SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2022, Vol. 65 182303:1–182303:16
https://doi.org/10.1007/s11432-021-3262-3

Outage-driven link selection for secure buffer-aided networks

Dawei WANG[1,2,3], Tianmi HE[1], Fuhui ZHOU[4,5*], Julian CHENG[6], Ruonan ZHANG[1] & Qihui WU[4,5]

[1]*School of Electronics and Information, Northwestern Polytechnical University, Xi'an* 710072*, China;*
[2]*Research & Development Institute of Northwestern Polytechnical University in Shenzhen, Shenzhen* 518057*, China;*
[3]*National Mobile Communications Research Laboratory, Southeast University, Nanjing* 210096*, China;*
[4]*College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing* 210000*, China;*
[5]*Key Laboratory of Dynamic Cognitive System of Electromagnetic Spectrum Space, Nanjing University of Aeronautics and Astronautics, Nanjing* 210000*, China;*
[6]*School of Engineering, The University of British Columbia, Kelowna* V1V1V7*, Canada*

Received 21 January 2021/Revised 27 April 2021/Accepted 12 May 2021/Published online 26 July 2022

Abstract In this paper, we investigate secure communication in a two-hop wireless network, where multiple buffer-aided relays assist to securely forward data from the sender to the destination threatened by a passive eavesdropper. To satisfy the security and delay requirements, we propose a novel link selection policy without the instantaneous wiretap channel state information. Different from the most current link selection policies, the proposed link selection policy is designed by joint considering the link secrecy outage probability and the buffer states. To evaluate the secrecy performance, we first characterize the system state transition matrix and the stationary state probability, and then derive the closed-form expressions for the secrecy outage probability and the secrecy rate. Moreover, we formulate a framework based on the queuing theory to analyze the end-to-end information delay at the source, the relays, and the queues, and derive the closed-form expression for the information delay. Finally, we conduct simulations to validate our theoretical performance analysis, and verify the performance improvement of the proposed outage-driven secure transmission scheme in terms of secrecy outage probability and information delay.

Keywords buffer-aided relay, information delay, link selection, secrecy outage probability

Citation Wang D W, He T M, Zhou F H, et al. Outage-driven link selection for secure buffer-aided networks. Sci China Inf Sci, 2022, 65(8): 182303, https://doi.org/10.1007/s11432-021-3262-3

1 Introduction

The rapid proliferation of wireless technologies and devices generates a large amount of personal information, such as bank account information, health information, and location information [1]. However, the open pervasion nature of the wireless signals makes privacy information susceptible to be eavesdropped, since any user can acquire the wireless signals within its transmission range. Although the upper-layer encryption algorithms can provide information protection for the wireless networks, these algorithms assume limited computing ability at the eavesdroppers, which are challenged by the rapid hardware development [2]. In addition, the complex secret key generation and management limit the upper-layer algorithms' applications in the energy and hardware constrained communication scenarios, such as the massive machine type of communication scenarios. Recently, physical-layer security, which employs the physical characteristic of the wireless channel to encrypt the privacy information, has attracted much research attention [3,4]. The initial physical-layer security model, known as the wiretap channel model, was conducted by Wyner, who proved that the physical-layer security can provide perfect information-theory security [5], when the legitimate channel is better than the wiretap channel. Subsequently, Wyner's work was extended to the broadcast channel [6] and the Gaussian channel [7]. In these studies, the secrecy

* Corresponding author (email: zhoufuhui@ieee.org)

performance is evaluated by the secrecy rate, which is defined as the difference between the legitimate channel rate and the wiretap channel rate.

Cooperative relaying and jamming are two main physical-layer security methods to protect the privacy information [8]. For the cooperative relaying method, one or multiple relays are employed to forward the privacy information and improve the legitimate information rate [9, 10]. For the cooperative jamming method, the cooperative users interfere with the wiretap channel while minimizing the impact on the legitimate users [11]. In addition, beamforming technique [12, 13], antenna selection [14], relay selection [15], and full-duplex [16, 17] are adopted to further improve the secrecy performance. However, the fixed relaying mode, where the source transmits the privacy information in the first slot and the relay forwards the information in the following slot, can cause network performance degradation, since the network performance is constrained by the weak link. Introducing a buffer at the relay can alleviate the above situation, as the received information can be stored in the data buffer and the system can flexibly select the suitable links from the source-to-relay link and relay-to-destination link [18, 19] to improve secrecy performance [20–22].

Recently, there have been several studies focusing on buffer-aided relay technique to protect the primary information [23–32]. In these studies, the information can be stored at the relay's buffer to wait for the secure transmission opportunities [23–27] and then, the randomize-and-forward or decode-and-forward relay policy is adopted for the secure forwarding [24]. When the buffer-aided relay is energy limited, the harvested energy technique will power the relay, and the joint power allocation and link selection strategies were proposed [25–27]. For the case with multiple relays, the relay selection technique was employed to further improve the link selection diversity [28–31]. The information delay for the buffer-aided secure relay networks was also analyzed by considering the exact and average wiretap channel state information (CSI) [32]. When the relays are untrusted, the privacy data with both strong and trusted links were aligned to protect the privacy information [30]. Equipped with multiple antennas at the relays, a joint relay and antenna selection policy was proposed [31] to protect the privacy information. Besides, closed-form expressions of the secrecy outage probabilities with the instantaneous and average wiretap CSI were derived. In the above studies, the best link is selected from the source-to-relay and relay-to-destination links, and closed-form expressions of the secrecy outage probability were derived.

Although the existing studies have promoted the development of buffer-aided secure relay networks, several open issues are remained to be tackled. First, Refs. [23–32] proposed the corresponding link selection policies to protect the privacy information. However, these policies just select the best link from the source-to-relay and relay-to-destination links, while the link secrecy outage is not considered. For example, when the best link suffers from secrecy outage, the transmitter still utilizes this link for the privacy information transmission which will experience secrecy outage. Second, introducing buffers at the relays will increase the information delay, and the performance of such information delay was not investigated in previous studies [23–31]. Although the information delay was considered in a recent study [32], the additional information delay caused by the secrecy outage was ignored. Therefore, since both the secrecy outage probability and information delay are affected by the link selection, it is necessary to investigate the secrecy outage and information delay when studying secure link selection schemes.

Motivated by the discussions above, we propose a new outage-driven secure transmission policy for buffer-aided two-hop networks, and investigate the secrecy outage-driven link selection, secrecy performance, and information delay. The contributions of this paper are summarized as follows.

• We propose a novel secrecy outage-driven link selection policy for the buffer-aided two-hop relay networks. In the proposed scheme, considering the partial CSI of the wiretap channels, we analyze the secrecy outage probability for all source-to-relays and relays-to-destination links. Under the constraint of the maximum permitted secrecy outage probability, we derive the lower bound of the legitimate channel, under which the privacy information can be securely transmitted. Based on this lower bound, a new secrecy outage-driven link selection policy is proposed. This policy is different from the previous studies [28–33] that ignore the secrecy event in the link selection. To the best of the authors' knowledge, this is the first work that investigates the secure link selection by considering the secrecy outage probability for multiple relays.

• Based on the proposed link selection policy, we formulate a Markov chain to characterize the system state transition and derive the corresponding transition matrix. According to the stationary system states, we analyze the information secrecy outage probability and the average secrecy rate for the proposed scheme, and derive their closed-form expressions.

• To analyze the information delay, we formulate another Markov chain to characterize the system

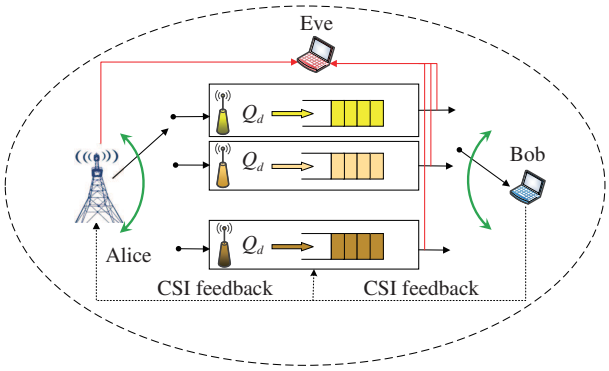

Figure 1 (Color online) A diagram of the proposed buffer-aided secure transmission.

states between the source and relays, and formulate another Markov chain to characterize the system states between the relays and the destination. According to the queuing theory, we derive the closed-form expression of the information delay, including the delay at the source's queue, the delay at the relays for link selection, and the delay at the relays' queue. The information delay is different from [32], since we consider the information delay when the system is waiting for secure transmission links.

The rest of this paper is organized as follows. Section 2 describes the system model of the considered two-hop network. In Section 3, we first propose the secure link selection. Following the above policy, we analyze the stationary system state. In Section 4, we analyze secrecy performance and information delay for the proposed scheme. Extensive simulations are presented in Section 5, and Section 6 concludes the paper.

