Physical Layer Security in Buffer-State-Based Max-Ratio Relay Selection Exploiting Broadcasting With Cooperative Beamforming and Jamming

Ryota Nakai, *Student Member, IEEE*, and Shinya Sugiura, *Senior Member, IEEE*

***Abstract*— In this paper, we propose a novel secure buffer-aided decode-and-forward relay selection that amalgamates the benefits of the buffer-state-based relay selection, the max-ratio criterion, the simultaneous activation of multiple source-to-relay links, and the cooperative beamforming in dual-hop networks. More specifically, the proposed scheme is designed for selecting a single or multiple relay nodes for packet reception or transmission based on the buffer states of relay nodes, while avoiding the detrimental effects of both an empty buffer state and a buffer overflow. Analytical bounds on the secrecy outage probability and the average delay are derived for our proposed scheme, based on a Markov chain process, in order to verify the system model of our proposed scheme. Furthermore, we introduce the concept of cooperative jamming into the proposed scheme, in order to interfere with an eavesdropper's reception, while dispensing with the full channel state information associated with an eavesdropper at a central coordinator. Our simulation results demonstrate that the proposed schemes outperform the existing buffer-based secure relay selection schemes, in terms of both the secrecy outage probability and the average delay, as the explicit benefits of our novel introduced concepts.**

***Index Terms*— Broadcast, buffers, cooperative communications, delay-tolerant network, Markov chain, packet delay, physical layer security, secrecy capacity, secrecy outage probability, spatial diversity.**

I. Introduction

PHYSICAL layer security [1], [2] has attracted much interest in the field of wireless communications as a supplement to traditional key-based cryptographic wireless communications, owing to its unique benefit of allowing us to prevent unauthorized eavesdroppers from intercepting data transmitted from a source node to an intended destination node. While the original concept of physical layer security dates back to the invention of a wire-tap channel in 1975 [3], recent investigations in physical layer security have proved that signal processing at relay nodes in cooperative networks, such as relay selection, cooperative beamforming, and jamming, significantly enhances secrecy performance [4]–[8]. The performance of secure communications is typically assessed based on specific metrics, such as the secrecy rate and the secrecy outage probability. Additionally, the delay profile has to be low for practical network operation.

Recent buffer-aided cooperative communications strategies [9]–[27] allow us to exploit additional design degrees of freedom in comparison to the conventional cooperative communication strategies, which do not rely on buffers at relay nodes [28]–[31]. More specifically, using buffers at relay nodes enables flexible link selection, i.e., a flexible schedule of packet reception and transmission at relay nodes. The beneficial effects of the buffer-aided relaying scheme are achieved at the sacrifice of the additional overhead that is required for monitoring the statuses of all the channels and for selecting the best available communication link. Furthermore, buffer-aided relaying schemes typically suffer from an increase in end-to-end packet delay, since source packets are stored in a distributed manner over the relay nodes and then relayed to the destination node in an unscheduled link selection process.

Most recently, in [26], [32], and [33], further design degrees of freedom were added to buffer-aided relay selection with the aid of the concept of simultaneous exploitation of multiple source-to-relay (SR) links, which is enabled owing to the broadcast nature of wireless channels. As a result, the packet delay of the buffer-aided relaying scheme was significantly reduced. Furthermore, in [34], not only simultaneous activation of multiple SR links in a broadcast phase but also that of multiple relay-to-destination (RD) links in a relaying phase are invoked by relying on relay nodes' cooperative beamforming. Moreover, this multiple-link-activation scheme was introduced into full-duplex [33] and amplify-and-forward scenarios [32].

In [35], Chen *et al.* introduced buffer-aided relay selection in the context of physical layer security, where, based on the max-ratio criterion, a single relay is selected for packet reception or transmission in each time slot. Additionally, in [36], Huang and Swindlehurst investigated the tradeoff between the secrecy throughput and the secrecy outage probability in a buffer-aided relaying network while focusing their attention on a single-relay scenario. In [37], the secure buffer-aided relaying communication of [35] was extended to a hybrid half- and full-duplex scenario. Note that all the above-mentioned

Manuscript received January 23, 2018; revised May 31, 2018; accepted June 26, 2018. Date of publication July 10, 2018; date of current version August 2, 2018. This work was supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant 26709028, Grant 16KK0120, and Grant 17H03259, in part by the Telecommunications Advancement Foundation, and in part by the Nakajima Foundation. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Sheng Zhong. *(Corresponding author: Shinya Sugiura.)*

The authors are with the Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Tokyo 184-8588, Japan (e-mail: sugiura@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2854711

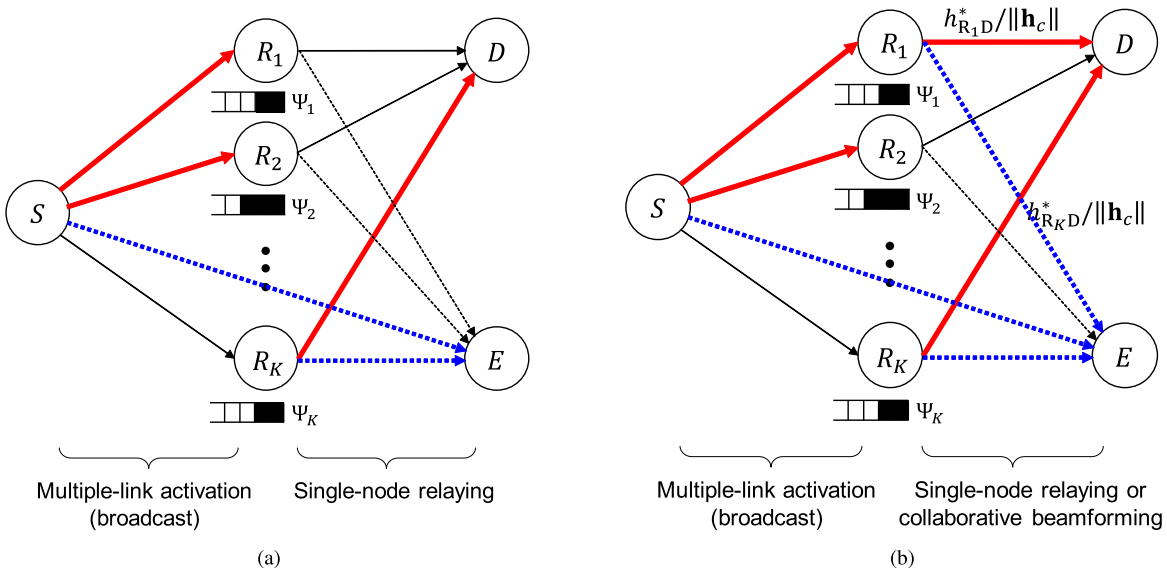


Fig. 1. System model of the proposed secure buffer-aided relaying schemes exploiting multiple SR links. (a) Proposed scheme without cooperative beamforming and (b) proposed scheme with cooperative beamforming.

secure relaying techniques consider only a single relay selection in each time slot, while owing to the broadcast nature of wireless channels, it is possible to simultaneously select multiple relay nodes, similar to [26], [32], and [33]. Moreover, while cooperative beamforming of buffer-aided relay nodes was proposed in [34], it has not been exploited in physical layer security. Furthermore, the previous secure buffer-aided relay selection schemes [35], [36] did not take into account the buffer states of relay nodes, hence potentially giving rise to the detrimental empty- or full-buffer states, which reduce the maximum number of available links.

Against this background, the novel contributions of this paper are as follows.

- We first propose a novel secure buffer-aided relay selection scheme that is capable of exploiting multiple SR links in a simultaneous manner. Since the number of design degrees of freedom is increased in comparison to the conventional max-ratio scheme, a significantly improved performance is achievable in terms of the secrecy outage probability and the end-to-end packet delay. Furthermore, our relay selection is carried out, based on buffer states of relay nodes, for the sake of avoiding the detrimental empty- and full-buffer states.
- We derive the analytical secrecy outage probability and packet delay bounds of our proposed scheme, based on a Markov chain model. Our bounds are used for an arbitrary signal-to-noise ratio (SNR) regime. Note that the generalized analytical framework introduced in this paper is also applicable to the previous max-ratio relay selection [35].
- The proposed scheme is further enhanced by introducing the concept of cooperative beamforming into our proposed buffer-aided relay selection. This is readily possible since our scheme allows relay nodes to share a packet in their buffers, while other previous buffer-aided secure communication schemes [35]–[37] do not. In this scheme, simultaneous activation of multiple RD links, i.e., cooperative beamforming, is exploited, in addition to that of SR links.
- Moreover, the concept of cooperative jamming is also incorporated into our scheme, in order to enhance the security, without relying on the use of full channel state information (CSI) associated with an eavesdropper. More specifically, a subset of a source, relay, and destination nodes are allowed to cooperatively transmit jammer to an eavesdropper, while the source node or the relay nodes simultaneously transmit a source packet.

The remainder of this paper is organized as follows. In Section II, the system model of our secure buffer-aided relay selection is introduced. In Section III, we derive the analytical bounds of secrecy outage probability and average packet delay for our scheme. In Section IV, the concept of cooperative beamforming is introduced into our scheme, while in Section V, the cooperative jamming technique is further amalgamated. Furthermore, Section VI provides our performance results, and finally, in Section VII, the present paper is concluded.

II. System Model

In this section, we introduce the system model of our buffer-state-based (BSB) secure relay selection, which is shown in Fig. 1(a). We consider a dual-hop cooperative network, comprising a single source node, K relay nodes, and a single destination node, with a single eavesdropper. The eavesdropper is capable of intercepting packets transmitted from the source and relay nodes. We assume a half-duplex mode for relay nodes, where either reception or transmission of a packet is possible in each time slot. Furthermore, no direct link between the source and the destination nodes exists, and hence a source packet has to be relayed by relay nodes, in order for the destination node to successfully receive it.

The complex-valued channel coefficients of the kth SR, the kth RD, the source-to-eavesdropper (SE), and the kth relay-to-eavesdropper (RE) links are respectively represented by h_{SR_k}, $h_{\mathrm{R}_k\mathrm{D}}$, h_{SE}, and $h_{\mathrm{R}_k\mathrm{E}}$, which are independently distributed quasi-static frequency-flat Rayleigh fading, having average gains of γ_{SR}, γ_{RD}, γ_{SE}, and γ_{RE}, respectively. For simplicity, we assume that all the channels and all the buffer states of relay nodes are accurately acquired at a central coordinator, similar to the conventional buffer-aided relay selection schemes [9]–[26], [32], [33], [35]–[37].[1] The kth relay node is equipped with a data buffer Ψ_k having a finite size L in terms of the number of packets, where data packets flow in a first-come first-out manner, similar to the previous studies. At each receiving node, the received signals are contaminated by additive white Gaussian noise (AWGN), whose power is assumed to be N_0.

In order to elaborate a little further, all the related buffer states and CSI at the central coordinator have to be updated every packet interval. However, the overhead imposed by this CSI update can be reduced for a scenario, having the channel coherence time longer than the packet interval, since CSI remains constant during the channel coherence time. A further overhead reduction is an open issue not only for the proposed scheme, but also for all the buffer-aided cooperative schemes.

The secrecy rates of the kth SR and the kth RD links are formulated as

$$\mathcal{C}_{\mathrm{SR}_k} = \frac{1}{2}\log_2\left(\frac{1+|h_{\mathrm{SR}_k}|^2/N_0}{1+|h_{\mathrm{SE}}|^2/N_0}\right), \tag{1}$$

$$\mathcal{C}_{\mathrm{R}_k\mathrm{D}} = \frac{1}{2}\log_2\left(\frac{1+|h_{\mathrm{R}_k\mathrm{D}}|^2/N_0}{1+|h_{\mathrm{R}_k\mathrm{E}}|^2/N_0}\right), \tag{2}$$

respectively, which represent the maximum achievable rates under the assumption that the eavesdropper is unable to decode the associated packet. Note that since we consider half-duplex relay nodes, a prelog factor of $1/2$ is imposed on the secrecy rates of (1) and (2). In this paper, we consider the scenario where there is a fixed end-to-end target rate r_{sc}. When the target rate is lower than the secrecy rate of a link, a packet is successful transmitted without being decoded by the eavesdropper. Otherwise, it becomes an outage event. For example, the secrecy outage probabilities of the local kth SR and RD links are represented by $P_{\mathrm{out}}^{\mathrm{SR}_k} = \Pr[\mathcal{C}_{\mathrm{SR}_k} < r_{\mathrm{sc}}]$, and $P_{\mathrm{out}}^{\mathrm{R}_k\mathrm{D}} = \Pr[\mathcal{C}_{\mathrm{R}_k\mathrm{D}} < r_{\mathrm{sc}}]$, respectively. Also note that in this fixed-rate scenario, the transmit power is adapted in order to minimize the total power consumption [34].

