Quantum Information and Computation III, vol. 5815, pp. 138–149. International Society for Optics and Photonics (2005). https://doi.org/10.1117/12.606489
6. Elliott, C., Yeh, H.: Darpa quantum network testbed. Technical report, BBN Technologies, Cambridge, MA (2007)
7. Alleaume, R., Roueff, F., Diamanti, E., Lütkenhaus, N.: Topological optimization of quantum key distribution networks. New J. Phys. **11**(7), 075002 (2009)
8. Dianati, M., Alléaume, R.: Architecture of the SECOQC quantum key distribution network. In: 2007 first international conference on quantum, nano, and micro technologies ICQNM'07, IEEE, pp. 13–13 (2007)
9. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., et al.: Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19**(11), 10387–10409 (2011)
10. Chen, L.K., Yong, H.L., Xu, P., Yao, X.C., Xiang, T., Li, Z.D., Liu, C., Lu, H., Liu, N.L., Li, L., et al.: Experimental nested purification for a linear optical quantum repeater. Nat. Photonics **11**(11), 695 (2017)
11. Yuan, Z., Plews, A., Takahashi, R., Doi, K., Tam, W., Sharpe, A., Dixon, A., Lavelle, E., Dynes, J., Murakami, A., et al.: 10-mb/s quantum key distribution. J. Lightwave Technol. **36**(16), 3427–3433 (2018)
12. Dixon, A.R., Yuan, Z., Dynes, J., Sharpe, A., Shields, A.: Continuous operation of high bit rate quantum key distribution. Appl. Phys. Lett. **96**(16), 161102 (2010)

13. Yin, H.L., Chen, T.Y., Yu, Z.W., Liu, H., You, L.X., Zhou, Y.H., Chen, S.J., Mao, Y., Huang, M.Q., Zhang, W.J., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. **117**(19), 190501 (2016)
14. Liao, S.K., Cai, W.Q., Liu, W.Y., Zhang, L., Li, Y., Ren, J.G., Yin, J., Shen, Q., Cao, Y., Li, Z.P., et al.: Satellite-to-ground quantum key distribution. Nature **549**(7670), 43 (2017)
15. Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., et al.: The SECOQC quantum key distribution network in Vienna. New J. Phys. **11**(7), 075001 (2009)
16. Razavi, M.: An introduction to quantum communications networks. 2053-2571. Morgan & Claypool Publishers (2018). https://doi.org/10.1088/978-1-6817-4653-1
17. Watanabe, S., Matsumoto, R., Uyematsu, T.: Security of quantum key distribution protocol with two-way classical communication assisted by one-time pad encryption. arXiv:quant-ph/0608030 (2006)
18. Dianati, M., Alléaume, R., Gagnaire, M., Shen, X.: Architecture and protocols of the future european quantum key distribution network. Secur. Commun. Netw. **1**(1), 57–74 (2008)
19. Diamanti, E., Lo, H.K., Qi, B., Yuan, Z.: Practical challenges in quantum key distribution. NPJ Quantum Inf. **2**, 16025 (2016)
20. Li, J., Chen, X.B., Xu, G., Yang, Y.X., Li, Z.P.: Perfect quantum network coding independent of classical network solutions. IEEE Commun. Lett. **19**(2), 115–118 (2015)
21. Li, J., Chen, X., Sun, X., Li, Z., Yang, Y.: Quantum network coding for multi-unicast problem based on 2d and 3d cluster states. Sci. China Inf. Sci. **59**(4), 042301 (2016)
22. Xu, G., Chen, X.B., Li, J., Wang, C., Yang, Y.X., Li, Z.: Network coding for quantum cooperative multicast. Quantum Inf. Process. **14**(11), 4297–4322 (2015)
23. Maurhart, O., Pacher, C., Happe, A., Lor, T., Tamas, C., Poppe, A., Peev, M.: New release of an open source QKD software: design and implementation of new algorithms, modularization and integration with IPSec. In: Proceedings of Qcrypt Citeseer (2013)
24. Yang, C., Zhang, H., Su, J.: The qkd network: model and routing scheme. J. Mod. Opt. **64**(21), 2350–2362 (2017)
25. Mehic, M., Maurhart, O., Rass, S., Voznak, M.: Implementation of quantum key distribution network simulation module in the network simulator ns-3. Quantum Inf. Process. **16**(10), 253 (2017)
26. Salvail, L., Peev, M., Diamanti, E., Alléaume, R., Lütkenhaus, N., Länger, T.: Security of trusted repeater quantum key distribution networks. J. Comput. Secur. **18**(1), 61–87 (2010)
27. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**(3), 1301 (2009)
28. Henderson, T.R., Lacage, M., Riley, G.F., Dowell, C., Kopena, J.: Network simulations with the ns-3 simulator. SIGCOMM Demonstr. **14**(14), 527 (2008)
29. Gelfond, R., Berzanskis, A.: Key management and user authentication for quantum cryptography networks. US Patent 8,340,298, (2012)
30. Poppe, A., Peev, M., Maurhart, O.: Outline of the secoqc quantum-key-distribution network in Vienna. Int. J. Quantum Inf. **6**(02), 209–218 (2008)
31. Mehic, M., Maurhart, O., Rass, S., Komosny, D., Rezac, F., Voznak, M.: Analysis of the public channel of quantum key distribution link. IEEE J. Quantum Electron. **53**(5), 1–8 (2017)
32. McHale, J.F.: Communication server apparatus and method. US Patent 5,668,857, (1997)
