Physical Layer Security of Buffer-Aided Hybrid Virtual Full-Duplex and Half-Duplex Relay Selection

Gan Srirutchataboon and Shinya Sugiura*
Institute of Industrial Science, The University of Tokyo, Japan
Email: {gan, sugiura}@iis.u-tokyo.ac.jp

***Abstract*—In this paper, we propose a novel secure buffer-aided relay selection that is capable of operating both virtual full-duplex (VFD) and half-duplex (HD) transmissions in a hybrid manner. The proposed scheme consists of five modes: two unicast modes, a broadcast mode, cooperative beamforming, and a VFD mode. Since the VFD mode has the potential of achieving a higher secrecy capacity than the other four HD modes, the proposed relay selection algorithm gives the highest priority to activating the VFD mode. Our performance results demonstrate that the proposed secure relay selection scheme outperforms the benchmarks in terms of the secrecy outage probability.**

I. Introduction

Physical layer (PHY) security [1, 2] has been developed to best serve confidential information in wireless communication systems. The use of signal processing techniques, such as relay selection, cooperative beamforming, and jamming, allows us to achieve an increased secrecy capacity [3, 4]. The secure relay selection techniques were presented in [5–7], which decrease an outage probability by selecting a link having the highest channel capacity.

Buffer-aided relay selection [8–11] is an extended version of relay selection, which increases the design degree of freedom compared with conventional relaying scheme [12]. More recently, non-orthogonal multiple access (NOMA) and full-duplex (FD) are exploited in the context of buffer-aided relay selection [13–16]. In [17], secure buffer-aided relay selection was considered while assuming that an eavesdropper intercepts information from only a relay node. Also, the max-min ratio scheme was proposed for secure buffer-aided relay selection [18], where a single link having the maximum secrecy capacity is selected from all the source-to-relay (SR) and relay-to-destination (RD) links in each time slot under the assumption that an eavesdropper is capable of intercepting information from both source and relay nodes. In [6], Chen *et al.* proposed the max-ratio relay selection with the knowledge of transmitter-to-eavesdropper links, which outperforms the max-min ratio counterpart in terms of the secrecy outage performance. In [7], the secure buffer-state-based (BSB) max-ratio relay selection was proposed to avoid the empty buffer states and buffer overflow, and the concept of cooperative jamming was exploited to minimize the possibility of interception by the eavesdropper.

In full-duplex (FD) transmission [19], transmission and reception are carried out simultaneously with the aid of self-interference (SI) cancellation techniques, and it may provide a doubled secrecy rate compared to the conventional half-duplex (HD) transmission. FD transmission is utilized in PHY security [20] to degrade the signal-to-interference and noise ratio (SINR) at an eavesdropper, where the receiver receives source information while transmitting an artificial noise to the eavesdropper. In [21], a source and an FD relay simultaneously transmit artificial noises to the eavesdropper while sending and relaying information, respectively. However, the performance suffers from the strong SI.

In [22, 23], the concept of virtual full-duplex (VFD) transmission was introduced to overcome the limitation of SI. More specifically, in the VFD transmission, the transmission and reception of packets are carried out by different nodes simultaneously, i.e., a source node transmits a packet to a relay node, while another relay node transmits a packet to a destination node. Furthermore, in [24, 25], interference between transmitting and receiving relay nodes, referred to as inter-relay interference (IRI), is eliminated with the aid of multiple antennas equipped at the relay nodes. Most recently, in [11], the hybrid use of HD and VFD transmission in buffer-aided relay selection was proposed.

Motivated by [11], this paper proposes a secure buffer-aided relay selection based on the hybrid HD and VFD transmission. The proposed scheme supports five transmission modes, i.e., one VFD mode and four HD modes. The VFD mode is given priority to be activated over the other four modes since the VFD mode has the potential of achieving a higher secrecy rate and a higher interference to the eavesdropper.[1] Owing to the benefits of the broadcast mode, the multiple relay nodes have a chance to share an information packet in their buffers in a

Preprint (accepted version) for publication in *2022 IEEE 95th Vehicular Technology Conference (VTC2022-Spring)*. © 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. This work was supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI (Grant Number 17H03259) and in part by the Japan Science and Technology Agency (JST) Precursory Research for Embryonic Science and Technology (PRESTO) (Grant Number JPMJPR1933). Also, this work was partially conducted as the research commissioned by National Institute of Information and Communications Technology (NICT), JAPAN.