2 System model

Figure 1 illustrates the system model, where Alice desires to transmit privacy information to Bob, and the legitimate link is eavesdropped by Eve. The direct channel between Alice and Bob is assumed to be poor due to the large scale fading or interference, which can be ignored. Therefore, Alice requires relays to forward privacy information to Bob. There are M relays, denoted by R_i ($i \in \{1, 2, \ldots, M\}$), utilizing the decode-and-forward (DF) relay protocol[1)] to securely forward the privacy information. We consider the worst case scenario where the eavesdropper can intercept the privacy information from both Alice and the relays. Similar to [32], Alice and the relays adopt different codebooks, thus the eavesdroppers cannot combine the received signals from Alice and relay for decoding. Each relay has only one antenna operating in the half-duplex mode with a buffer, denoted by Q_i for R_i, to store the privacy information. All the buffers have the maximum buffer length L.

In this system, each frame is equally divided into a series of time slots and the duration of each time-slot is denoted as T [34, 35]. In each time slot, a relay is scheduled to receive or transmit the privacy information. All channels experience block, Rayleigh, and flat fading, which means that in one scheduling slot, the CSI remains constant and the CSI varies independently in different scheduling slots [36, 37]. The channels Alice $\rightarrow R_i$, Alice $\rightarrow$ Eve, $R_i \rightarrow$ Bob, and $R_i \rightarrow$ Eve are denoted by h_{ar_i}, h_{ae}, h_{r_ib}, and h_{r_ie}, respectively. The corresponding channel power gains are denoted by $g_{ar_i} = |h_{ar_i}|^2$, $g_{ae} = |h_{ae}|^2$, $g_{r_ib} = |h_{r_ib}|^2$, and $g_{r_ie} = |h_{r_ie}|^2$, which follow exponential distributions with parameters λ_{ar}, λ_{ae}, λ_{rb}, and λ_{re}, respectively. Through pilot estimation, the CSI of Alice-to-relays and relays-to-Bob is available. For practical consideration, the wiretap CSI is unavailable since Eve is passive and we only has the channel distribution information (CDI) for g_{ae} and g_{r_ie} [38, 39]. Moreover, we assume that the received noises are cyclic complex Gaussian random variables with mean zero and variance N_0.

To securely transmit the privacy information, the wiretap coding is adopted to encrypt the privacy information, and the target secrecy rate and the target transmit rate are set to be R_s and R_b, respectively. The rate redundancy $R_b - R_s$ is available against the eavesdropping. When R_i is selected to receive Alice's

1) Since Alice and the relays utilize difference codebooks in the decode-and-forward relay protocol, the eavesdropper cannot utilize the combined scheme to process the signal in both hops. Therefore, the secrecy rate will increase. The proposed scheme can be extended to the other relay protocols. However, in order to improve the secrecy performance and simply the mathematic analysis, we utilize the decode-and-forward relay protocol.

privacy information in the tth time slot, the received signal is

$$y_{r_i}[t] = \sqrt{P_a} h_{ar_i}[t] x_a[t] + n_{r_i}[t], \tag{1}$$

where P_a is Alice's transmit power; $h_{ar_i}[t]$ is the channel coefficient between Alice and R_i in the tth time slot; $x_a[t]$ is Alice's privacy information in the tth time slot, which is normalized as $\mathrm{E}\{|x_a[t]|^2\} = 1$ and $\mathrm{E}\{\cdot\}$ denotes the expectation operation; $n_{r_i}[t]$ is the received noise at R_i in the tth time slot. After receiving the privacy information, R_i decodes the privacy information and stores the privacy information in its buffer. Meanwhile, the privacy information is eavesdropped by Eve as

$$y_{e_i,1}[t] = \sqrt{P_a} h_{ae}[t] x_a[t] + n_e[t], \tag{2}$$

where $h_{ae}[t]$ is the channel coefficient between Alice and Eve in the tth time slot; $n_e[t]$ is the received noise at Eve in the tth time slot. After k time slots, if R_i is scheduled to transmit the stored privacy information in the $(t+k)$th time slot, the received signal at Bob is shown as

$$y_b[t+k] = \sqrt{P_r} h_{r_i b}[t+k] x_{r_i}[t+k] + n_b[t+k], \tag{3}$$

where P_r is R_i's transmit power; $h_{r_i b}[t+k]$ is the channel coefficient between R_i and Bob in the $(t+k)$th time slot; $x_{r_i}[t+k]$ is Alice's privacy information in the $(t+k)$th time slot, which is normalized as $\mathrm{E}\{|x_{r_i}[t]|^2\} = 1$; $n_b[t+k]$ is the received noise at Bob in the $(t+k)$th time slot. Similarly, Eve eavesdrops the privacy information as

$$y_{e_i,2}[t+k] = \sqrt{P_r} h_{r_i e}[t+k] x_{r_i}[t+k] + n_e[t+k], \tag{4}$$

where $h_{r_i e}[t+k]$ is the channel coefficient between R_i and Eve in the $(t+k)$th time slot; $n_e[t+k]$ is the received noise at Eve in the $(t+k)$th time slot.

In this system, the privacy information at Alice and the relays are threatened by the eavesdropping. Assisted by the data buffers and the relays, the system can schedule one relay to securely receive or forward the privacy information. Moreover, we propose a secure outage-driven link selection policy to confirm the secure transmission. In the following, we will interpret the secrecy outage probability and information delay.

3 Secrecy outage-driven buffer-aided relay transmission scheme

In this section, we first analyze the secrecy outage probability of the privacy information. Then, we will propose a secure outage driven link selection policy and analyze the stationary state of the two-hop relay network.

3.1 Secrecy transmission link selection policy

When R_i is selected to receive Alice's privacy information in the tth time slot, the information rate at R_i is derived as

$$R_{ar_i}[t] = \log_2\left(1 + \frac{P_a g_{ar_i}[t]}{N_0}\right). \tag{5}$$

In addition, Eve also receives the privacy information and the wiretap rate at Eve is derived as

$$R_{ae}[t] = \log_2\left(1 + \frac{P_a g_{ae}[t]}{N_0}\right). \tag{6}$$

Therefore, for the first hop, the secrecy rate, which is the rate difference between the legitimate channel and the wiretap channel, in the tth time slot is derived as

$$R_{ai,\mathrm{sec}}[t] = \left(R_{ar_i}[t] - R_{ae}[t]\right)^+, \tag{7}$$

where $(a)^+ = \max(a, 0)$. Since the wiretap CSI is unavailable at Eve, we evaluate the secrecy performance by the secrecy outage probability, where a secrecy outage occurs when the secrecy rate is less than the target secrecy rate. Therefore, the secrecy outage probability for the first hop is derived as [40]

$$P_{ai,\mathrm{out}}[t] = \Pr\left\{R_{ai,\mathrm{sec}}[t] < R_s\right\}$$

$$= \Pr\left\{g_{ae} > 2^{-R_s}\left(1+\frac{P_a g_{ar_i}[t]}{N_0}\right)\frac{N_0}{P_a} - \frac{N_0}{P_a}\right\}$$
$$= \exp\left(-\left(2^{-R_s}\left(1+\frac{P_a g_{ar_i}[t]}{N_0}\right)\frac{N_0}{\lambda_{ae}P_a} - \frac{N_0}{\lambda_{ae}P_a}\right)\right). \tag{8}$$

Setting the maximum permitted secrecy outage probability as $P_{\text{out}}^{\text{upper}}$, the link between Alice and R_i in the tth time slot is secure only when $P_{ai,\text{out}}[t] < P_{\text{out}}^{\text{upper}}$. Therefore, we can derive the secure link quality in the first hop as

$$\begin{aligned} P_{ai,\text{out}}[t] \leqslant P_{\text{out}}^{\text{upper}} &\Leftrightarrow \exp\left(-\left(2^{-R_s}\left(1+\frac{P_a g_{ar_i}[t]}{N_0}\right)\frac{N_0}{\lambda_{ae}P_a} - \frac{N_0}{\lambda_{ae}P_a}\right)\right) \leqslant P_{\text{out}}^{\text{upper}} \\ &\Leftrightarrow -\left(2^{-R_s}\left(1+\frac{P_a g_{ar_i}[t]}{N_0}\right)\frac{N_0}{\lambda_{ae}P_a} - \frac{N_0}{\lambda_{ae}P_a}\right) \leqslant \ln P_{\text{out}}^{\text{upper}} \\ &\Leftrightarrow g_{ar_i}[t] \geqslant \Upsilon_{ar} = \frac{N_0(2^{R_s}-1)}{P_a} - \lambda_{ae}2^{R_s}\ln P_{\text{out}}^{\text{upper}}. \end{aligned} \tag{9}$$

When $P_{ai,\text{out}}[t] < P_{\text{out}}^{\text{upper}}$, $g_{ar_i}[t] \geqslant \Upsilon_{ar}$. Therefore, the selected secure link between Alice and relays should satisfy $g_{ar_i}[t] \geqslant \Upsilon_{ar}$ ($i \in \{1,2,\ldots,M\}$)[2)].