33. Weigle, M.C., Adurthi, P., Hernández-Campos, F., Jeffay, K., Smith, F.D.: Tmix: a tool for generating realistic tcp application workloads in ns-2. ACM SIGCOMM Comput. Commun. Rev. **36**(3), 65–76 (2006)
34. Varet, A., Larrieu, N.: How to generate realistic network traffic? In: 2014 IEEE 38th annual computer software and applications conference, pp. 299–304. IEEE (2014)
35. Bonelli, N., Giordano, S., Procissi, G., Secchi, R.: Brute: A high performance and extensible traffic generator. In: Proceedings of SPECTS, pp. 839–845 (2005)
36. Ammar, D., Begin, T., Guerin-Lassous, I.: A new tool for generating realistic internet traffic in ns-3. In: Proceedings of the 4th international ICST conference on simulation tools and techniques, pp. 81–83 (2011)
37. Botta, A., Dainotti, A., Pescapé, A.: A tool for the generation of realistic network workload for emerging networking scenarios. Comput. Netw. **56**(15), 3531–3547 (2012)
38. Gardiner, C.: Stochastic Methods, vol. 4. Springer, Berlin (2009)
39. Tamaki, K., Lo, H.K., Wang, W., Lucamarini, M.: Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. arXiv:1805.05511 (2018)

40. Gottesman, D., Lo, H.K., Lutkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. In: International symposium on information theory, 2004. ISIT 2004. Proceedings, p. 136. IEEE (2004)
41. Tang, Z., Wei, K., Bedroya, O., Qian, L., Lo, H.K.: Experimental measurement-device-independent quantum key distribution with imperfect sources. Phys. Rev. A **93**(4), 042308 (2016)
42. Zhou, Y.H., Yu, Z.W., Wang, X.B.: Making the decoy-state measurement-device-independent quantum key distribution practically useful. Phys. Rev. A **93**(4), 042324 (2016)
43. Tang, Y.L., Yin, H.L., Zhao, Q., Liu, H., Sun, X.X., Huang, M.Q., Zhang, W.J., Chen, S.J., Zhang, L., You, L.X., et al.: Measurement-device-independent quantum key distribution over untrustful metropolitan network. Phys. Rev. X **6**(1), 011024 (2016)
44. Lucamarini, M., Yuan, Z.L., Dynes, J.F., Shields, A.J.: Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature **557**(7705), 400 (2018)
45. Rosenberg, D., Harrington, J.W., Rice, P.R., Hiskett, P.A., Peterson, C.G., Hughes, R.J., Lita, A.E., Nam, S.W., Nordholt, J.E.: Long-distance decoy-state quantum key distribution in optical fiber. Phys. Rev. Lett. **98**(1), 010503 (2007)
46. Zhao, Y., Qi, B., Ma, X., Lo, H.K., Qian, L.: Experimental quantum key distribution with decoy states. Phys. Rev. Lett. **96**(7), 070502 (2006)
47. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**(2), 022320 (2006)
48. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**(13), 130503 (2012)
49. Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J.G., et al.: Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys. Rev. Lett. **98**(1), 010504 (2007)
50. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**(5), 052319 (2004)
51. Braunstein, S.L., Pirandola, S.: Side-channel-free quantum key distribution. Phys. Rev. Lett. **108**(13), 130502 (2012)
52. Ma, X., Qi, B., Zhao, Y., Lo, H.K.: Practical decoy state for quantum key distribution. Phys. Rev. A **72**(1), 012326 (2005)
53. Ma, X., Fung, C.H.F., Razavi, M.: Statistical fluctuation analysis for measurement-device-independent quantum key distribution. Phys. Rev. A **86**(5), 052305 (2012)
54. Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.K.: Finite-key analysis for measurement-device-independent quantum key distribution. Nat. Commun. **5**, 3732 (2014)
55. Yin, H.L., Cao, W.F., Fu, Y., Tang, Y.L., Liu, Y., Chen, T.Y., Chen, Z.B.: Long-distance measurement-device-independent quantum key distribution with coherent-state superpositions. Opt. Lett. **39**(18), 5451–5454 (2014)
56. Perkins, C.E., Bhagwat, P.: Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In: ACM SIGCOMM computer communication review. vol. 24, pp. 234–244. ACM (1994)
57. Almes, G., Kalidindi, S., Zekauskas, M., Morton, A.: A one-way delay metric for ip performance metrics (ippm). Technical report (2016)
58. Burgess, N.: Rfc 2544 testing of ethernet services in telecom networks. White paper (2004)
59. Evans, S.C., Pearlman, M.R., Hartman, M.J., Rothe, A., Leiva, M.A., Egan, M.W.: Routing cost based network congestion control for quality of service. US Patent 7,489,635, (2009)
60. Dodson, D., Fujiwara, M., Grangier, P., Hayashi, M., Imafuku, K., Kitayama, K.i., Kumar, P., Kurtsiefer, C., Lenhart, G., Luetkenhaus, N., et al.: Updating quantum cryptography report ver. 1. arXiv:0905.4325 (2009)
61. Cederlof, J., Larsson, J.Å.: Security aspects of the authentication used in quantum cryptography. IEEE Trans. Inf. Theory **54**(4), 1735–1741 (2008)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.