A. The Proposed Relay Selection Exploiting SR Broadcast Channels

In this section, we introduce our buffer-state-based relay selection scheme that ensures secure communications while maintaining a low secrecy outage probability and a low average packet delay. The basic relay selection criterion is to choose a link that has the maximum ratio of the channel gain over the associated eavesdropper channel, similar to [35] and [38], hence selecting the maximum from among $2K$ values, i.e.,

$$\zeta_{\mathrm{SR}_k} = |h_{\mathrm{SR}_k}|^2/|h_{\mathrm{SE}}|^2 \tag{3}$$

$$\zeta_{\mathrm{R}_k\mathrm{D}} = |h_{\mathrm{R}_k\mathrm{D}}|^2/|h_{\mathrm{R}_k\mathrm{E}}|^2 \quad (k = 1, \cdots, K). \tag{4}$$

However, the novel contributions over the previous secure buffer-aided transmission schemes [35–37] are two-fold. Our relay selection is carried out based on the buffer states of relay nodes, in order to avoid empty- and full-buffer states, which reduce the achievable performance. Furthermore, we exploit the broadcast nature of SR channels, where multiple SR links may be activated in a source broadcast phase, rather than selecting only a single one.

TABLE I
PRIORITY CLASSIFICATIONS OF AVAILABLE SR AND RD LINKS

Priority	Level 1 (Low)	Level 2 (Medium)	Level 3 (High)
SR links	$\Psi_k = L-1$	$1 < \Psi_k < L-1$	$\Psi_k = 0, 1$
RD links	$\Psi_k = 1$	$1 < \Psi_k < \xi$	$\Psi_k \geq \xi$

After acquiring the buffer states of all the relay nodes and the channel coefficients of $2K+2$ links, the central coordinator activates a single SR link, multiple SR links, or a single RD link, based on the proposed two-stage criterion. Firstly, from (1) and (2), each link is judged for whether it is in outage or not. Here, the numbers of available SR and RD links, which are not in outage, are denoted by N_{SR} and N_{RD} ($0 \leq N_{\mathrm{SR}}, N_{\mathrm{RD}} \leq K$), respectively. Then, depending on the buffer states, the central coordinator evaluates the priority of each available link, according to Table I, similar to [34]. More specifically, the N_{SR} available SR links are classified into three categories: Levels 1 to 3. The numbers of SR links having Level-1 (low), Level-2 (medium), and Level-3 (high) priorities are $N_{\mathrm{SR}}^{\mathrm{low}}$, $N_{\mathrm{SR}}^{\mathrm{med}}$, and $N_{\mathrm{SR}}^{\mathrm{high}}$, respectively, where $N_{\mathrm{SR}} = N_{\mathrm{SR}}^{\mathrm{low}} + N_{\mathrm{SR}}^{\mathrm{med}} + N_{\mathrm{SR}}^{\mathrm{high}}$. The priority of the kth SR link is Level 1 (low) when the number of packets stored at the associated relay buffer is $\Psi_k = L-1$, because only one additional packet is storable. The priority is Level 2 (medium) for $1 < \Psi_k < L-1$. Finally, the priority of the SR links is Level 3 (high) when the number of stored packets is $\Psi_k = 0$ or 1. Note, again, that when the priority of an SR link is low, the buffer state of the associated relay node is close to full, which is undesirable in terms of the maximum number of available links.

Similarly, the available N_{RD} RD links that are not in outage are categorized as Levels 1 to 3, where the numbers of links of the categories are denoted respectively by $N_{\mathrm{RD}}^{\mathrm{low}}$, $N_{\mathrm{RD}}^{\mathrm{med}}$, and $N_{\mathrm{RD}}^{\mathrm{high}}$. By introducing a thresholding parameter ξ ($< L$), the priority of the available RD links is classified as shown in Table I. When the buffer of a relay node is $\Psi_k = 1$, the priority of the associated RD link is Level 1 (low). Moreover, the priority is Level 2 (medium) for $1 < \Psi_k < \xi$ and is Level 3 (high) for $\Psi_k \geq \xi$. In order to provide further insights, the thresholding parameter ξ plays an important role in reducing the maximum number of packets stored in buffers

[1] This idealistic assumption of full CSI associated with an eavesdropper at a central coordinator is eliminated, by introducing cooperative jamming into our scheme in Section V.

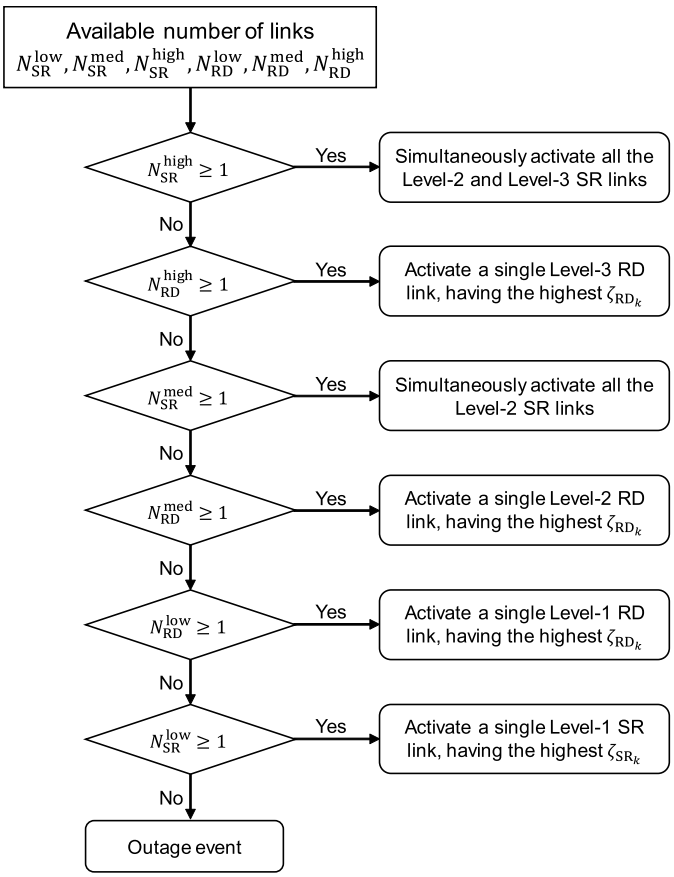


Fig. 2. Flow diagram of the decision rule for link activation of the proposed scheme without cooperative beamforming.

to below ξ. This contributed not only to the avoidance of a buffer overflow, but also to the reduction of a packet delay, as described later in Section III-B.

Having decided the priority of the available SR and RD links, link activation is carried out according to the proposed decision classification algorithm, which is shown in Fig. 2. When the number of Level-3 SR links is greater than one, all of the $N_{\mathrm{SR}}^{\mathrm{high}} + N_{\mathrm{SR}}^{\mathrm{med}}$ Level-3 and Level-2 SR links are simultaneously activated, where a source packet is copied to all buffers of the relay nodes associated with the activated SR links. When there is no Level-3 SR link, and when there is at least one Level-3 RD link, a single RD link having the highest $\zeta_{\mathrm{R}_k\mathrm{D}}$ value is activated. After the destination node decodes the relayed packet, the destination node sends an ACK packet to all of the relay nodes via the stable feedback channels, and the corresponding packet copied in the buffers of the relay nodes is deleted. Furthermore, when there are Level-2 SR links but neither Level-3 SR links nor Level-3 RD links, all of the $N_{\mathrm{SR}}^{\mathrm{med}}$ SR links are activated. Moreover, when there is at least one Level-2 RD link but no Level-3 SR, Level-3 RD, or Level-2 SR links, a single highest-$\zeta_{\mathrm{R}_k\mathrm{D}}$ Level-2 RD link is activated. If none of the above cases holds, we can have only Level-1 SR and RD links. More specifically, when we have at least one Level-1 RD link, a single highest-$\zeta_{\mathrm{R}_k\mathrm{D}}$ RD link is activated. Otherwise, a single Level-1 SR link having the highest ζ_{SR_k} value is activated. Finally, when we have no available links, this corresponds to an outage event.

III. Analysis of Secrecy Outage Probability and Average Delay

In this section, analytical bounds on the secrecy outage probability and the average packet delay are derived for the proposed scheme.

In a similar manner to the conventional bounds introduced for the previous buffer-aided relay selection schemes [13], [25], [26], [33], [34], we assume that a sufficiently high number of packets are transmitted from the source node to the destination node. Note that in this section, independently distributed channels are assumed, and hence the bounds derived here are readily applicable not only to symmetric, but also to asymmetric channels, such that the average SNRs corresponding to the SR an RD links are different, i.e., $\gamma_{\mathrm{SR}} \neq \gamma_{\mathrm{RD}}$.

A. Analytical Bound on Secrecy Outage Probability

We consider a Markov chain model that is valid specifically for the proposed scheme, where the number of states is given by the combination of packets stored at the buffers of relay nodes. Note that in our proposed scheme, a packet may be shared by multiple relay nodes, hence exhibiting more legitimate states than the conventional buffer-aided secure communication schemes [35], [36], which do not allow a packet copy in the buffers of multiple relay nodes.

Let us define Ξ_n and Ξ_n^a as the set of legitimate links and the set of available links, respectively, for state s_n [34]. Also, the number of legitimate states is given by N_{state}, while U_n is the set of states that have the possibility of having arrived from state s_n through a one-step transition. For instance, the legitimate states for the scenario of $(K, L) = (2, 2)$ are exemplified in Table II, similar to [34]. Note that the four symbols shown in Table II, i.e., ◯, △, □, and △, denote four different packets. The total number of states is $N_{\mathrm{state}} = 19$. Similarly, the related state transition of the proposed scheme with $(K, L) = (2, 2)$ is also the same as that of [34, Fig. 2(b)].

Furthermore, $\mathbf{A} \in \mathbb{R}^{N_{\mathrm{state}} \times N_{\mathrm{state}}}$ is defined as the transition matrix of the Markov model, where the element in the ith-row and jth-column of $\mathbf{A}$ is given by

$$\mathrm{A}_{ij} = \sum_{\Xi_j^a \subset \Xi_j} \Pr^{\mathrm{SR}}(\Xi_j^a) \Pr^{\mathrm{RD}}(\Xi_j^a) \Pr(s_j \rightarrow s_i | \Xi_j^a), \tag{5}$$

in which $s_i \in U_j$ is a state that is directly connected to the state s_j. Furthermore, $\Pr^{\mathrm{SR}}(\Xi_j^a)$ represents the probability of having available SR links in the subset Ξ_j^a, while $\Pr^{\mathrm{RD}}(\Xi_j^a)$ is that of having RD links in the same subset. Moreover, the conditional probability $\Pr(s_j \rightarrow s_i | \Xi_j^a)$ is calculated, according to the algorithm of Fig. 2. Since the steady-state probabilities $\boldsymbol{\pi} \in \mathbb{R}^{N_{\mathrm{state}}}$ are formulated in closed form as [26]

$$\boldsymbol{\pi} = (\mathbf{A} - \mathbf{I} + \mathbf{B})^{-1} \mathbf{b} \in \mathbb{R}^{N_{\mathrm{state}}}, \tag{6}$$

we arrive at the theoretical bound of the secrecy outage probability as [13]

$$P_{\mathrm{out}} = \mathrm{diag}(\mathbf{A}) \boldsymbol{\pi}. \tag{7}$$

Here, all the elements in $\mathbf{B} \in \mathbb{R}^{N_{\mathrm{state}} \times N_{\mathrm{state}}}$ and $\mathbf{b} \in \mathbb{R}^{N_{\mathrm{state}}}$ are ones, while $\mathbf{I} \in \mathbb{R}^{N_{\mathrm{state}} \times N_{\mathrm{state}}}$ is the identity matrix.