Similarly, for the second hop, if R_i is scheduled to forward the privacy information in the $(t+k)$th time slot, the information rates at Bob and Eve are derived as

$$\begin{cases} R_{r_ib}[t+k] = \log_2\left(1+\dfrac{P_r g_{r_ib}[t+k]}{N_0}\right), \\ R_{r_ie}[t+k] = \log_2\left(1+\dfrac{P_r g_{r_ie}[t+k]}{N_0}\right). \end{cases} \tag{10}$$

Therefore, the secrecy rate for the second hop in the $(t+k)$th time slot is $R_{ib,\text{sec}}[t+k] = (R_{r_ib}[t+k] - R_{r_ie}[t+k])^+$, and the secrecy outage probability for the second hop is derived as

$$P_{ib,\text{out}}[t+k] = \Pr\left\{R_{ib,\text{sec}}[t+k] < R_s\right\} = \exp\left(\frac{N_0}{\lambda_{re}P_r} - \frac{2^{-R_s}N_0}{\lambda_{re}P_r}\left(1+\frac{P_r g_{r_ib}[t+k]}{N_0}\right)\right). \tag{11}$$

According to the maximum permitted secrecy outage probability $P_{\text{out}}^{\text{upper}}$, the link between R_i and Bob is secure in the $(t+k)$th time slot if $P_{ib,\text{out}}[t+k] < P_{\text{out}}^{\text{upper}}$. Then, we can derive

$$P_{ib,\text{out}}[t+k] \leqslant P_{\text{out}}^{\text{upper}} \Leftrightarrow g_{r_ib}[t+k] \geqslant \Upsilon_{rb} \triangleq \frac{N_0\left(2^{R_s}-1\right)}{P_r} - \lambda_{re}2^{R_s}\ln P_{\text{out}}^{\text{upper}}. \tag{12}$$

When $P_{ib,\text{out}}[t+k] < P_{\text{out}}^{\text{upper}}$, we can derive $g_{ar_i}[t+k] \geqslant \Upsilon_{rb}$. Therefore, the selected secure link between the relays and Bob should satisfy $g_{r_ib}[t+k] \geqslant \Upsilon_{rb}$.

According to the above discussion, the links in the first hop are secure only when $g_{ar_i} \geqslant \Upsilon_{ar}$ and the links in the second hop are secure only when $g_{ar_i} \geqslant \Upsilon_{rb}$ ($i \in \{1,2,\ldots,M\}$). Considering all the links in the system, we select the transmission link at each slot with the policy

$$R_{\text{opt}} = \arg\max_{R_k}\left(\frac{\max\limits_{R_k:\Psi(Q_k)\neq L, g_{ar_k}[i]\geqslant\Upsilon_{ar}} g_{ar_k}[i]}{\lambda_{ae}}, \frac{\max\limits_{R_k:\Psi(Q_k)\neq 0, g_{r_kb}[i]\geqslant\Upsilon_{rb}} g_{r_kb}[i]}{\lambda_{re}}\right), \tag{13}$$

where $\Psi(Q_k)$ is the buffer state of R_k. In (13), the term $\frac{\max\limits_{R_k:\Psi(Q_k)\neq L, g_{ar_k}[i]\geqslant\Upsilon_{ar}} g_{ar_k}[i]}{\lambda_{ae}}$ indicates that the link between Alice and the relay is secure with the best channel quality and the corresponding relay's buffer is not full; the term $\frac{\max\limits_{R_k:\Psi(Q_k)\neq 0, g_{r_kb}[i]\geqslant\Upsilon_{rb}} g_{r_kb}[i]}{\lambda_{re}}$ indicates that the link between the relay and Bob is secure with the best channel quality and the corresponding relay's buffer is not empty. Therefore, only one relay will be selected in each time slot for receiving or transmitting. Adopting the proposed policy in (13),

2) The constraint $g_{ar_i}[t] \geqslant \Upsilon_{ar}$ will show the available secure links between Alice and the relays. Then, in the following link selection policy, we will select one relay for transmitting or receiving from the available secure link.

the selected link not only provides information security but also improves the transmission efficiency. To the best of the authors' knowledge, this is the first work that considers the information secrecy outage in the link selection. Moreover, the proposed relay selection policy is different from the current buffer-aided secure relay selection schemes as we consider the secrecy outage constraint during the relay selection process.

3.2 Stationary states under the proposed link selection policy

According to the proposed link selection policy, a link is secure only when it satisfies $g_{ar_i} \geqslant \Upsilon_{ar}$ or $g_{r_ib} \geqslant \Upsilon_{rb}$. Otherwise, there is no available secure transmission link. The probability of no secure link is derived as

$$\begin{aligned} P_{\text{null}} &= \prod_{i=1}^{M} \Pr\left\{g_{ar_i} < \Upsilon_{ar}\right\} \Pr\left\{g_{r_ib} < \Upsilon_{rb}\right\} \\ &= \left(1 - \exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M} \left(1 - \exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M}, \end{aligned} \tag{14}$$

where the subscript null denotes the probability that there is no available link for the secure transmission. Therefore, the system has at least one secure transmission link with probability $1 - P_{\text{null}}$.

When a link in the first hop is secure and available, it should satisfy $g_{ar_i} \geqslant \Upsilon_{ar}$ and $Q_i \neq L$ ($i \in \{1, 2, \ldots, M\}$). Therefore, in the tth time slot, we assume that there are at least M_1 available secure links in the first hop with probability as

$$P_{\text{first}}(M_1) = \sum_{k=M_1}^{M} \left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k} \left(1 - \exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k}, \tag{15}$$

where the superscript first denotes the first hop. Eq. (15) indicates that there are at least M_1 secure links in the first hop. When a link in the second hop is secure and available, it should satisfy $g_{r_ib} < \Upsilon_{rb}$ and $Q_i > 0$ ($i \in \{1, 2, \ldots, M\}$). In the tth time slot, we assume that there are M_2 available secure links in the second hop with probability

$$P_{\text{second}}(M_2) = \sum_{k=M_2}^{M} \left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k} \left(1 - \exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k}, \tag{16}$$

where the superscript of second denotes the second hop. Eq. (16) indicates that there are at least M_2 secure links in the second hop.

The state space for the buffer-aided two-hop relay network in the tth time slot is denoted by s_n which is given by

$$s_n = \left[\vartheta_{s_n}(Q_1), \vartheta_{s_n}(Q_2), \ldots, \vartheta_{s_n}(Q_M)\right], \tag{17}$$

where $\vartheta_{s_n}(Q_k)$ denotes R_k's buffer state at s_n, which is the number of bits in R_k's buffer. Since each buffer can store L bits, there are $(L+1)^M$ states for the network having M relays. In the $(t+1)$th time slot, a relay is selected to receive or forward the secrecy information, and the system state will transfer to state s_l. When a link from Alice to a relay is selected for the privacy information transmission, the buffer at this relay will increase and we denote this event by Ω_l^+. Otherwise, when a link from a relay to Bob is selected in the $(t+1)$th time slot for forwarding the privacy information, the buffer at this relay will decrease and we denote this event by Ω_l^-. Since all the links of Alice to the relays and the relays to Bob are independent identically distributed, the system will equally select the links from Alice to a relay and from a relay to Bob. Therefore, according to the above discussion, the probability that the system

state transfers from s_n to s_l in the tth time-slot is derived as

$$a_{n,l}=\begin{cases}\sum\limits_{k_1=M_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=M_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2}\\ \quad\times\frac{\left(1-(1-\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}}))^{M}(1-\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}}))^{M}\right)}{M_2}\left(\frac{\lambda_{re}M_2}{\lambda_{rb}\exp\left(-\frac{M_1\Upsilon_{ar}}{\lambda_{ar}}-\frac{(M_2-1)\Upsilon_{rb}}{\lambda_{rb}}\right)}\right.\\ \quad\left.\times\sum\limits_{i=0}^{M_1}\sum\limits_{i=0}^{M_2-1}C_{M_1}^{i}C_{M_2-1}^{i}(-1)^{i+j}\frac{\lambda_{rb}\lambda_{ar}}{(j+1)\lambda_{re}\lambda_{ar}+i\lambda_{ae}\lambda_{rb}}\right),\quad s_l\in\Omega^{+},\\ \sum\limits_{k_1=M_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=M_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2}\\ \quad\times\frac{\left(1-(1-\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}}))^{M}(1-\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}}))^{M}\right)}{M_1}\left(1-\frac{\lambda_{re}M_2}{\lambda_{rb}\exp\left(-\frac{M_1\Upsilon_{ar}}{\lambda_{ar}}-\frac{(M_2-1)\Upsilon_{rb}}{\lambda_{rb}}\right)}\right.\\ \quad\left.\times\sum\limits_{i=0}^{M_1}\sum\limits_{i=0}^{M_2-1}C_{M_1}^{i}C_{M_2-1}^{i}(-1)^{i+j}\frac{\lambda_{rb}\lambda_{ar}}{(j+1)\lambda_{re}\lambda_{ar}+i\lambda_{ae}\lambda_{rb}}\right),\quad s_l\in\Omega^{-},\\ 1-\sum\limits_{k_1=M_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=M_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2},\quad s_n=s_l,\end{cases}\tag{18}$$

where $C_A^B=\frac{B!}{A!(A-B)!}$.