[1] Note that in [11], capacity, rather than secrecy capacity, is employed as a metric to activate one out of transmission modes, implying that the presence of eavesdroppers is not taken into account.

seamless manner. Thus, it is possible to resolve the influence of IRI with the aid of successive interference cancellation (SIC).

II. System Model

We consider a two-hop cooperative relay network that consists of one source node (Alice), one destination node (Bob), one eavesdropper (Eve), and K decode-and-forward (DF) relays nodes. Each node is equipped with a single antenna operated in HD transmission. The kth relay is denoted as R_k $(k \in \{1, \cdots, K\})$. We assume that Alice needs the assistance of a relay node to communicate with Bob due to the presence of an obstacle between Alice and Bob. Eve tries to intercept information transmitted from Alice to the relay nodes as well as that from the relay nodes and Bob. Additionally, each relay node has a data buffer of size L, and the number of packets stored at the kth relay node's buffer is denoted as ψ_k $(0 \leq \psi_k \leq L)$.

The channel coefficients of the ith SR link, the jth RD link, the relay-to-relay (RR) link between of the ith and jth relay nodes, the source-to-eavesdropper (SE) link, and the relay-to-eavesdropper (RE) link between the jth relay node and the eavesdropper denote h_{SR_i}, h_{RE_j}, $h_{\mathrm{RR}_{ji}}$, h_{SE_i}, h_{RE_j}, respectively. We assume each of the $2K+2$ links is modeled by an independent and identically distributed (IID) frequency-flat Rayleigh fading channel, and each channel coefficient is generated as a random variable, following complex-valued Gaussian distribution with a zero mean and unit variance. Similar to [11], Bob acts as a central coordinator to gather all channel state information (CSI) and buffer state information (BSI). More specifically, Alice periodically broadcasts a pilot signal to the K relay nodes, and each relay node acquires CSI based on the received pilot signal. Then, each relay node relays the estimated SR CSI, its BSI, and a pilot signal to Bob. Finally, in each time slot, Bob sends a control packet to each node to collect CSI and BSI, and decides the transmission mode based on the collected CSI and BSI. After Bob successfully receives the packet, Bob sends back an acknowledgment packet through a low-rate feedback channel to the relay nodes. Then, the associated relay nodes delete the packet from their buffer.

In the proposed scheme, we have five transmission modes, i.e., a unicast mode for SR transmission, the unicast mode for RD transmission, the broadcast mode for SR transmission, the cooperative beamforming mode for RD transmission, and the VFD mode. One out of the five transmission modes is activated based on CSI and BSI, which have to be successfully collected at the coordinator under the assumption of the use of powerful channel coding.

A. Unicast Mode for SR Transmission

In the unicast mode for SR transmission, Alice transmits an information packet to a single selected relay node. Here, the channel capacities of the ith SR link and the SE link are given, respectively, by

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

$$\mathcal{C}_{\mathrm{SE}} = \frac{1}{2}\log_2\left(1 + \gamma_{\mathrm{SE}}|h_{\mathrm{SE}}|^2\right). \tag{2}$$

The secrecy capacity of the ith SR link, where Eve is not able to intercept information, is given by [7]

$$\begin{aligned} \mathcal{C}^{\text{secure}}_{\mathrm{SR}_i} &= \mathcal{C}_{\mathrm{SR}_i} - \mathcal{C}_{\mathrm{SE}}, \\ &= \frac{1}{2}\log_2\left(\frac{1 + \gamma_{\mathrm{SR}}|h_{\mathrm{SR}_i}|^2}{1 + \gamma_{\mathrm{SE}}|h_{\mathrm{SE}}|^2}\right), \end{aligned} \tag{3}$$

and γ_{SR_i} and γ_{SE} are the average signal-to-noise ratio (SNR) of the ith SR link and the SE link, respectively. The unicast SR transmission from Alice to the ith relay node is successful, if the buffer of the ith relay node is not full and if we have $\mathcal{C}^{\text{secure}}_{\mathrm{SR}_i} > r_{\mathrm{sc}}$, where r_{sc} is a target secrecy rate.