TABLE II
LEGITIMATE BUFFER STATES OF $K = 2$ RELAY NODES WITH ($L = 2$)-SIZED BUFFERS. ©2018 IEEE. REPRINTED, WITH PERMISSION, FROM [34]

States	Relay 1		Relay 2	
s_1	empty	empty	empty	empty
s_2	◯	empty	empty	empty
s_3	empty	empty	◯	empty
s_4	◯	□	empty	empty
s_5	◯	empty	□	empty
s_6	empty	empty	◯	□
s_7	◯	△	□	empty
s_8	◯	empty	□	△
s_9	◯	△	□	◇
s_{10}	◯	empty	◯	empty
s_{11}	◯	△	◯	empty
s_{12}	◯	empty	◯	△
s_{13}	◯	△	◯	△
s_{14}	◯	△	◯	□
s_{15}	◯	empty	□	◯
s_{16}	◯	△	□	◯
s_{17}	□	◯	◯	empty
s_{18}	□	◯	◯	△
s_{19}	□	◯	△	◯

Next, we derive the probabilities $\Pr^{\mathrm{SR}}(\Xi_j^a)$ and $\Pr^{\mathrm{RD}}(\Xi_j^a)$ of (5) in the closed forms, in order to calculate the theoretical secrecy outage probability of (7). In [39], a general cooperative wiretap model, i.e., multiple-input multiple-output channel in the presence of a single eavesdropper (MIMOSE), was investigated, which supports multiple source nodes and multiple destination nodes. The secrecy outage probability of the MIMOSE wiretap model is formulated by [39]

$$\Pr\left(\frac{C_M}{C_E} < r_0\right) = F(2^{2r_0}-1) + e^{\frac{-\left(\frac{1}{2^{2r_0}}-1\right)}{\gamma_E}}\mathcal{G}(r_0), \tag{8}$$

where

$$\mathcal{G}(r_0) = \int_{e^{r_0}-1}^{\infty} e^{\frac{-\theta e^{-r_0}}{\gamma_M}} f(\theta)d\theta, \tag{9}$$

and

$$F(x) = \left[1 - \sum_{m=0}^{N_{\mathrm{S}}-1} \frac{e^{-x/\gamma_M}}{m!}\left(\frac{x}{\gamma_M}\right)^m\right]^{N_{\mathrm{D}}} \tag{10}$$

$$f(x) = N_{\mathrm{D}}\left[1 - \sum_{m=0}^{N_{\mathrm{S}}-1} \frac{e^{-x/\gamma_M}}{m!}\left(\frac{x}{\gamma_M}\right)^m\right]^{N_{\mathrm{D}}-1} \times \left[\sum_{m=0}^{N_{\mathrm{S}}-1}\left(\frac{x}{\gamma_M} - m\right)\frac{e^{-x/\gamma_M}}{m!}\frac{x^{m-1}}{\gamma_M^m}\right]. \tag{11}$$

Here, C_M and C_E are the capacities of the main and the eavesdropper channels, respectively, while γ_M and γ_E are the corresponding SNR values. Also, N_{S} and N_{D} are the number of source and destination nodes in the MIMOSE model.

Since the SR transmission in the proposed scheme corresponds to that considered in the MIMOSE model with $N_{\mathrm{S}} = 1$, by applying the theory of order statistics [40], the CDF of having available SR links in the subset of Ξ_j^a is given by

$$F_{\Xi_j^a}^{\mathrm{SR}}(x) = \left(e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{S_{\mathrm{SR}}}\left(1 - e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{O_{\mathrm{SR}}}, \tag{12}$$

where S_{SR} and $\tilde{S}_{\mathrm{SR}}$ are the numbers of the SR links in the subset Ξ_j^a and the set Ξ_j, respectively, and $O_{\mathrm{SR}} = \tilde{S}_{\mathrm{SR}} - S_{\mathrm{SR}}$. Moreover, the PDF of (12) is formulated by

$$\begin{aligned} f_{\Xi_j^a}^{\mathrm{SR}}(x) &= \frac{1}{\gamma_{\mathrm{SR}}}\left[O_{\mathrm{SR}}\left(e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{S_{\mathrm{SR}}+1}\left(1 - e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{O_{\mathrm{SR}}-1} - \frac{S_{\mathrm{SR}}(O_{\mathrm{SR}}+1)}{O_{\mathrm{SR}}+1}\left(e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{S_{\mathrm{SR}}}\left(1 - e^{-\frac{x}{\gamma_{\mathrm{SR}}}}\right)^{O_{\mathrm{SR}}}\right] \\ &= \frac{1}{\gamma_{\mathrm{SR}}}\left[\sum_{i=1}^{O_{\mathrm{SR}}}(-1)^{i-1}\binom{O_{\mathrm{SR}}}{i} i e^{\frac{-(i+S_{\mathrm{SR}})x}{\gamma_{\mathrm{SR}}}} - \frac{S_{\mathrm{SR}}}{O_{\mathrm{SR}}+1} \times \sum_{j=1}^{O_{\mathrm{SR}}+1}(-1)^{j-1}\binom{O_{\mathrm{SR}}+1}{j} j e^{\frac{-(j+S_{\mathrm{SR}}-1)x}{\gamma_{\mathrm{SR}}}}\right]. \end{aligned} \tag{13}$$

By substituting (9)–(13) into (8), we arrive at $\Pr^{\mathrm{SR}}(\Xi_j^a)$ as

$$\begin{aligned} \Pr^{\mathrm{SR}}(\Xi_j^a) = \left(e^{-\frac{2^{2r}-1}{\gamma_{\mathrm{SR}}}}\right)^{S_{\mathrm{SR}}}\left(1 - e^{-\frac{2^{2r}-1}{\gamma_{\mathrm{SR}}}}\right)^{O_{\mathrm{SR}}} + \frac{e^{-\frac{2^{-2r}-1}{\gamma_{\mathrm{SE}}}}}{\gamma_{\mathrm{SR}}} \\ \times \left[\sum_{i=1}^{O_{\mathrm{SR}}}(-1)^{i-1}\binom{O_{\mathrm{SR}}}{i} i e^{-(2^{2r}-1)\tau_1} - \frac{S_{\mathrm{SR}}}{O_{\mathrm{SR}}+1} \times \sum_{j=1}^{O_{\mathrm{SR}}+1}(-1)^{j-1}\binom{O_{\mathrm{SR}}+1}{j}\frac{j}{\tau_2}e^{-(2^{2r}-1)\tau_2}\right], \end{aligned} \tag{14}$$

where we have

$$\tau_1 = \frac{2^{-2r}}{\gamma_{\mathrm{SE}}} + \frac{i + S_{\mathrm{SR}}}{\gamma_{\mathrm{SR}}} \tag{15}$$

$$\tau_2 = \frac{2^{-2r}}{\gamma_{\mathrm{SE}}} + \frac{j + S_{\mathrm{SR}} - 1}{\gamma_{\mathrm{SR}}}. \tag{16}$$

Similarly, the RD transmission in the proposed scheme corresponds to that considered in the MIMOSE model with $N_{\mathrm{S}} = N_{\mathrm{D}} = 1$, because each RD link in the proposed scheme is independently tractable, unlike the SR links. More specifically, the probability $\Pr^{\mathrm{RD}}(\Xi_j^a)$ of (5) is expressed by

$$\Pr^{\mathrm{RD}}(\Xi_j^a) = (1 - P_e)^{S_{\mathrm{RD}}}(P_e)^{O_{\mathrm{RD}}}, \tag{17}$$

where S_{RD} and O_{RD} are defined as the number of available and unavailable RD links in the jth state, similar to the SR hop. Also, P_e is the probability that each RD link is in secrecy outage. More specifically, by substituting the CDF and the PDF of

$$F_e = 1 - e^{-\frac{x}{\gamma_{\mathrm{RD}}}} \tag{18}$$

$$f_e = \frac{1}{\gamma_{\mathrm{RD}}}e^{-\frac{x}{\gamma_{\mathrm{RD}}}} \tag{19}$$

into (8) and (9), we obtain P_e as

$$P_e = 1 - e^{-\frac{2^{2r}-1}{\gamma_{\mathrm{RD}}}} + \frac{1}{\gamma_{\mathrm{RD}}} e^{-\frac{2^{-2r}-1}{\gamma_{\mathrm{RE}}}} \frac{1}{\tau_3} e^{-(2^{2r}-1)\tau_3} = 1 - \frac{1}{1 + 2^{2r_0} \frac{\gamma_{\mathrm{RE}}}{\gamma_{\mathrm{RD}}}} e^{-\frac{2^{2r}-1}{\gamma_{\mathrm{RD}}}}, \tag{20}$$

where we have

$$\tau_3 = \frac{2^{-2r}}{\gamma_{\mathrm{RE}}} + \frac{1}{\gamma_{\mathrm{RD}}}. \tag{21}$$

Finally, by substituting (20) into (17), we arrive at

$$\Pr^{\mathrm{RD}}(\Xi_j^a) = \sum_{i=0}^{O_{\mathrm{RD}}} (-1)^{i+1} \binom{O_{\mathrm{RD}}}{i} \left(\frac{e^{-\frac{2^{2r}-1}{\gamma_{\mathrm{RD}}}}}{1 + 2^{2r_0} \frac{\gamma_{\mathrm{RE}}}{\gamma_{\mathrm{RD}}}} \right)^{S_{\mathrm{RD}}+i}. \tag{22}$$

B. Analytical Bound of Average Packet Delay

Let us assume that the average gains of the SR and RD links are identical. Then, similar to [34], the average packet delay at the kth relay node of interest is given by

$$\mathbb{E}[T_k] = \frac{\mathbb{E}[\Psi_k]}{\eta_k}, \tag{23}$$

where η_k is the average throughput of the kth relay node. Since the probability of selecting each relay node is identical in our assumed system, similar to [19], the average delay is given in the same manner as (23).

To be more specific, (23) is rewritten as

$$\mathbb{E}[T_k] = \frac{2}{1 - P_{\mathrm{out}}} \sum_{i=1}^{N_{\mathrm{state}}} \pi_i \Psi(i), \tag{24}$$

where π_i is the ith element of the states $\boldsymbol{\pi}$, and $\Psi(i)$ is the number of different packets stored at the K relay nodes for state π_i. Additionally, $p_{kj}(i)$ is the probability of selecting the jth RD link, which decreases the number of packets stored at the kth relay node.

Note that as clearly shown in (23), the average number of packets stored in buffers is directly related to the packet delay. Hence, it is analytically true that the packet delay decreases, upon decreasing the thresholding parameter ξ, introduced in our protocol.

IV. The Proposed Scheme Supporting Cooperative Beamforming

In this section, we introduce the concept of cooperative beamforming into our relaying scheme proposed in Section II, which allows us to exploit not only the simultaneous activation of multiple SR links but also that of the multiple RD links. Hence, this allows us to further increase the number of design degrees of freedom.

The system model of our secure buffer-state-based relaying scheme relying on cooperative beamforming is shown in Fig. 1(b). Firstly, according to Table I, the priority of each SR and RD link is assessed by a central coordinator. Then, the appropriate link(s) are activated from among the four modes: activation of a single SR link, a single RD link, multiple SR links, or multiple RD links. The decision rule of the link activation is similar to the proposed scheme without cooperative beamforming, with the only difference being that, in the proposed scheme with cooperative beamforming, multiple RD-link activation mode (i.e., cooperative beamforming) is enabled when a packet is shared among the relay nodes.

Define the RD channels corresponding to the cooperative relay nodes as $\mathbf{h}_c = [h_c^{(1)}, \cdots, h_c^{(Q)}]^T$, where Q is the number of cooperative relay nodes. When the multiple RD link activation mode is selected according to the above-mentioned selection rule, the cooperative relay nodes simultaneously transmit a shared packet, where the conjugates of normalized channel coefficients $h_c^{(q)*}/\|\mathbf{h}_c\|$ are amplified by the symbol at the qth cooperative relay node before the transmission. Hence, the associated information rate is given by $\mathcal{C}_c = \frac{1}{2}\log_2\left(1 + \gamma_{\mathrm{RD}}\|\mathbf{h}_c\|^2\right)$.