Proof. According to the proposed link selection policy, the system state transfers from s_n to s_l with probability as

$$a_{n,l}=\begin{cases}\frac{1}{M_2}\left(1-P_{\text{null}}\right)P_{\text{first}}(M_1)P_{\text{second}}(M_2)P_{rb}, & s_l\in\Omega^{+},\\ \frac{1}{M_1}\left(1-P_{\text{null}}\right)P_{\text{first}}(M_1)P_{\text{second}}(M_2)P_{sr}, & s_l\in\Omega^{-},\\ 1-P_{\text{first}}(M_1)P_{\text{second}}(M_2), & s_n=s_{n+1},\end{cases}\tag{19}$$

where P_{ar} is the probability that the link from Alice to a relay is selected for the privacy information transmission when there are M_1 and M_2 available links for the first and second hops, respectively; P_{rb} is the probability that the link from a relay to Bob is selected for forwarding the privacy information when there are M_1 and M_2 available links for the first and second hops, respectively; $P_{ar}+P_{rb}=1$. In the following, we will present the derivation of P_{ar}.

Assume that R_k is selected for the privacy information receiving at state s_n. Since all channels experience flat Rayleigh fading, the channel power gain g_{ar_k} follows an exponential distribution with the probability density function (PDF) as $f_{g_{ar_k}}(x)=\frac{1}{\lambda_{ar}}\exp(-\frac{x}{\lambda_{ar}})$. According to the secure requirement in (13), this link can be selected for the privacy information transmission only if $g_{ar_k}\geqslant\Upsilon_{ar}$. Therefore, the PDF of $f_{g_{ak}}(x)$ under the condition $g_{ar_k}\geqslant\Upsilon_{ar}$, denoted by $f_{g_{ak}}(x|x\geqslant\Upsilon_{ar})$, can be derived as

$$f_{g_{ar_k}}(x|x\geqslant\Upsilon_{ar})=\begin{cases}\frac{-\frac{1}{\lambda_{ar}}\exp(-\frac{x}{\lambda_{ar}})}{\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}})}, & x\geqslant\Upsilon_{ar},\\ 0, & x<\Upsilon_{ar}.\end{cases}\tag{20}$$

At the state s_n, the link Alice $\rightarrow R_k$ is selected for the privacy information receiving with probability as

$$P_{ar} = \Pr\left\{ \frac{\max\limits_{R_k:\Psi(Q_k)\neq L, g_{ak}\geqslant \Upsilon_{ar}} g_{ak}}{\lambda_{ae}} \geqslant \frac{\max\limits_{R_k:\Psi(Q_k)\neq 0, g_{kb}\geqslant \Upsilon_{rb}} g_{kb}}{\lambda_{ke}} \right\}. \tag{21}$$

Let

$$\begin{cases} X \triangleq \dfrac{\max\limits_{R_k:\Psi(Q_k)\neq L, g_{ak}\geqslant \Upsilon_{ar}} g_{ak}}{\lambda_{ae}}, \\ Y \triangleq \dfrac{\max\limits_{R_k:\Psi(Q_k)\neq 0, g_{kb}\geqslant \Upsilon_{rb}} g_{kb}}{\lambda_{ke}}, \end{cases} \tag{22}$$

then, the cumulative distribution functions of X and Y are derived as

$$\begin{cases} F_X(x) = \left(\dfrac{1-\exp(-\frac{\lambda_{ae}x}{\lambda_{ar}})}{\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}})} \right)^{M_1}, \\ F_Y(y) = \left(\dfrac{1-\exp(-\frac{\lambda_{re}y}{\lambda_{rb}})}{\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}})} \right)^{M_2}. \end{cases} \tag{23}$$

Substituting (23) into (21), we can derive P_{ar} as

$$\begin{aligned} P_{ar} &= \Pr\{X \geqslant Y\} \\ &= \int_0^\infty \left(1 - \left(\frac{1-\exp(-\frac{\lambda_{ae}y}{\lambda_{ar}})}{\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}})} \right)^{M_1}\right) \mathrm{d}\left(\frac{1-\exp(-\frac{\lambda_{re}y}{\lambda_{rb}})}{\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}})} \right)^{M_2} \\ &= 1 - \int_0^\infty \left(\frac{1-\exp(-\frac{\lambda_{ae}y}{\lambda_{ar}})}{\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}})} \right)^{M_1} \frac{\lambda_{re}M_2}{\lambda_{rb}} \exp\left(-\frac{\lambda_{re}y}{\lambda_{rb}}\right) \left(\frac{1-\exp(-\frac{\lambda_{re}y}{\lambda_{rb}})}{\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}})} \right)^{M_2-1} \mathrm{d}y \\ &= 1 - \frac{\lambda_{re}M_2}{\lambda_{rb}\exp\left(-\frac{M_1\Upsilon_{ar}}{\lambda_{ar}} - \frac{(M_2-1)\Upsilon_{rb}}{\lambda_{rb}}\right)} \\ &\quad \times \underbrace{\int_0^\infty \left(1-\exp\left(-\frac{\lambda_{ae}y}{\lambda_{ar}}\right)\right)^{M_1} \exp\left(-\frac{\lambda_{re}y}{\lambda_{rb}}\right) \left(1-\exp\left(-\frac{\lambda_{re}y}{\lambda_{rb}}\right)\right)^{M_2-1} \mathrm{d}y}_{I_1}, \end{aligned} \tag{24}$$

where I_1 is given by

$$\begin{aligned} I_1 &= \left(-\exp\left(-\frac{\lambda_{ae}y}{\lambda_{ar}}\right)\right)^i \exp\left(-\frac{\lambda_{re}y}{\lambda_{rb}}\right) \sum_{i=0}^{M_2-1} C_{M_2-1}^i \left(-\exp\left(-\frac{\lambda_{re}y}{\lambda_{rb}}\right)\right)^j \mathrm{d}y \\ &= \sum_{i=0}^{M_1}\sum_{i=0}^{M_2-1} C_{M_1}^i C_{M_2-1}^i \frac{(-1)^{i+j}\lambda_{rb}\lambda_{ar}}{(j+1)\lambda_{re}\lambda_{ar} + i\lambda_{ae}\lambda_{rb}}. \end{aligned} \tag{25}$$

Therefore, by substituting (15), (16), and (24) into (19), we can derive the transition probability $a_{n,l}$. Then, we have proved the derivation of (37).

Since each queue has $L+1$ states, the dimension of the transition matrix is $(L+1)^M \times (L+1)^M$ and we denote this transition matrix by $\boldsymbol{A}$. According to [32], the stationary states are derived as

$$\boldsymbol{\pi} = (\boldsymbol{A} - \boldsymbol{I} + \boldsymbol{B})^{-1}\boldsymbol{b}, \tag{26}$$

where $\boldsymbol{\pi}$ is $(L+1)^M \times 1$; $\boldsymbol{b} = [1, 1, \ldots, 1]^{\mathrm{T}}$; $\boldsymbol{I}$ is the identity matrix; $\boldsymbol{B}$ is an all-ones matrix.

4 Performance analysis

Based on the above analysis, we will analyze the secrecy outage probability and average secrecy rate. In addition, the information delay is studied.

4.1 Secrecy outage probability

Adopting the wiretap coding, the privacy information will experience a secrecy outage when the secrecy rate is less than R_s. Therefore, for the proposed link selection policy, the secrecy outage probability is derived as

$$P_{\text{out,sec}} = \sum_{n=1}^{(L+1)^M} \boldsymbol{\pi} P_{\text{out},s_n}, \tag{27}$$

where P_{out,s_n} is the secrecy outage probability at state s_n[3)].