The beamforming exemplified in this paper corresponds to simple conjugate beamforming [34], [41], which maximizes the SNR at the destination node. As the explicit benefit of conjugate beamforming, overhead imposed by the collaboration between the relay nodes is significantly simplified. However, in terms of the achievable secrecy rate performance, a cooperative beamforming scheme that takes into account the channels associated with the eavesdropper, such as cooperative jamming, is beneficial. The related detailed investigations are left for the future study.

Note that while the proposed scheme relying on cooperative beamforming is expected to achieve a higher performance than the proposed scheme without cooperative beamforming, this is achieved at the sacrifice of additional overhead imposed by synchronization between relay nodes.

V. The Proposed Scheme Supporting Cooperative Jamming

In this section, the concept of cooperative jamming is introduced into our scheme of Section IV, where artificial noises are transmitted from the subset of source node, relay nodes, and destination node, in order to interfere with an eavesdropper's reception, hence increasing security. This technique is especially beneficial, when full CSI associated with an eavesdropper is unavailable at a central coordinator. In this section, we assume that the partial CSI of an eavesdropper, i.e., the average SNRs of SE and RE links γ_{SE} and γ_{RE}, are acquired at a central coordinator.

Fig. 3 illustrates the system model of our scheme with cooperative jamming, where solid lines represent channels of signal transmissions, while dashed lines correspond to those of artificial noise transmissions. In this proposed scheme, cooperative jamming is carried out in a different manner, depending on the SR broadcast phase and the RD relaying phase, which are shown in Figs. 3(a) and 3(b), respectively.

A. Cooperative Jamming in SR Broadcast Phase

As shown in Fig. 3(a), in the SR broadcast phase, K relay nodes are divided into K^{d} relay nodes that receive a source packet and K^{j} relay nodes that transmit artificial noises, where

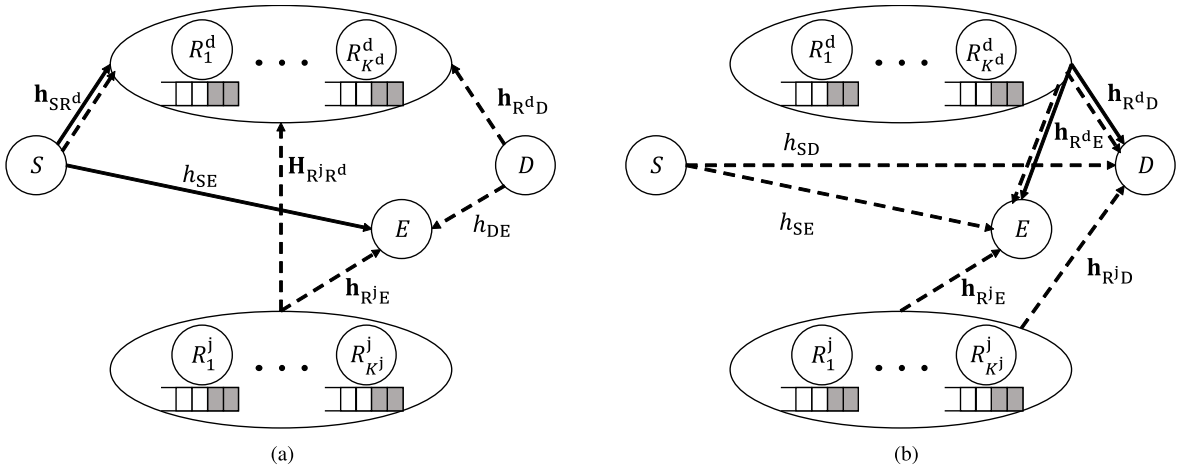


Fig. 3. System model of the proposed secure buffer-aided relaying schemes using cooperative jamming. (a) SR broadcast phase and (b) RD relaying phase.

we have $K = K^{\mathrm{d}} + K^{\mathrm{j}}$. Here, we impose the constraint of $K^{\mathrm{d}} \leq \lceil K/2 \rceil$, in order to configure nulls to K^{d} relay nodes . We assume that the average SNRs of relay-to-relay and destination-to-eavesdropper (DE) links are represented by γ_{RR} and γ_{DE}, respectively.

Similar to [42], the source node broadcasts source signals $x(t)$ added by artificial noises $a(t)$ as follows:

$$s_{\mathrm{S}}(t) = \sqrt{P_x}x(t) + w_S\sqrt{P_a}a(t) \in \mathbb{C}, \tag{25}$$

where P_x and P_a denote the powers of source signals and artificial noises, respectively. Furthermore, w_S is a weight, multiplied by the artificial noises at the source node.

Here, K^{j} relay nodes and the destination node cooperatively transmit artificial noises $a(t)$ simultaneously with the source node's transmission of (25), where the signals are given, respectively, by

$$\mathbf{s}_{\mathrm{R}}(t) = \mathbf{w}_R\sqrt{P_a}a(t) \in \mathbb{C}^{K^{\mathrm{j}}}, \tag{26}$$

$$s_{\mathrm{D}}(t) = w_D\sqrt{P_a}a(t) \in \mathbb{C}. \tag{27}$$

Here, $\mathbf{w}_R \in \mathbb{C}^{K^{\mathrm{j}}}$ and $w_D \in \mathbb{C}$ are weights, multiplied by the artificial noises at the K^{j} relay nodes and the destination node, respectively.

Hence, the signals received at the K^{d} relay nodes $\mathbf{r}_{\mathrm{R}}(t) \in \mathbb{C}^{K^{\mathrm{d}}}$ are given by

$$\begin{aligned}\mathbf{r}_{\mathrm{R}}(t) &= \mathbf{h}_{\mathrm{SR^d}}\sqrt{P_x}x(t) \\ &\quad + \left(\mathbf{H}_{\mathrm{R^jR^d}}^T\mathbf{w}_R + \mathbf{h}_{\mathrm{SR^d}}w_S + \mathbf{h}_{\mathrm{R^dD}}w_D\right)\sqrt{P_a}a(t) \\ &= \mathbf{h}_{\mathrm{SR^d}}\sqrt{P_x}x(t) + \mathbf{H}^{\mathrm{j}}\mathbf{w}\sqrt{P_a}a(t),\end{aligned} \tag{28}$$

where $\mathbf{h}_{\mathrm{SR^d}} \in \mathbb{C}^{K^{\mathrm{d}}}$ and $\mathbf{h}_{\mathrm{R^dD}} \in \mathbb{C}^{K^{\mathrm{d}}}$ are the channel vector between the source node and the K^{d} relay nodes, and that between the K^{d} relay nodes and the destination node, respectively. Also, $\mathbf{H}_{R^jR^d} = \mathbb{C}^{K^{\mathrm{j}}\times K^{\mathrm{d}}}$ represents the channel coefficients between the K^{d} and K^{j} relay nodes. Furthermore, we have $\mathbf{w} = [w_S, w_D, \mathbf{w}_R^T]^T \in \mathbb{C}^{K^{\mathrm{j}}+2}$ and $\mathbf{H}^{\mathrm{j}} = [\mathbf{h}_{\mathrm{SR^d}}, \mathbf{h}_{\mathrm{R^dD}}, \mathbf{H}_{\mathrm{R^jR^d}}^T] \in \mathbb{C}^{K^{\mathrm{d}}\times(K^{\mathrm{j}}+2)}$. Furthermore, by setting the weight vector, such that $\mathbf{H}^{\mathrm{j}}\mathbf{w} = \mathbf{0}$ and $\|\mathbf{w}\|^2 = 1$ are satisfied, the K^{d} relay nodes do not suffer from the effects of the artificial noises in (28). Note that the total transmit power of the source node is $P_x + P_a$.

By contrast, the signals received at the eavesdropper $r_{\mathrm{E}}(t) \in \mathbb{C}$ is given by

$$\begin{aligned}r_{\mathrm{E}}(t) &= h_{\mathrm{SE}}\sqrt{P_x}x(t) \\ &\quad + \left(\mathbf{h}_{\mathrm{R^jE}}^T\mathbf{w}_R + h_{\mathrm{SE}}w_S + h_{\mathrm{DE}}w_D\right)\sqrt{P_a}a(t) \\ &= h_{\mathrm{SE}}\sqrt{P_x}x(t) + (\mathbf{h}^{\mathrm{E}})^T\mathbf{w}\sqrt{P_a}a(t),\end{aligned} \tag{29}$$

where we have $\mathbf{h}^{\mathrm{E}} = [h_{\mathrm{SE}}, h_{\mathrm{DE}}, \mathbf{h}_{\mathrm{R^jE}}^T]^T \in \mathbb{C}^{K^{\mathrm{j}}+2}$.

Finally, we obtain the secrecy rate in the SR broadcast phase as

$$\mathcal{C}_{\mathrm{SR}}^{J} = \frac{1}{2}\log_2\left(\frac{1 + \dfrac{P_x|h_{\mathrm{SR}}^{\min}|^2}{N_0}}{1 + \dfrac{P_x|h_{\mathrm{SE}}|^2}{N_0 + P_a\|\mathbf{h}^{\mathrm{E}}\|^2}}\right), \tag{30}$$

where $|h_{\mathrm{SR}}^{\min}|$ represents the minimum absolute value of elements in $\mathbf{h}_{\mathrm{SR^d}}$.

B. Cooperative Jamming in RD Relaying Phase

The system model of the RD relaying phase in our cooperative jamming is shown in Fig. 3(b). The K^{d} relay nodes that retransmit source signals as well as artificial noises are selected, based on the algorithm of Section V-C. Simultaneously with the relay nodes' retransmission, the source node, the remaining $K^{\mathrm{j}} = K - K^{\mathrm{d}}$ relay nodes, and the destination node cooperatively transmit artificial noises $a(t)$.

The signals transmitted from the K^{d} relay nodes $\mathbf{s}_{\mathrm{R^d}}(t) \in \mathbb{C}^{K^{\mathrm{d}}}$ are represented by

$$\mathbf{s}_{\mathrm{R^d}}(t) = \mathbf{v}\sqrt{P_x}x(t) + \mathbf{w}_{R^{\mathrm{d}}}\sqrt{P_a}a(t), \tag{31}$$

where we have $\mathbf{v} = \mathbf{h}_{\mathrm{R^dD}}^*/\|\mathbf{h}_{\mathrm{R^dD}}\| \in \mathbb{C}^{K^{\mathrm{d}}}$, which is the weight vector used for cooperative beamforming, and $\mathbf{w}_{R^{\mathrm{d}}} \in \mathbb{C}^{K^{\mathrm{d}}}$ are the weights used for the K^{d} relay nodes' artificial noises.

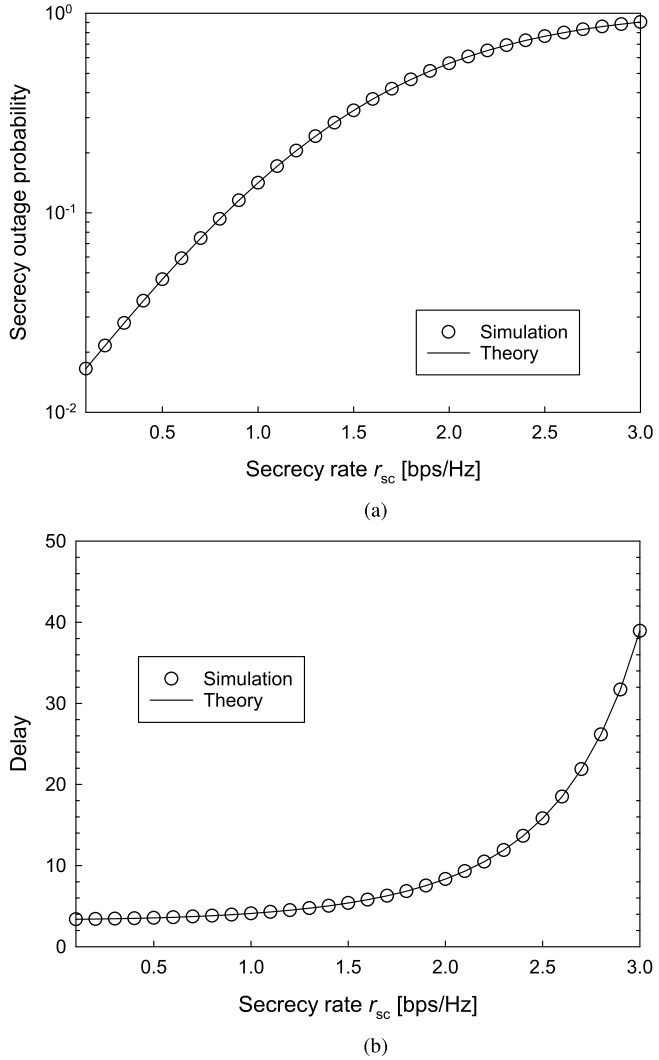


Fig. 4. Theoretical and numerical curves of the proposed scheme without beamforming with parameters $(K, L) = (2, 2)$, SNR $\gamma_{SR} = \gamma_{RD} = 20$ dB, and the secrecy rate r_{sc} varied from 0.1 to 3.0 bps/Hz. (a) Secrecy outage probability and (b) delay.

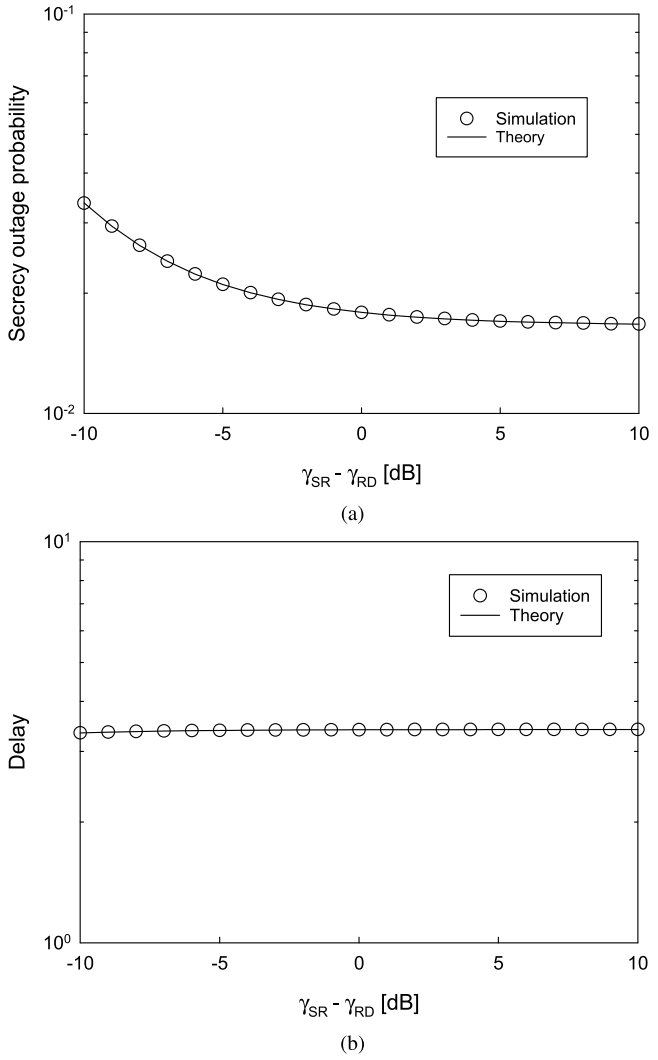


Fig. 5. Theoretical and numerical curves of the proposed scheme without beamforming with parameters $(K, L) = (2, 2)$, while considering the asymmetric channels, having the average SNRs of $\gamma_{SR} = 10$ dB and $\gamma_{RD} = 0$–20 dB. The secrecy rate was given by $r_{sc} = 1$ bps/Hz. (a) Secrecy outage probability and (b) delay.

Furthermore, the artificial noises, transmitted from the source node and the K^{j} relay nodes, are expressed, respectively, as

$$s_{\mathrm{S}}(t) = w_S\sqrt{P_a}a(t) \in \mathbb{C} \tag{32}$$

$$\mathbf{s}_{\mathrm{R^j}}(t) = \mathbf{w}_{\mathrm{R^j}}\sqrt{P_a}a(t) \in \mathbb{C}^{K^{\mathrm{j}}}, \tag{33}$$

where $\mathbf{w}_{\mathrm{R^j}}$ are the weights, associated with the K^{j} relay nodes.

Hence, we arrive at the signals received at the destination node $r_{\mathrm{D}}(t) \in \mathbb{C}$ as follows:

$$\begin{aligned} r_{\mathrm{D}}(t) &= \mathbf{h}_{\mathrm{R^dD}}^T\mathbf{v}\sqrt{P_x}x(t) \\ &\quad + \left(\mathbf{h}_{\mathrm{R^dD}}^T\mathbf{w}_{\mathrm{R^d}} + \mathbf{h}_{\mathrm{R^jD}}^T\mathbf{w}_{\mathrm{R^j}}\right)\sqrt{P_a}a(t) \\ &= \sqrt{\|\mathbf{h}_{\mathrm{R^dD}}\|^2\ P_x}x(t) + (\mathbf{h}^{\mathrm{j}})^T\mathbf{w}\sqrt{P_a}a(t). \end{aligned} \tag{34}$$

where we have $\mathbf{w} = [\mathbf{w}_{\mathrm{R^d}}^T, \mathbf{w}_{\mathrm{R^j}}^T]^T \in \mathbb{C}^K$ and $\mathbf{h}^{\mathrm{j}} = [\mathbf{h}_{\mathrm{R^dD}}^T, \mathbf{h}_{\mathrm{R^jD}}^T]^T \in \mathbb{C}^K$. Then, the weights are calculated, so as to satisfy $(\mathbf{h}^{\mathrm{j}})^T\mathbf{w} = 0$ and $\|\mathbf{w}\|^2 = 1$, hence canceling out the second term of (34). The signals received at the eavesdropper are given by

$$\begin{aligned} r_{\mathrm{E}}(t) &= \mathbf{h}_{\mathrm{R^dE}}^T\mathbf{v}\sqrt{P_x}x(t) \\ &\quad + \left(h_{\mathrm{SE}}w_S + \mathbf{h}_{\mathrm{R^dE}}^T\mathbf{w}_{\mathrm{R^d}} + \mathbf{h}_{\mathrm{R^jE}}^T\mathbf{w}_{\mathrm{R^j}}\right)\sqrt{P_a}a(t) \\ &= \frac{\mathbf{h}_{\mathrm{R^dE}}^T\mathbf{h}_{\mathrm{R^dD}}^*}{\|\mathbf{h}_{\mathrm{R^dD}}\|}\sqrt{P_x}x(t) + (\mathbf{h}^{\mathrm{E}})^T\mathbf{w}\sqrt{P_a}a(t), \end{aligned} \tag{35}$$

where $\mathbf{h}_{\mathrm{R^dE}} \in \mathbb{C}^{K^{\mathrm{d}}}$ are the channel coefficients between the K^{d} relay nodes and the eavesdropper, while we have $\mathbf{h}^{\mathrm{E}} = [h_{\mathrm{SE}}, \mathbf{h}_{\mathrm{R^dE}}^T, \mathbf{h}_{\mathrm{R^jE}}^T]^T \in \mathbb{C}^{K+1}$.

Hence, the secrecy rate in the RD relaying phase of our cooperative jamming is formulated by

$$\mathcal{C}_{\mathrm{RD}}^J = \frac{1}{2}\log_2\left(\frac{1 + \dfrac{P_x\|\mathbf{h}_{\mathrm{R^dD}}\|^2}{N_0}}{1 + \dfrac{P_x\left|\mathbf{h}_{\mathrm{R^dE}}^T\mathbf{h}_{\mathrm{R^dD}}^*\right|^2/\|\mathbf{h}_{\mathrm{R^dD}}\|^2}{N_0 + P_a\|\mathbf{h}^{\mathrm{E}}\|^2}}\right). \tag{36}$$

TABLE III
BASIC SYSTEM PARAMETERS EMPLOYED IN OUR SIMULATIONS

Number of Monte Carlo simulatoins	10^4
Frame length	10^5 packets
Channels	Symmetric Rayleigh fading
SNR	$\gamma_{\rm SR} = \gamma_{\rm RD} = \gamma_{\rm RR} = [20, 40]$ dB
SNR ratios of SR and SE links	$\zeta_{{\rm SR}_k} = [1, 5]$
SNR ratios of RD and RE links	$\zeta_{{\rm R}_k{\rm D}} = [1, 5]$
SNR ratios of DR and DE links	$\zeta_{\rm DE} = [1, 5]$
Thresholding parameter	$\xi = 2$
Target secrecy rate	$r_{\rm sc} \in [0.1, 3.0]$
Number of relay nodes	$K \in [2, 20]$
Buffer size	$L = 5$

C. Link Selection Algorithm

In this section, we introduce the link selection algorithm of our cooperative jamming scheme. The underlying concept of our protocol is that the relay nodes, having the channels unfavorable for sending a source packet in terms of the secrecy rate, are assigned for sending artificial noises.

More specifically, in order to judge whether each link is outage or not, instead of (1) and (2), we herein use the following rates

$$\mathcal{C}^{\rm jam}_{{\rm SR}_k} = \frac{1}{2}\log_2\left(\frac{1 + P_x|h_{{\rm SR}_k}|^2/N_0}{1 + P_x\gamma_{\rm SE}}\right) \tag{37}$$

$$\mathcal{C}^{\rm jam}_{\rm RD} = \frac{1}{2}\log_2\left(\frac{1 + P_x\|\mathbf{h}_{{\rm R}^{\rm d}{\rm D}}\|^2/N_0}{1 + P_x\gamma_{\rm RE}}\right). \tag{38}$$

This is because we assume that only partial CSI associated with the eavesdropper can be used at the central coordinator of our cooperative jamming.

Similar to our scheme without cooperative jamming, the link priority set is first determined, according to Table I. Then, based on the algorithm of Fig. 2, active link sets are decided, where we limit the number of relay nodes that receive a source packet in the SR broadcast phase, or retransmit a source packet in the RD relaying phase, up to $\lceil K/2 \rceil$. Here, the relay nodes, having the highest secrecy rates (37), are selected. Then, the remaining unselected relay nodes are set to the ones transmitting artificial noises.

VI. PERFORMANCE RESULTS

In this section, we provide our performance results based on Monte Carlo simulations carried out in order to characterize the proposed scheme. The basic system parameters employed in our simulations are listed in Table III. In addition, we considered 10^4 frames per simulation, each having 10^5 packets, and all the channel coefficients were randomly generated in each time slot. The thresholding parameter was maintained at $\xi = 2$ unless otherwise noted. The buffer-aided max-ratio scheme [35] was chosen as a benchmark scheme. Furthermore, we considered symmetric channels, i.e., $\gamma_{\rm SR} = \gamma_{\rm RD}$ and $\gamma_{\rm SE} = \gamma_{\rm RE}$, with the ratios maintained at $\zeta_{{\rm SR}_k} = \zeta_{{\rm R}_k{\rm D}} = 5$.

A. Theoretical Results

Fig. 4 compares the theoretical and numerical curves of the proposed scheme without beamforming, where we considered the system parameters of $(K, L) = (2, 2)$, and the SNR was set to $\gamma_{\rm SR} = \gamma_{\rm RD} = 20$ dB while varying the secrecy rate $r_{\rm sc}$ from 0.1 to 3.0 bps/Hz. More specifically, Figs. 4(a) and 4(b) show the secrecy outage probability and the end-to-end delay, respectively. Note that the theoretical curves were calculated from (7) and (24), derived in Section III. As shown, the theoretical and numerical curves matched well, and hence the system model of our proposed scheme is validated.

In Fig. 5, we considered the asymmetric channels, having $\gamma_{\rm SR} \neq \gamma_{\rm RD}$, where the SNR of SR links was maintained to be $\gamma_{\rm SR} = 10$ dB, while varying that of RD links from $\gamma_{\rm RD} = 0$ to 20 dB. The other system parameters were the same as those used in Fig. 4. It was found in Fig. 5 that similar to Fig. 4, the theoretical and numerical curves coincided.