To analyze the secrecy outage probability at each state, we assume that R_i is selected to receive the privacy information with the secrecy rate $R_{ai,\text{sec}}[t]$ for state s_n in the tth time slot. When $R_{ai,\text{sec}}[t] < R_s$, the privacy information will experience secrecy outage with probability

$$\begin{aligned} P_{\text{out},ai}[t] &= \Pr\left\{R_{ai,\text{sec}}[t] < R_s\right\} \\ &= \Pr\left\{\left(\log_2\left(1+\frac{P_a g_{ar_i}[t]}{N_0}\right) - \log_2\left(1+\frac{P_a g_{ae}[t]}{N_0}\right)\right) < R_s\right\}. \end{aligned} \tag{28}$$

Assuming the high signal-to-noise ratio regime, $P_{\text{out},ai}[t]$ can be approximated as

$$\begin{aligned} P_{\text{out},ai}[t] &\approx \Pr\left\{\log_2\left(\frac{g_{ar_i}[t]}{g_{ae}[t]}\right) < R_s\right\} \\ &= \int_0^{\infty} \left(\frac{1-\exp(-\frac{2^{R_s}x}{\lambda_{ar}})}{\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}})}\right)^{M_1} \frac{1}{\lambda_{re}} \exp\left(-\frac{x}{\lambda_{ae}}\right) \mathrm{d}x \\ &= \exp\left(-\frac{M_1\Upsilon_{ar}}{\lambda_{ar}}\right) \sum_{i=1}^{M_1} C_{M_1}^i (-1)^i \frac{\lambda_{ar}}{2^{R_s} i\lambda_{ae} + \lambda_{ar}}. \end{aligned} \tag{29}$$

Similarly, when R_i is selected to forward the privacy information for state s_n in the tth time slot, the privacy information will experience secrecy outage with probability as

$$\begin{aligned} P_{\text{out},ib}[t] &= \Pr\left\{R_{ib,\text{sec}}[t] < R_s\right\} \\ &= \Pr\left\{\left(\log_2\left(1+\frac{P_r g_{r_i b}[t]}{N_0}\right) - \log_2\left(1+\frac{P_r g_{r_i e}[t]}{N_0}\right)\right) < R_s\right\} \\ &\approx \Pr\left\{\log_2\left(\frac{g_{r_i b}[t]}{g_{r_i e}[t]}\right) < R_s\right\} \\ &= \int_0^{\infty} \left(\frac{1-\exp(-\frac{2^{R_s}x}{\lambda_{rb}})}{\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}})}\right)^{M_1} \frac{1}{\lambda_{re}} \exp\left(-\frac{x}{\lambda_{re}}\right) \mathrm{d}x \\ &= \exp\left(-\frac{M_2\Upsilon_{rb}}{\lambda_{rb}}\right) \sum_{i=1}^{M_2} C_{M_2}^i (-1)^i \frac{\lambda_{rb}}{2^{R_s} i\lambda_{re} + \lambda_{rb}}. \end{aligned} \tag{30}$$

When the first hop is selected, the transmission experiences secure outage with probability $P_{\text{first}}(M_1)P_{\text{out},ai}[t]$. When the second hop is selected, the transmission experiences secure outage with probability $P_{\text{second}}(M_2)P_{\text{out},ib}[t]$. For the proposed scheme, when the first hop or the second hop experiences a secrecy outage, the system will experience a secrecy outage. Therefore, the secrecy outage probability at s_n is derived as

$$P_{\text{out},s_n} = 1 - \left(1 - P_{\text{first}}(M_1)P_{\text{out},ai}[t]\right)\left(1 - P_{\text{second}}(M_2)P_{\text{out},ib}[t]\right)$$

3) When the buffer is not ready to receive information and the transmitter is still transmitting, the system will experience secrecy outage.

$$
\begin{aligned}
&= 1 - \left(1 - \sum_{k=M_1}^{M} \left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^k \left(1 - \exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k} \right. \\
&\quad \times \left. \left(1 - \exp\left(-\frac{M_1\Upsilon_{ar}}{\lambda_{ar}}\right) \sum_{i=1}^{M_1} C_{M_1}^i (-1)^i \frac{\lambda_{ar}}{2^{R_s} i\lambda_{ae} + \lambda_{ar}}\right)\right) \\
&\quad \times \left(1 - \sum_{k=M_2}^{M} \left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^k \left(1 - \exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k} \right. \\
&\quad \times \left. \left(1 - \exp\left(-\frac{M_2\Upsilon_{rb}}{\lambda_{rb}}\right) \sum_{i=1}^{M_2} C_{M_2}^i (-1)^i \frac{\lambda_{rb}}{2^{R_s} i\lambda_{re} + \lambda_{rb}}\right)\right). \qquad (31)
\end{aligned}
$$

By substituting (31) into (27), we can derive the average secrecy outage probability for the proposed link selection policy.

Remark 1. For the proposed policy, a link is selected when it satisfies $g_{ar_i} < \Upsilon_{ar}$ or $g_{r_ib} < \Upsilon_{rb}$. In other words, a link is selected under the maximum permitted secrecy outage probability $P_{\text{out}}^{\text{upper}}$. Therefore, the maximum secrecy outage probability of the proposed link selection policy is $P_{\text{out}}^{\text{upper}}$ which is the upper bound of $P_{\text{out,sec}}$.

4.2 Average secrecy rate

According to the proposed policy, when the information is securely forwarded, the information is successfully transmitted. Therefore, the average secrecy rate of the network is equivalent to the secrecy rate of the second hop. In addition, since the wiretap CSI is unavailable, we utilize the ergodic wiretap rate to evaluate the secrecy rate. According to the system transition matrix, the average secrecy rate of the system is derived as

$$
\begin{aligned}
R_{\text{sec,ave}} &= \sum_{n=1}^{(L+1)^M} a_{n.l}^{+}(s_n)\boldsymbol{\pi}(s_n) \left(\sum_{i=1}^{M} \phi_i(s_n) \left(R_{r_ib}(s_n) - (R_{r_ie}(s_n))\right)\right) \\
&= \sum_{n=1}^{(L+1)^M} a_{n.l}^{+}(s_n)\boldsymbol{\pi}(s_n) \left\{\sum_{i=1}^{M} \phi_i(s_n) \left(R_{r_ib}(s_n) - \underbrace{\frac{1}{\ln 2} \exp\left(-\frac{1}{\lambda_{re}}\right) E_i\left(-\frac{1}{\lambda_{re}}\right)}_{I_2}\right)\right\},
\end{aligned}
$$

where $E_i(\cdot)$ is defined in [41, eq. (8.211.1)]; I_2 is the ergodic rate of the wiretap channel; $\boldsymbol{\pi}(s_n)$ is the stationary probability of state s_n; $a_{n,l}^{+}(s_n)$ denotes the transition probability from the state s_n to the state s_l, when a relay is selected to forward the privacy information; $\phi_i(s_n)$ denotes the relay selection option, such as $\phi_i(s_n) = 1$ denotes that the relay R_i is selected for forwarding the secure information and $\phi_i(s_n) = 0$ denotes that the relay R_i is not selected for forwarding the secure information.

4.3 Information delay

In the proposed scheme, the information delay is the time consumed for the information waiting in the queues. In the proposed system, the information delay consists of three components: the information delay at Alice T_a, the information delay at the head of the relays T_r, and the information delay at the relays' queues T_a. In the following, we will separately analyze the information delay from the above three components.

4.3.1 *Information delay at Alice T_a*

In the proposed system, the service rate at Alice is the information rate that the relays successfully receive the privacy information from Alice. According to the stationary states in Subsection 3.2 and the

proposed link selection policy, Alice's average service rate is the information rate at all relays for all the states as

$$R_{r,\text{ave}} = \sum_{n=1}^{(L+1)^M} a_{n.l}^{-}(s_n)\boldsymbol{\pi}(s_n)\left(\sum_{i=1}^{M}\tilde{\phi}_i(s_n)R_{ar_i}(s_n)\right), \tag{32}$$

where $a_{n,l}^{-}(s_n)$ denotes the transition probability of transferring from state s_n to state s_l when a relay is selected to receive the privacy information; $\tilde{\phi}_i(s_n)$ denotes the relay selection policy. We have $\tilde{\phi}_i(s_n) = 1$ when the relay R_i is selected for receiving the secure information and $\tilde{\phi}_i(s_n) = 0$ when the relay R_i is not selected for receiving the secure information.