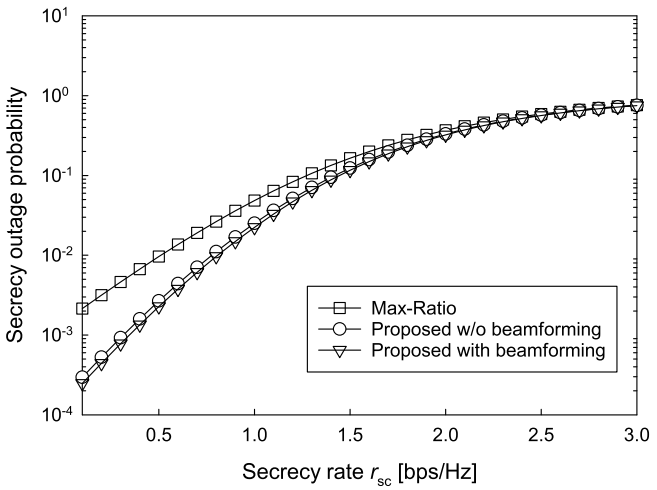


Fig. 6. Secrecy outage probability of the proposed schemes with/without cooperative beamforming and the max-ratio scheme with parameters $(K, L) = (3, 5)$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc}$ varied from 0.1 to 3.0 bps/Hz.

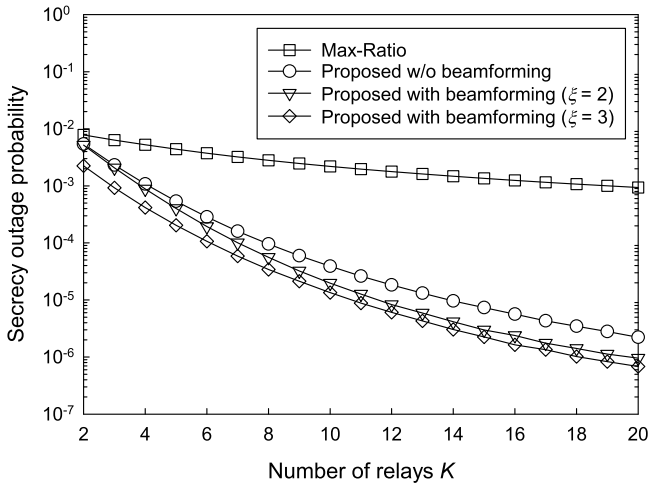
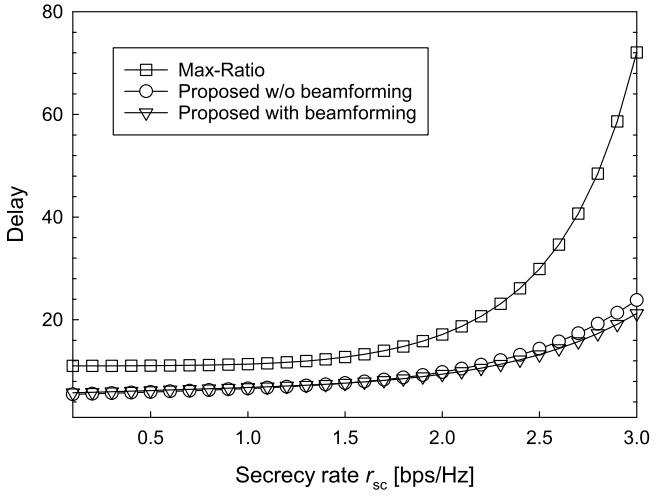


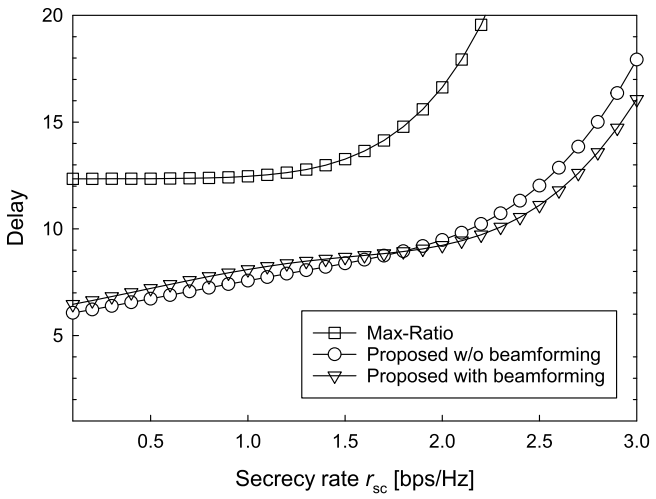
Fig. 7. Secrecy outage probability of the proposed scheme and the max-ratio scheme with parameters K varied from 2 to 20, buffer size $L = 5$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc} = 1$ bps/Hz.

B. Numerical Results of the Proposed Scheme With and Without Cooperative Beamforming

Next, in Fig. 6, we compared the secrecy outage probability of the proposed and max-ratio schemes, where the system

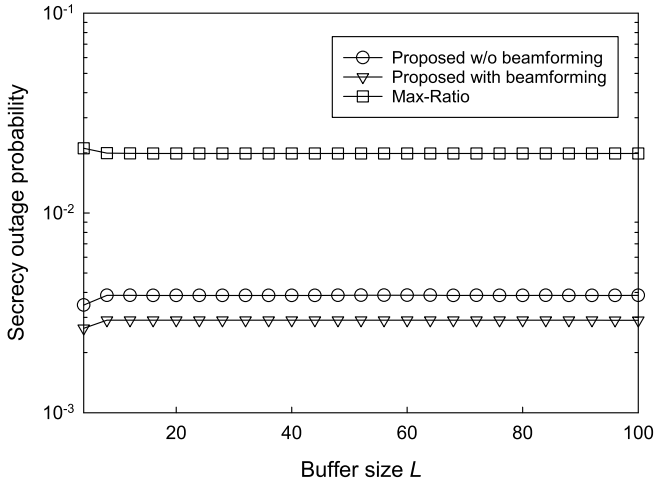


(a)

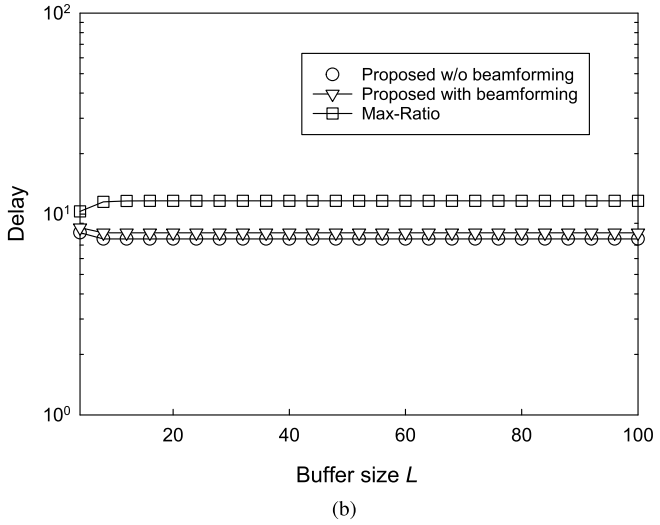


(b)

Fig. 8. Delay of the proposed and max-ratio schemes with parameters $L = 5$, SNR $\gamma_{SR} = \gamma_{RD} = 40$ dB, and secrecy rate r_{sc} varied from 0.1 to 3.0 bps/Hz. The number of relay nodes was (a) $K = 3$ or (b) $K = 5$.



(a)



(b)

Fig. 9. The effects of the buffer size L on the achievable performance of the proposed scheme and the conventional max-ratio scheme, where we considered $K = 5$ relay nodes; (a) secrecy outage probability and (b) delay.

parameters were $(K, L) = (3, 5)$ and the secrecy rate r_{sc} was varied from 0.1 to 3.0 bps/Hz. Fig. 6 shows that while the proposed scheme with cooperative beamforming exhibited a slightly better performance than that without cooperative beamforming, both proposed schemes clearly outperformed the max-ratio benchmark scheme over the entire secrecy rate regime.

In Fig. 7, we investigated the effects of the number of relay nodes K on the secrecy outage probability of the proposed and the max-ratio schemes. The number of relay nodes K was varied from 2 to 20, while the buffer size was maintained at $L = 5$. We considered SNR of $\gamma_{SR} = \gamma_{RD} = 40$ dB and a secrecy rate of $r_{sc} = 1$ bps/Hz. Observe in Fig. 7 that the proposed scheme with cooperative beamforming and parameter $\xi = 3$ exhibited the best performance. In addition, the performance advantage of the proposed schemes with and without cooperative beamforming increased with an increasing number of relay nodes K.

In Fig. 8, a comparison of the delay profile between the proposed and the max-ratio schemes is provided, where we considered a buffer size of $L = 5$, and the SNR was set to $\gamma_{SR} = \gamma_{RD} = 40$ dB while varying the secrecy rate r_{sc} from 0.1 to 3.0 bps/Hz. The number of relay nodes was $K = 3$ and $K = 5$ in Figs. 8(a) and 8(b), respectively. Observe in Fig. 8 that the delay of the proposed schemes was lower than that of the max-ratio scheme over the entire secrecy rate region and for each K value. In addition, as well as increasing the number of relay nodes, increasing the secrecy rate increased the performance advantage of the proposed schemes.

Furthermore, in Figs. 9(a) and 9(b), we investigated the effects of the buffer size L on the secrecy outage probability and the delay, respectively, where we considered $K = 5$ relay nodes. Observe in Figs. 9(a) and 9(b) that both the secrecy outage probability and the delay converged less than the buffer size of $L = 10$. This implies that in both the proposed scheme and the conventional max-ratio scheme, the buffer size does not have to be larger than $L = 10$.

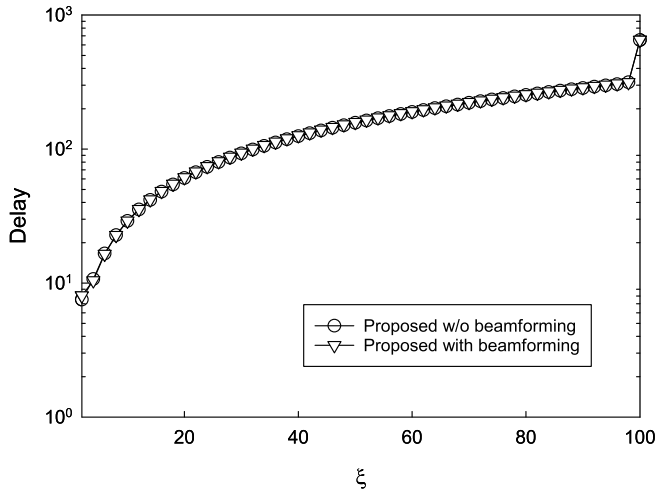


Fig. 10. Delay of the proposed schemes with/without cooperative beamforming, where we considered the $K = 5$ relay nodes, buffer size of $L = 100$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc} = 1$ bps/Hz.

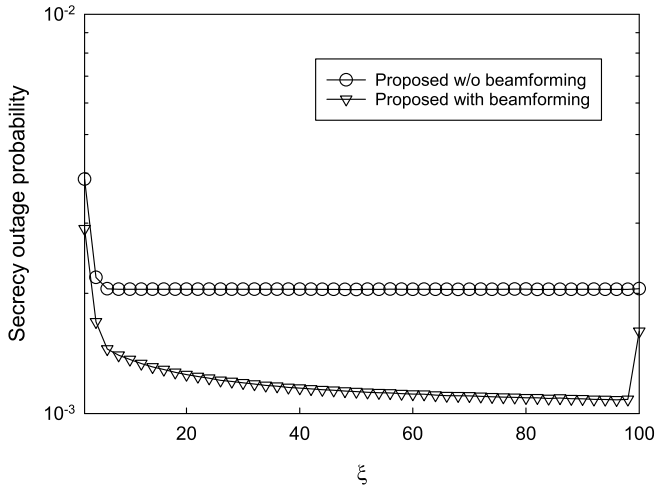


Fig. 11. Secrecy outage probability of the proposed schemes with/without cooperative beamforming, where we considered the $K = 5$ relay nodes, buffer size of $L = 100$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc} = 1$ bps/Hz.

Next, in Figs. 10 and 11 the effects of the thresholding parameter ξ on the proposed scheme's delay profile and secrecy outage probability were investigated, respectively, where we considered the $K = 5$ relay nodes, buffer size of $L = 100$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc} = 1$ bps/Hz. Observe in Fig. 10, upon decreasing the ξ value, the packet delay monotonically decreased, as expected from the analytical bound of (23). Since $\xi = 1$ is not supported in our protocol, $\xi = 2$ is optimal in terms of a packet delay profile. Furthermore, in Fig. 11 it was found that the secrecy outage probability remained almost unchanged for $\xi \geq 2$ in the proposed scheme without beamforming, while that of the proposed scheme with beamforming gradually improved, upon increasing ξ value. Since the effects of ξ on the secrecy outage probability is not significantly high, it may be preferable to set ξ (≥ 2) to be as low as possible, for the sake of attaining a low delay.

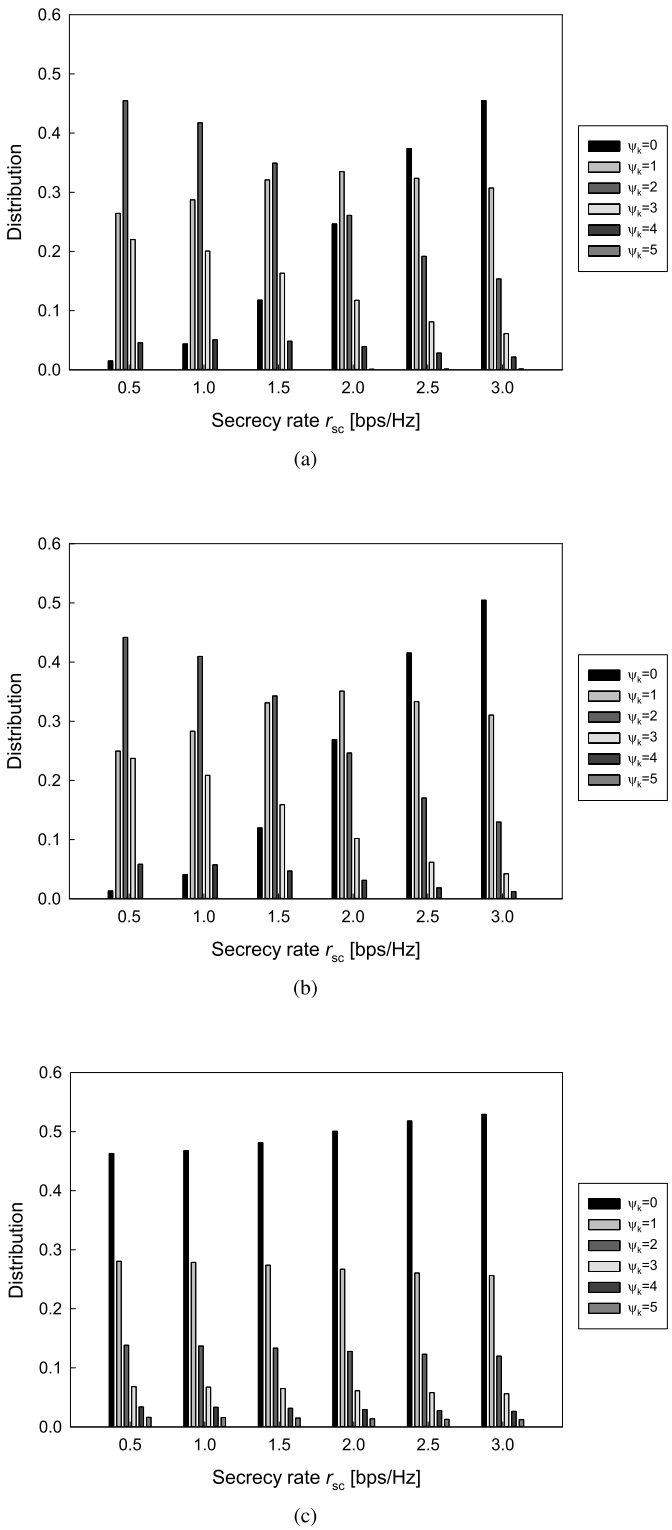


Fig. 12. Average distributions of buffer states at relay nodes with parameters $(K, L) = (5, 5)$, SNR $\gamma_{\rm SR} = \gamma_{\rm RD} = 40$ dB, and secrecy rate $r_{\rm sc}$ varied from 0.5 to 3.0 bps/Hz. (a) Proposed scheme without beamforming. (b) Proposed scheme with beamforming. (c) Max-ratio scheme.

Fig. 12 shows the average distributions of buffer states of relay nodes for the proposed and the max-ratio schemes. Note that we counted a packet shared among the relay nodes in the proposed schemes as one packet. Here, we considered

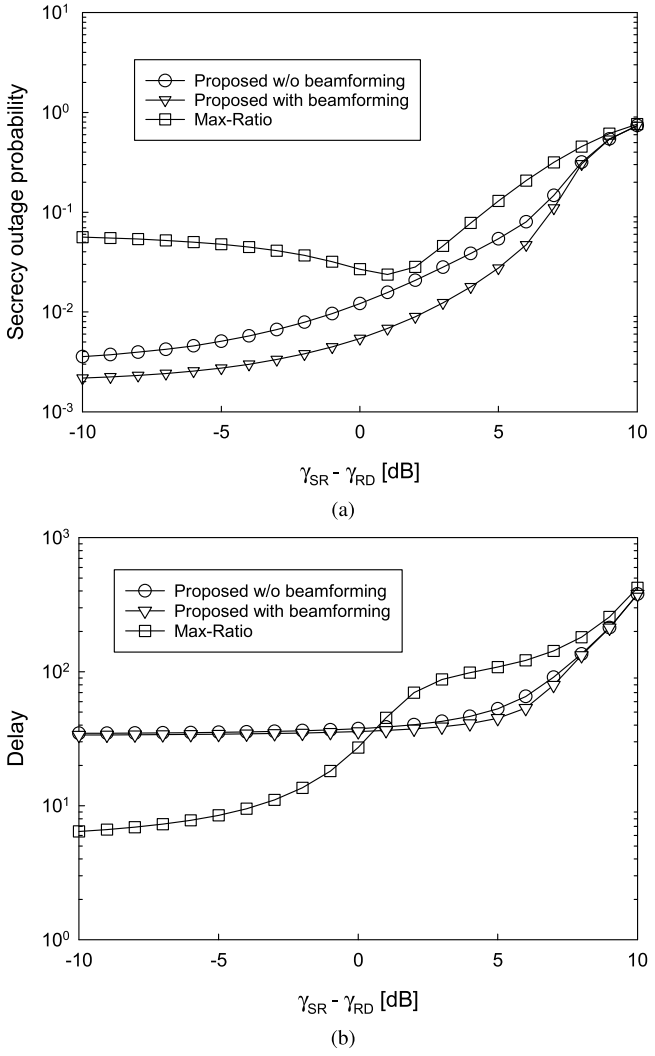


Fig. 13. The proposed schemes with and without cooperative beamforming, having the parameters of $(K, L) = (5, 10)$, while considering the asymmetric channels, having the average SNRs of $\gamma_{\mathrm{SR}} = 10$ dB and $\gamma_{\mathrm{RD}} = 0$–20 dB. The secrecy rate was given by $r_{\mathrm{sc}} = 1.0$ bps/Hz. (a) Secrecy outage probability and (b) delay.

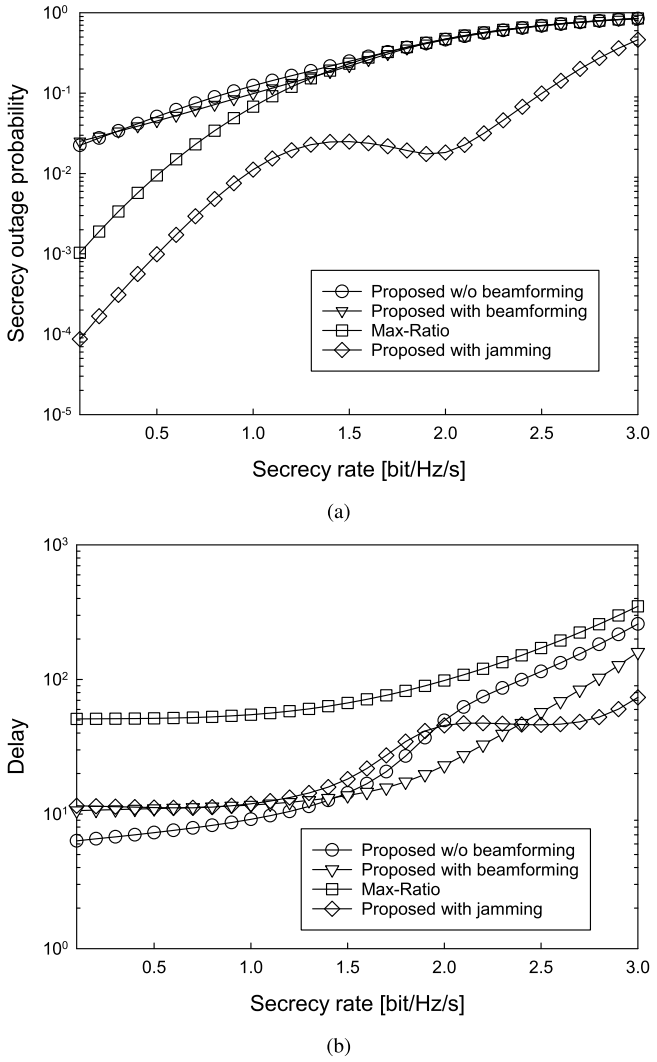


Fig. 14. The achievable performance of the proposed schemes with/without cooperative beamforming, the proposed scheme with cooperative jamming, and the conventional max-ratio scheme, while assuming that the average SNRs of the channels associated with an eavesdropper were available at a central coordinator. Also, we set the ratios of $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = \zeta_{\mathrm{DE}} = 5$ and the average SNR was given by $\gamma_{\mathrm{SR}} = \gamma_{\mathrm{RD}} = \gamma_{\mathrm{RR}} = 20$ dB. The secrecy rate was given by $r_{\mathrm{sc}} = 1.0$ bps/Hz. (a) Secrecy outage probability and (b) delay.

the system parameters of $(K, L) = (5, 5)$ and the SNR was set to $\gamma_{\mathrm{SR}} = \gamma_{\mathrm{RD}} = 40$ dB while varying the secrecy rate r_{sc} from =0.5 to 3.0 bps/Hz. Figs. 12(a), 12(b), and 12(c) show the packet distributions of the proposed schemes without and with cooperative beamforming and the max-ratio scheme, respectively. As the explicit benefits of the BSB algorithm of the proposed schemes, the ratio of the empty-buffer state ($\Psi_k = 0$) was lower in the proposed schemes than in the max-ratio scheme, especially in the low secrecy-rate region. This allows us to maintain the number of available links as high as possible, hence resulting in a better secrecy outage probability, as shown in the results shown in Figs. 6 and 7.

Moreover, in Fig. 13 we investigated the effects of the asymmetric channels on the achievable performance of the proposed scheme, where we considered the system parameters of $(K, L) = (5, 10)$ and the secrecy rate of $r_{\mathrm{sc}} = 1.0$. The SNR of the SR links was fixed to $\gamma_{\mathrm{SR}} = 10$ dB, and that of the RD links was varied from $\gamma_{\mathrm{RD}} = 0$ to 20 dB. Fig. 13(c) shows the secrecy outage probability, while Fig. 13(b) represents the delay. Observe in Fig. 13(a) that the proposed schemes with/without cooperative beamforming exhibited a better secrecy outage probability than the conventional max-ratio scheme in entire SNR regime. Furthermore, as shown in Fig. 13(b), the proposed schemes outperformed the max-ratio scheme in terms of the delay for the scenario of $\gamma_{\mathrm{SR}} \gg \gamma_{\mathrm{RD}}$, while the max-ratio exhibited a lower delay than the proposed schemes for $\gamma_{\mathrm{SR}} \ll \gamma_{\mathrm{RD}}$. This is because the conventional max-ratio scheme simply tended to select RD links, owing to $\gamma_{\mathrm{SR}} \ll \gamma_{\mathrm{RD}}$, which reduced the average number of packets stored in relay buffers. However, this condition deteriorated the secrecy outage performance of the max-ratio scheme, due to the increased empty-buffer states.