Therefore, the average information delay at Alice can be derived as

$$T_a = \frac{1}{\sum_{n=1}^{(L+1)^M} a_{n.l}^{-}(s_n)\boldsymbol{\pi}(s_n)(\sum_{i=1}^{M}\tilde{\phi}_i(s_n)R_{ar_i}(s_n))}. \tag{33}$$

4.3.2 *Information delay at the relays' head*

When the privacy information at the head of R_k, the packet will wait for scheduling to forward the privacy information. In this scenario, there will be $L(L+1)^{(M-1)}$ states. To describe this scenario, we first analyze the stationary states for this scenario. Define the state space as

$$\tilde{s}_n = [\vartheta_{\tilde{s}_n}(Q_1), \vartheta_{\tilde{s}_n}(Q_2), \ldots, \vartheta_{\tilde{s}_n}(Q_k), \ldots, \vartheta_{\tilde{s}_n}(Q_N)], \tag{34}$$

where $\vartheta_{\tilde{s}_n}(Q_k)$ denotes relay R_k's queue at state $\tilde{s}_n$. At state $\tilde{s}_n$, there are $\tilde{M}_1$ available links from Alice to the relays and there are $\tilde{M}_2$ available links from the relays to Bob. The probabilities of $\tilde{M}_1$ and $\tilde{M}_2$ are, respectively, given by

$$\tilde{P}_{\text{first}}(\tilde{M}_1) = \sum_{k=\tilde{M}_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^k\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k} \tag{35}$$

and

$$\tilde{P}_{\text{second}}(\tilde{M}_1) = \sum_{k=\tilde{M}_1}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^k\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k}. \tag{36}$$

In the tth time slot, the system state is $\tilde{s}_n$. In the $(t+1)$th time slot, a relay is selected to receive or forward the secrecy information, and the system state will transfer to state $\tilde{s}_l$. When a link from Alice to a relay is selected for privacy information transmission, the buffer of the corresponding relay will increase and we denote this event by $\tilde{\Omega}_l^{+}$. Otherwise, when a link from a relay to Bob is selected at the $(t+1)$th time slot for the privacy information forwarding, the buffer of the corresponding relay will decrease and we denote this event by $\tilde{\Omega}_l^{-}$. Since all the links from Alice to the relays and from the relays to Bob are independent identically distributed, the system will equally select the links from Alice to a relay and from

a relay to Bob. Therefore, the probability that the system state transfers from $\tilde{s}_n$ to $\tilde{s}_l$ is derived as

$$\tilde{a}_{n,l}=\begin{cases}\sum\limits_{k_1=\tilde{M}_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=\tilde{M}_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2}\\ \quad\times\frac{\left(1-(1-\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}}))^{M}(1-\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}}))^{M}\right)}{\tilde{M}_2}\left(\frac{\lambda_{re}\tilde{M}_2}{\lambda_{rb}\exp\left(-\frac{\tilde{M}_1\Upsilon_{ar}}{\lambda_{ar}}-\frac{(\tilde{M}_2-1)\Upsilon_{rb}}{\lambda_{rb}}\right)}\right.\\ \quad\left.\times\sum\limits_{i=0}^{M_1}\sum\limits_{i=0}^{\tilde{M}_2-1}C_{\tilde{M}_1}^{i}C_{\tilde{M}_2-1}^{i}(-1)^{i+j}\frac{\lambda_{rb}\lambda_{ar}}{(j+1)\lambda_{re}\lambda_{ar}+i\lambda_{ae}\lambda_{rb}}\right),\quad s_l\in\tilde{\Omega}^{+},\\ \sum\limits_{k_1=\tilde{m}_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=\tilde{m}_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2}\\ \quad\times\frac{\left(1-(1-\exp(-\frac{\Upsilon_{ar}}{\lambda_{ar}}))^{M}(1-\exp(-\frac{\Upsilon_{rb}}{\lambda_{rb}}))^{M}\right)}{\tilde{M}_1}\left(1-\frac{\lambda_{re}\tilde{M}_2}{\lambda_{rb}\exp\left(-\frac{\tilde{M}_1\Upsilon_{ar}}{\lambda_{ar}}-\frac{(M_2-1)\Upsilon_{rb}}{\lambda_{rb}}\right)}\right.\\ \quad\left.\times\sum\limits_{i=0}^{\tilde{M}_1}\sum\limits_{i=0}^{\tilde{M}_2-1}C_{\tilde{M}_1}^{i}C_{\tilde{M}_2-1}^{i}(-1)^{i+j}\frac{\lambda_{rb}\lambda_{ar}}{(j+1)\lambda_{re}\lambda_{ar}+i\lambda_{ae}\lambda_{rb}}\right),\quad s_l\in\tilde{\Omega}^{-},\\ 1-\sum\limits_{k_1=\tilde{m}_1}^{M}\left(\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{k_1}\left(1-\exp\left(-\frac{\Upsilon_{ar}}{\lambda_{ar}}\right)\right)^{M-k_1}\\ \quad\times\sum\limits_{k_2=\tilde{M}_2}^{M}\left(\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{k_2}\left(1-\exp\left(-\frac{\Upsilon_{rb}}{\lambda_{rb}}\right)\right)^{M-k_2},\quad s_n=s_l.\end{cases}\tag{37}$$

Since there are $L(L+1)^{(M-1)}$ states in the state space, the transition matrix, denoted by $\tilde{\boldsymbol{A}}$, has dimension $L(L+1)^{(M-1)}\times L(L+1)^{(M-1)}$. The stationary state probability vector is derived as [32]

$$\tilde{\boldsymbol{\pi}}=(\tilde{\boldsymbol{A}}-\boldsymbol{I}+\boldsymbol{B})^{-1}\boldsymbol{b},\tag{38}$$

where $\tilde{\boldsymbol{\pi}}$ is $L(L+1)^{(M-1)}\times 1$.

Therefore, the relay forwarding rate can be derived as

$$R_{b,\text{ave}}=\sum_{n=1}^{L(L+1)^{M-1}}\tilde{a}_{n.l}^{+}(\tilde{s}_n)\tilde{\boldsymbol{\pi}}(\tilde{s}_n)\left(\sum_{i=1}^{M}\phi(\tilde{s}_n)R_{r_ib}(\tilde{s}_n)\right),\tag{39}$$

where $\tilde{\boldsymbol{\pi}}(\tilde{s}_n)$ is the stationary probability of state $\tilde{s}_n$; $\tilde{a}_{n.l}^{+}(\tilde{s}_n)$ denotes the transition probability to transfer from state $\tilde{s}_n$ to state $\tilde{s}_l$ when a relay is selected to forward the privacy information; $\phi_i(\tilde{s}_n)$ denotes the relay selection policy, such as $\phi_i(\tilde{s}_n)=1$ when the relay R_i is selected to forward the secure information and $\phi_i(\tilde{s}_n)=0$ when the relay R_i is not selected to forward the secure information.

Then, the information delay at the head of the relays is derived as

$$T_r=\frac{1}{\sum_{n=1}^{L(L+1)^{M-1}}\tilde{a}_{n.l}^{+}(\tilde{s}_n)\tilde{\boldsymbol{\pi}}(\tilde{s}_n)(\sum_{i=1}^{M}\phi_i(\tilde{s}_n)R_{r_ib}(\tilde{s}_n))}.\tag{40}$$

4.3.3 *Information delay for the queuing*

According to the Little's law, the average queuing delay is $T_q=\frac{\sum_{i=1}^{M}\vartheta(Q_i)}{R_{r,\text{ave}}}$, where the numerator is the average queue length and the denominator is the average service rate of Alice, which is equal to the

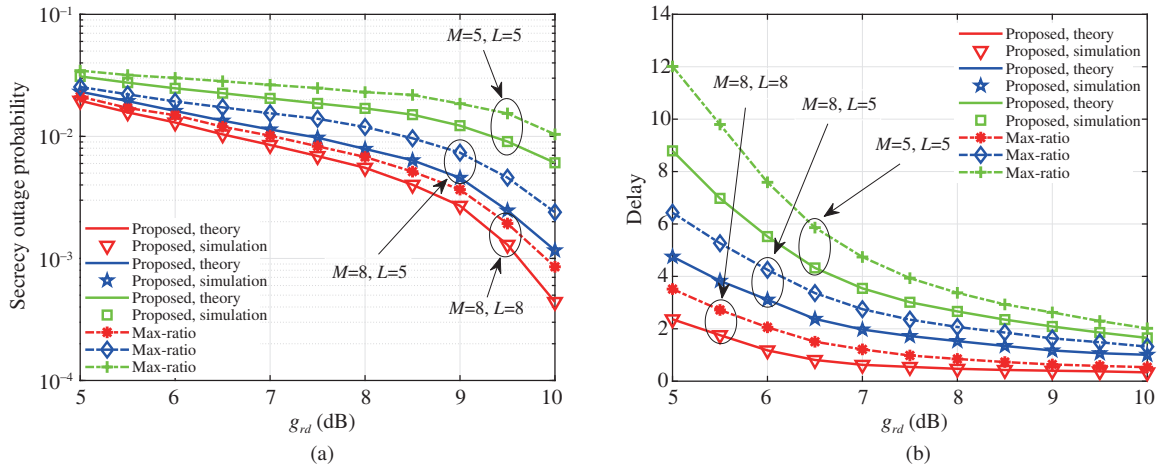

Figure 2 (Color online) The secrecy outage probability (a) and the information delay (b) versus the average channel power gain g_{rd} with $g_{sr} \geqslant g_{rd}$.