C. Numerical Results of the Proposed Scheme With Cooperative Beamforming and Jamming

Having investigated the achievable performance of the proposed scheme with and without cooperative beamforming,

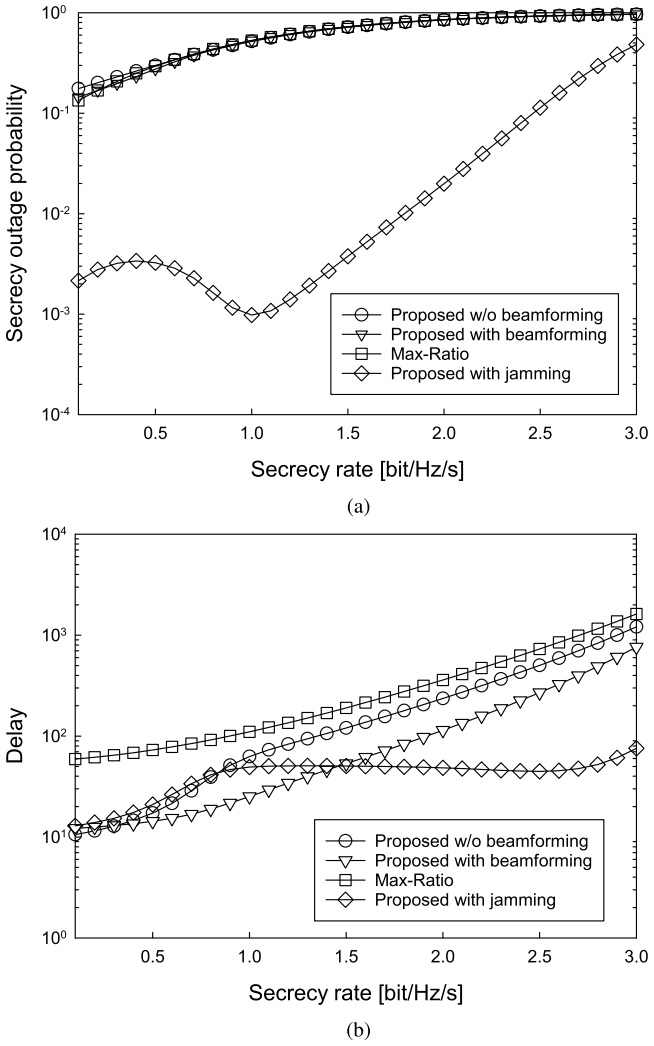


Fig. 15. The achievable performance of the proposed schemes with/without cooperative beamforming, the proposed scheme with cooperative jamming, and the conventional max-ratio scheme, while assuming that the average SNRs of the channels associated with an eavesdropper were available at a central coordinator. Also, we set the ratios of $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = \zeta_{\mathrm{DE}} = 1$ and the average SNR was given by $\gamma_{\mathrm{SR}} = \gamma_{\mathrm{RD}} = \gamma_{\mathrm{RR}} = 20$ dB. The secrecy rate was given by $r_{\mathrm{sc}} = 1.0$ bps/Hz. (a) Secrecy outage probability and (b) delay.

now we carried out the numerical study of the proposed scheme with both cooperative beamforming and jamming, which is presented in Section V. Here, the CSI associated with an eavesdropper is not assumed to be fully acquired at a central coordinator. More specifically, we assumed that only the related average SNRs, γ_{SE} and γ_{RE}, were available at a central coordinator. Furthermore, the system parameters were given by $(K, L) = (5, 10)$.

Figs. 14(a) and 14(b) compare the secrecy outage probability and the delay between the three proposed schemes and the conventional max-ratio scheme, where we set the ratios of $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = \zeta_{\mathrm{DE}} = 5$ and the average SNR was given by $\gamma_{\mathrm{SR}} = \gamma_{\mathrm{RD}} = \gamma_{\mathrm{RR}} = 20$ dB. Observe in Fig. 14(a) that the proposed scheme with cooperative jamming outperformed three other schemes in the entire range of the secrecy rate, since cooperative jamming successfully interferes with an eavesdropper's reception. By contrast, the secrecy outage probability of other schemes deteriorated by the challenging assumption of the absence of full CSI associated with an eavesdropper. Furthermore, as shown in Fig. 14(b), the proposed scheme with cooperative jamming exhibited a good delay profile, comparable to two other proposed schemes, while outperforming the conventional max-ratio scheme.

Moreover, in Figs. 15(a) and 15(b), the ratios ζ_{SR_k}, $\zeta_{\mathrm{R}_k\mathrm{D}}$, and ζ_{DE} were changed from $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = \zeta_{\mathrm{DE}} = 5$ to 1, while other system parameters were the same as those used in Figs. 14(a) and 14(b). As seen in the $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = 1$ scenario of Fig. 15(a), the performance advantages of the proposed scheme with cooperative jamming increased, in comparison to those shown in the $\zeta_{\mathrm{SR}_k} = \zeta_{\mathrm{R}_k\mathrm{D}} = \zeta_{\mathrm{DE}} = 5$ scenario of Fig. 14(a). Additionally, in Fig. 15(b), it was found that the proposed scheme with cooperative jamming exhibited explicit advantage over other schemes, especially for the security rate of $r_{\mathrm{sc}} \geq 2$ bps/Hz.

VII. Conclusions

In this paper, we proposed novel buffer-aided secure relaying schemes that rely on multiple SR- and RD-link selections. More specifically, simultaneous activation of multiple SR links owing to the broadcast nature of wireless channels is used and a source packet is shared among multiple nodes, which also enables coherent cooperative beamforming by the buffer-aided relay nodes. Furthermore, BSB relay selection is also incorporated into our schemes, in order to avoid the detrimental empty- and full-buffer states. We derived the analytical bounds of the secrecy outage probability and delay for the proposed schemes. Furthermore, we introduced the concept of cooperative jamming into the proposed scheme, in order to interfere with an eavesdropper's reception. Our simulation results demonstrated that the proposed schemes outperformed the existing benchmark scheme in terms of both the secrecy outage probability and the delay profile.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[5] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[6] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[7] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.

[9] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, "Buffering in a three-node relay network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[10] R. Wang, V. K. N. Lau, and H. Huang, "Opportunistic buffered decode-wait-and-forward (OBDWF) protocol for mobile wireless relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1224–1231, Apr. 2011.

[11] N. B. Mehta, V. Sharma, and G. Bansal, "Performance analysis of a cooperative system with rateless codes and buffered relays," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1069–1081, Apr. 2011.

[12] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, Mar. 2012.

[13] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

[14] C. Dong, L.-L. Yang, and L. Hanzo, "Performance analysis of multihop-diversity-aided multihop links," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2504–2516, Jul. 2012.

[15] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.

[16] H. Liu, P. Popovski, E. de Carvalho, and Y. Zhao, "Sum-rate optimization in a two-way relay network with buffering," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 95–98, Jan. 2013.

[17] T. Islam, A. Ikhlef, R. Schober, and V. K. Bhargava, "Diversity and delay analysis of buffer-aided BICM-OFDM relaying," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5506–5519, Nov. 2013.

[18] N. Zlatanov, A. Ikhlef, T. Islam, and R. Schober, "Buffer-aided cooperative communications: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 146–153, Apr. 2014.

[19] Z. Tian, G. Chen, Y. Gong, Z. Chen, and J. A. Chambers, "Buffer-aided max-link relay selection in amplify-and-forward cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 553–565, Feb. 2015.

[20] C. Dong, L.-L. Yang, and L. Hanzo, "Multi-hop diversity aided multi-hop communications: A cumulative distribution function aware approach," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4486–4499, Nov. 2013.

[21] C. Dong, L.-L. Yang, J. Zuo, S. X. Ng, and L. Hanzo, "Energy, delay, and outage analysis of a buffer-aided three-node network relying on opportunistic routing," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 667–682, Mar. 2015.

[22] S. Huang, J. Cai, and H. Zhang, "Relay selection for average throughput maximization in buffer-aided relay networks," in *Proc. IEEE Int. Conf. Commun.*, London, U.K., Jun. 2015, pp. 3597–3601.

[23] S. Luo and K. C. Teh, "Buffer state based relay selection for buffer-aided cooperative relaying systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5430–5439, Oct. 2015.

[24] C. Dong, L. Li, B. Zhang, L.-L. Yang, and L. Hanzo, "Energy dissipation versus delay tradeoffs in a buffer-aided two-hop link," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8060–8071, Oct. 2016.

[25] M. Oiwa, C. Tosa, and S. Sugiura, "Theoretical analysis of hybrid buffer-aided cooperative protocol based on max-max and max-link relay selections," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9236–9246, Nov. 2016.

[26] M. Oiwa and S. Sugiura, "Reduced-packet-delay generalized buffer-aided relaying protocol: Simultaneous activation of multiple source-to-relay links," *IEEE Access*, vol. 4, pp. 3632–3646, Jun. 2016.

[27] Z. Tian, Y. Gong, G. Chen, and J. A. Chambers, "Buffer-aided relay selection with reduced packet delay in cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2567–2575, Mar. 2017.

[28] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

[29] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: Performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1099–1109, Aug. 2004.

[30] S. Sugiura, S. Chen, H. Haas, P. M. Grant, and L. Hanzo, "Coherent versus non-coherent decode-and-forward relaying aided cooperative space-time shift keying," *IEEE Trans. Commun.*, vol. 59, no. 6, pp. 1707–1719, Jun. 2011.

[31] Q. Li, Q. Yan, K. C. Teh, K. H. Li, and Y. Hu, "A multi-relay-selection scheme with cyclic delay diversity," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 349–352, Feb. 2013.

[32] M. Oiwa, R. Nakai, and S. Sugiura, "Buffer-state-and-thresholding-based amplify-and-forward cooperative networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 674–677, Oct. 2017.

[33] M. Oiwa and S. Sugiura, "Generalized virtual full-duplex relaying protocol based on buffer-aided half-duplex relay nodes," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, May 2017, pp. 1–5.

[34] R. Nakai, M. Oiwa, K. Lee, and S. Sugiura, "Generalized buffer-state-based relay selection with collaborative beamforming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1245–1257, Feb. 2018.

[35] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[36] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[37] A. El Shafie, A. Sultan, and N. Al-Dhahir, "Physical-layer security of a buffer-aided full-duplex relaying system," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1856–1859, Sep. 2016.

[38] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[39] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

[40] H. David and H. Nagaraja, *Order Statistics* (Wiley Series in Probability and Statistics). Hoboken, NJ, USA: Wiley, 2004.

[41] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[42] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

Ryota Nakai (S'17) received the B.E. degree in computer and information sciences from the Tokyo University of Agriculture and Technology, Koganei, Japan, in 2017, where he is currently a postgraduate student. His research interests are in cooperative wireless communications and physical layer security. He received the IEEE VTS Tokyo Chapter 2017 Young Researcher's Encouragement Award.

Shinya Sugiura (M'06–SM'12) received the B.S. and M.S. degrees in aeronautics and astronautics from Kyoto University, Kyoto, Japan, in 2002 and 2004, respectively, and the Ph.D. degree in electronics and electrical engineering from the University of Southampton, Southampton, U.K., in 2010.

From 2004 to 2012, he was a Research Scientist with Toyota Central R&D Labs., Inc., Nagakute, Japan. Since 2013, he has been an Associate Professor with the Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Tokyo, Japan, where he heads the Wireless Communications Research Group. He authored or coauthored over 60 IEEE journal papers. His research has covered a range of areas in wireless communications, networking, signal processing, and antenna technology.

Dr. Sugiura was a recipient of a number of awards, including the Sixth RIEC Award from the Foundation for the Promotion of Electrical Communication in 2016, the Young Scientists' Prize by the Minister of Education, Culture, Sports, Science and Technology of Japan in 2016, the 14th Funai Information Technology Award (First Prize) from the Funai Foundation in 2015, the 28th Telecom System Technology Award from the Telecommunications Advancement Foundation in 2013, the Sixth IEEE Communications Society Asia-Pacific Outstanding Young Researcher Award in 2011, the 13th Ericsson Young Scientist Award in 2011, and the 2008 IEEE Antennas and Propagation Society Japan Chapter Young Engineer Award. He was also certified as an Exemplary Reviewer of IEEE COMMUNICATIONS LETTERS in 2013 and 2014, and IEEE TRANSACTIONS ON COMMUNICATIONS in 2018.