average arrive rate at relay. Based on the stationary states, the average queue length is derived as

$$\sum_{i=1}^{M} \vartheta(Q_i) = \sum_{i=1}^{(L+1)^M} \sum_{j=1}^{M} \pi_{s_i} \vartheta_{s_i}(Q_j). \tag{41}$$

Substituting (41) into $T_q = \frac{\sum_{i=1}^{M} \vartheta(Q_i)}{R_{r,\text{ave}}}$, we obtain the information delay of the all queues. For each queue, its average queuing delay is

$$T_q = \frac{\sum_{i=1}^{(L+1)^M} \sum_{j=1}^{M} \pi_{s_i} \vartheta_{s_i}(Q_j)}{\sum_{n=1}^{(L+1)^M} a_{n.l}^{-}(s_n) \boldsymbol{\pi}(s_n) (\sum_{i=1}^{M} \tilde{\phi}_i(s_n) R_{ar_i}(s_n))}. \tag{42}$$

According to the above discussion, the closed-form expression of the information delay is obtained as

$$T_{\text{delay}} = T_a + T_r + T_q. \tag{43}$$

5 Simulation results

In this section, we will evaluate the performance of the proposed scheme. In the simulation, the relays are located between Alice and Bob to assist the secure transmission. Each relay is equipped with a buffer. Alice and the relays adopt the wiretap coding and the target transmission rate R_b is set to 1.5 bit/s/Hz. In addition, we also simulate the traditional max-ratio scheme where the maximum signal-to-interference-plus-noise link is selected for transmission. In the following, we will simulate the secrecy outage probability, information delay, and the average secure rate versus the channel power gain g_{rd}, the target secrecy rate R_s and the secure outage probability upper bound.

In Figure 2(a), we plot the secrecy outage probability versus the average channel power gain between the relays and Bob. In this figure, we can observe that the theoretical results are in excellent agreement with the simulation results. In addition, the secrecy outage probability is a decreasing function of g_{rd}. A large value of g_{rd} indicates that Alice and the relays have much more power to guarantee the secure transmission in both the first and second hop. Therefore, the secrecy outage probability decreases with g_{rd}. More relays will increase the selection diversity and the secrecy outage probability will decrease. In the traditional max-ratio scheme, the link security is not considered and the secrecy outage probability increases.

In Figure 2(b), we plot the information delay versus the average channel power gain between the relays and Bob. In this figure, we can also observe that the theoretical results are in excellent agreement with the simulation results. In addition, the information delay is a decreasing function of g_{rd}. A large value of g_{rd} indicates that the source and the relays have more power to protect the privacy information in both the first and second hops. Therefore, the privacy information can secure transmission with high

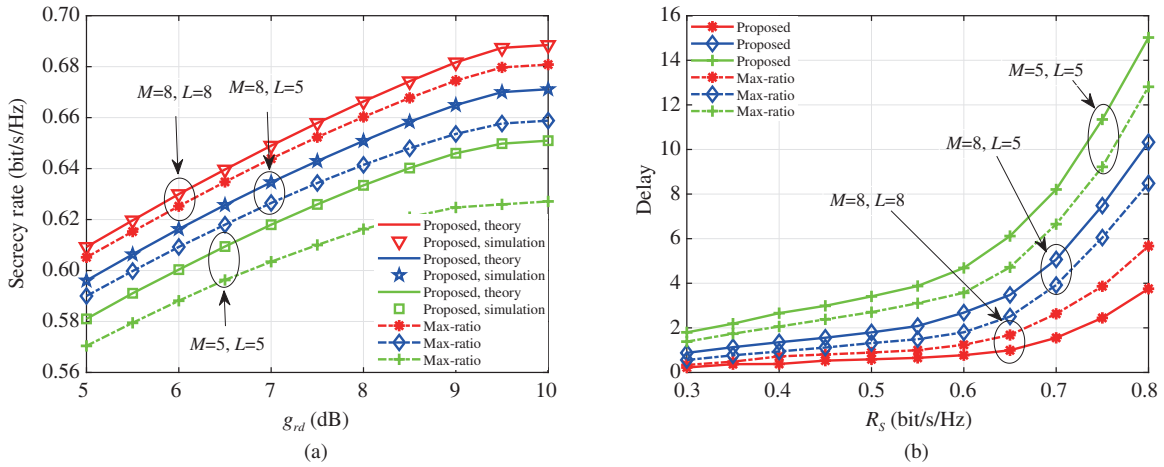

Figure 3 (Color online) (a) The average secrecy rate versus the average channel power gain g_{rd} with $g_{sr} \geqslant g_{rd}$; (b) the information delay versus the target secrecy rate R_s.

secrecy rate and the information delay will decrease with g_{rd}. When the buffer can store more packets, the network can select the link with high rate. Therefore, the information delay will decrease with g_{rd}. For the traditional max-ratio scheme, the security of each hop is not considered, which will increase the information delay.

In Figure 3(a), we plot the average secrecy rate versus the average channel power gain between the relays and Bob. In this figure, we can also observe that the theoretical results are in excellent agreement with the simulation results. In addition, the average secrecy rate is an increasing function of g_{rd}. A large value of g_{rd} indicates that Alice and relays have much more power to securely transmit the privacy information. Therefore, the privacy information can secure transmission with high secrecy rate. The increase in buffer size and the number of the relays will provide increased link selection diversity and improve the average secrecy rate. When g_{rd} is large, the information rate will limit the increase in the average secrecy rate. For the traditional max-ratio scheme, the security of each hop is not considered and the information delay will increase.

In Figure 3(b), we plot the information delay versus the target secrecy rate R_s. In this figure, the information delay is an increasing function of g_{rd}. A large value of R_s indicates that it is challenging to securely transmit the privacy information and the available links will decrease. Therefore, the information delay will increase with R_s. The increase in buffer size and the number of the relays will increase the link selection diversity and decrease the information delay decrease. For the traditional max-ratio scheme, the system always selects a link from the links of the Alice-to-relay or the links of the relay-to-destination, while the transmission outage event is ignored. Therefore, when the transmission outage occurs, Alice will retransmit the privacy information and thus increase the information delay. Moreover, if the privacy information experiences a secrecy outage, the privacy information will be useless and Alice will transmit the alternative information, and thus also increase the information delay.

In Figure 4(a), we plot the secrecy outage probability versus the upper-bound secrecy outage probability $P_{\text{out}}^{\text{upper}}$. In this figure, the secrecy outage probability is a decreasing function of $P_{\text{out}}^{\text{upper}}$. A large value of $P_{\text{out}}^{\text{upper}}$ indicates that the secrecy outage probability constraint is loose and there will be more available secure transmission links. Therefore, the secrecy outage probability will decrease with the upper-bound secrecy outage probability $P_{\text{out}}^{\text{upper}}$. The increase in buffer size and the number of the relays will increase the link selection diversity and decrease the secrecy outage probability.

In Figure 4(b), we plot the information delay versus the upper-bound secrecy outage probability $P_{\text{out}}^{\text{upper}}$. In this figure, the information delay is a decreasing function of $P_{\text{out}}^{\text{upper}}$. A large value of $P_{\text{out}}^{\text{upper}}$ indicates that the secrecy outage probability constraint is loose and there will be more available secure transmission links for the secrecy transmission. Therefore, the information delay will decrease with $P_{\text{out}}^{\text{upper}}$. The increase in buffer size and the number of the relays will increase the diversity of the link selection diversity and decrease the information delay.

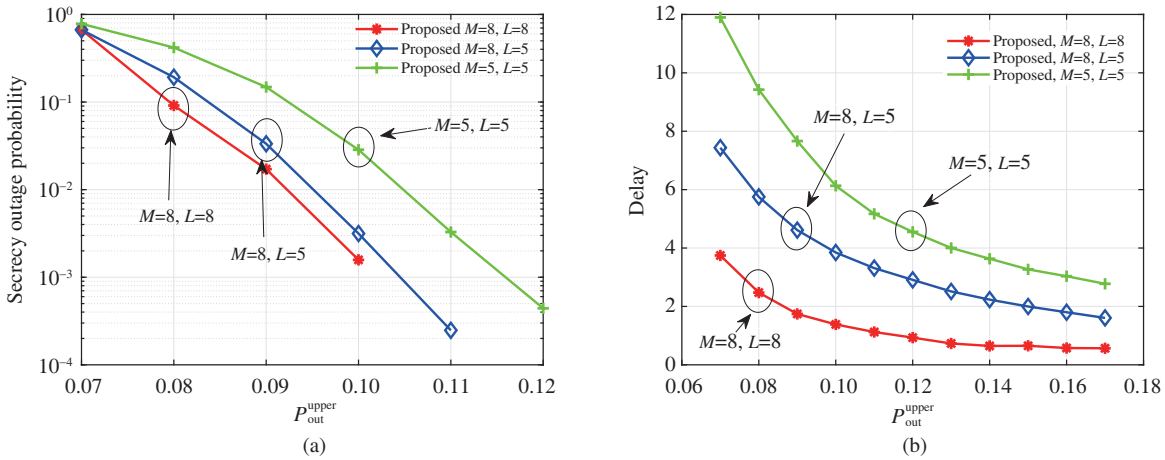

Figure 4 (Color online) The secrecy outage probability (a) and the information delay (b) versus the upper-bound secrecy outage probability $P_{\text{out}}^{\text{upper}}$.

6 Conclusion

We proposed an outage-driven secure transmission scheme for buffer-aided two-hop networks to protect the information secrecy. In the proposed scheme, an outage-driven link selection policy was designed and the system stationary states were derived. Based on the stationary states, we analyzed the secrecy outage probability, the average secrecy rate, and the information delay. Numerical results validated the performance analysis and demonstrated the performance superiority of the proposed scheme in terms of secrecy outage probability and information delay.

In addition to those problems listed above, there are still some open problems remained to be further investigated. In future work, we plan to study the buffer-aided multi-hop cooperative networks, that can fully explore the benefit brought by relay assistance. In addition, the information security problems for the above networks are an interesting aspect that deserves a detailed study.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61901379, 61941119, 62071223, 62031012), in part by National Key Research and Development Project (Grant No. 2020YFB1807-602), in part by Young Elite Scientist Sponsorship Program by CAST, in part by Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (Grant No. 2020D04), and in part by Foundation of the Science, Technology, and Innovation Commission of Shenzhen Municipality (Grant No. JCYJ20190806160218174).

References

1 Wang G, Lin Y, Meng C, et al. Secrecy energy efficiency optimization for AN-aided SWIPT system with power splitting receiver. Sci China Inf Sci, 2019, 62: 029301
2 Wang L, Wong K K, Jin S, et al. A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks. IEEE Commun Mag, 2018, 56: 49–55
3 Xu C, Zeng P, Liang W, et al. Secure resource allocation for green and cognitive device-to-device communication. Sci China Inf Sci, 2018, 61: 029305
4 Qi X H, Huang K Z, Li B, et al. Physical layer security in multi-antenna cognitive heterogeneous cellular networks: a unified secrecy performance analysis. Sci China Inf Sci, 2018, 61: 022310
5 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
6 Csiszar I, Korner J. Broadcast channels with confidential messages. IEEE Trans Inform Theory, 1978, 24: 339–348
7 Leung-Yan-Cheong S, Hellman M. The Gaussian wire-tap channel. IEEE Trans Inform Theory, 1978, 24: 451–456
8 Rodriguez L J, Tran N H, Duong T Q, et al. Physical layer security in wireless cooperative relay networks: state of the art and beyond. IEEE Commun Mag, 2015, 53: 32–39
9 Arafa A, Shin W, Vaezi M, et al. Secure relaying in non-orthogonal multiple access: trusted and untrusted scenarios. IEEE Trans Inform Forensic Secur, 2020, 15: 210–222
10 Lim J T, Lee K, Han Y. Secure communication with outdated channel state information via untrusted relay capable of energy harvesting. IEEE Trans Veh Technol, 2020, 69: 11323–11337
11 Abdullah Z, Chen G, Abdullah M A M, et al. Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming. IEEE Trans Inform Forensic Secur, 2021, 16: 161–172
12 Lin J, Li Q, Yang J, et al. Physical-layer security for proximal legitimate user and eavesdropper: a frequency diverse array beamforming approach. IEEE Trans Inform Forensic Secur, 2018, 13: 671–684
13 Deng Z, Li Q, Zhang Q, et al. Beamforming design for physical layer security in a two-way cognitive radio IoT network with SWIPT. IEEE Int Things J, 2019, 6: 10786–10798
14 Zhao R, Lin H, He Y C, et al. Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI. IEEE Trans Commun, 2018, 66: 546–559
15 Fan L, Lei X, Yang N, et al. Secrecy cooperative networks with outdated relay selection over correlated fading channels. IEEE Trans Veh Technol, 2017, 66: 7599–7603

16 Zhu F C, Gao F F, Zhang T, et al. Physical-layer security for full duplex communications with self-interference mitigation. IEEE Trans Wirel Commun, 2016, 15: 329–340
17 Zheng T X, Wang H M, Yuan J, et al. Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. IEEE Trans Wirel Commun, 2017, 16: 3827–3839
18 Ni W, Zhang J A, Fang Z, et al. Analysis of finite buffer in two-way relay: a queueing theoretic point of view. IEEE Trans Veh Technol, 2018, 67: 3690–3694
19 Manoj B R, Mallik R K, Bhatnagar M R. Performance analysis of buffer-aided priority-based max-link relay selection in DF cooperative networks. IEEE Trans Commun, 2018, 66: 2826–2839
20 Razlighi M M, Zlatanov N. Buffer-aided relaying for the two-hop full-duplex relay channel with self-interference. IEEE Trans Wirel Commun, 2018, 17: 477–491
21 Morsi R, Michalopoulos D S, Schober R. Performance analysis of near-optimal energy buffer aided wireless powered communication. IEEE Trans Wirel Commun, 2018, 17: 863–881
22 Tian Z, Gong Y, Chen G J, et al. Buffer-aided relay selection with reduced packet delay in cooperative networks. IEEE Trans Veh Technol, 2017, 66: 2567–2575
23 Lan X L, Ren J J, Chen Q C, et al. Achievable secrecy rate region for buffer-aided multiuser MISO systems. IEEE Trans Inform Forensic Secur, 2020, 15: 3311–3324
24 Ren J J, Lei X F, Diamantoulakis P D, et al. Buffer-aided secure relay networks with SWIPT. IEEE Trans Veh Technol, 2020, 69: 6485–6499
25 Wan J, Qiao D, Wang H M, et al. Buffer-aided two-hop secure communications with power control and link selection. IEEE Trans Wirel Commun, 2018, 17: 7635–7647
26 Wang D W, Ren P Y, Cheng J L. Cooperative secure communication in two-hop buffer-aided networks. IEEE Trans Commun, 2018, 66: 972–985
27 Zhang Q, Liang Z J, Li Q Z, et al. Buffer-aided non-orthogonal multiple access relaying systems in Rayleigh fading channels. IEEE Trans Commun, 2017, 65: 95–106
28 Chen G J, Tian Z, Gong Y, et al. Max-ratio relay selection in secure buffer-aided cooperative wireless networks. IEEE Trans Inform Forensic Secur, 2014, 9: 719–729
29 Nakai R, Sugiura S. Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming. IEEE Trans Inform Forensic Secur, 2019, 14: 431–444
30 Gong Y, Chen G J, Xie T. Using buffers in trust-aware relay selection networks with spatially random relays. IEEE Trans Wirel Commun, 2018, 17: 5818–5826
31 Tang X X, Cai Y M, Huang Y Z, et al. Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems. IEEE Trans Veh Technol, 2018, 67: 2035–2048
32 Liao X N, Zhang Y Y, Wu Z Q, et al. On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection. IEEE Trans Wirel Commun, 2018, 17: 1893–1906
33 Liao X N, Zhang Y Y, Wu Z Q, et al. Buffer-aided relay selection for secure two-hop wireless networks with decode-and-forward relays and a diversity-combining eavesdropper. Ad Hoc Netw, 2020, 98: 102039
34 Zhang H S, Zhang H J, Liu W, et al. Energy efficient user clustering, hybrid precoding and power optimization in terahertz MIMO-NOMA systems. IEEE J Sel Areas Commun, 2020, 38: 2074–2085
35 Zhang H J, Zhang J M, Long K P. Energy efficiency optimization for NOMA UAV network with imperfect CSI. IEEE J Sel Areas Commun, 2020, 38: 2798–2809
36 Ke M L, Gao Z, Wu Y P, et al. Massive access in cell-free massive MIMO-based Internet of Things: cloud computing and edge computing paradigms. IEEE J Sel Areas Commun, 2021, 39: 756–772
37 Liao A W, Gao Z, Wang D M, et al. Terahertz ultra-massive MIMO-based aeronautical communications in space-air-ground integrated networks. IEEE J Sel Commun, 2021. doi: 10.1109/JSAC.2021.3071834
38 Cao K R, Wang B H, Ding H Y, et al. On the security enhancement of uplink NOMA systems with jammer selection. IEEE Trans Commun, 2020, 68: 5747–5763
39 Yue X W, Liu Y W, Yao Y Y, et al. Secure communications in a unified non-orthogonal multiple access framework. IEEE Trans Wirel Commun, 2020, 19: 2163–2178
40 Jiang W Y, Huang K Z, Xiao S F, et al. Secure transmission for heterogeneous cellular network with limited feedback. Sci China Inf Sci, 2020, 63: 220304
41 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products. Orlando: Academic Press, 2014