B. Unicast Mode for RD Transmission

In the unicast mode for RD transmission, the jth relay node relays a packet stored in the buffer to Bob. The channel capacity of the jth RD link and the jth RE link are given, respectively, by

$$\mathcal{C}_{\mathrm{RD}_j} = \frac{1}{2}\log_2\left(1 + \gamma_{\mathrm{RD}_j}|h_{\mathrm{RD}_j}|^2\right), \tag{4}$$

$$\mathcal{C}_{\mathrm{RE}_j} = \frac{1}{2}\log_2\left(1 + \gamma_{\mathrm{RE}_j}|h_{\mathrm{RE}_j}|^2\right). \tag{5}$$

Similar to (3), the secrecy capacity of the jth RD link is formulated by

$$\begin{aligned} \mathcal{C}^{\text{secure}}_{\mathrm{RD}_j} &= \mathcal{C}_{\mathrm{RD}_j} - \mathcal{C}_{\mathrm{RE}_j}, \\ &= \frac{1}{2}\log_2\left(\frac{1 + \gamma_{\mathrm{RD}_j}|h_{\mathrm{RD}_j}|^2}{1 + \gamma_{\mathrm{RE}_j}|h_{\mathrm{RE}_j}|^2}\right), \end{aligned} \tag{6}$$

where γ_{RE_j} and γ_{RE_j} are the average SNRs of the jth RD link and the jth RE link, respectively. The secure unicast transmission of the jth RD link is successful, if the buffer of the jth relay node is not empty and if $\mathcal{C}^{\text{secure}}_{\mathrm{RD}_j} > r_{\mathrm{sc}}$.

C. Broadcast Mode for SR Transmission

In the broadcast mode for SR transmission, Alice broadcasts an information packet to multiple relay nodes. Hence, the SR links, which satisfy (3) and the buffers of the related relay nodes are not full, are activated. In this mode, an information packet can be shared among the relay nodes corresponding to the activated SR links, which allows us to perform single-antenna-based SIC in the VFD mode and cooperative beamforming. Let us define $\mathcal{I}$ as the subset of the SR links, which are activated in the broadcast mode. Note that if there is only a single activated SR link, i.e., $|\mathcal{I}| = 1$, this mode becomes equivalent to the unicast mode.

D. Cooperative Beamforming Mode for RD Transmission

In the cooperative beamforming mode for RD transmission, multiple relay nodes cooperatively transmit a common packet to Bob. Here, $\mathcal{J}$ denotes the subset of the RD links, which are available for cooperative beamforming, where the related relay nodes share a common packet in their buffers. Then, let us introduce the RD channel coefficients associated with cooperative beamforming as $\mathbf{g} = [g_1, \cdots, g_Q]^T \in \mathcal{J}$, where $|\mathcal{J}| = Q$. According to [7], each activated relay node's beamforming weight is given by the conjugate of the associated RD link, normalized by $\|\mathbf{g}\|$. Hence, the capacity of the cooperative beamforming mode is given by

$$\mathcal{C}_{\text{Beam}} = \frac{1}{2}\log_2(1 + \gamma_{\text{RD}} \|\mathbf{g}\|^2), \tag{7}$$

under the assumption that the average SNRs of all the RD links are identical as $\gamma_{\text{RD}_1} = \cdots = \gamma_{\text{RD}_K} = \gamma_{\text{RD}}$. Similarly, when considering the channel coefficients of the Q RE links, associated with those of the RD links $\mathbf{g}$, to be $\mathbf{g}' = [g'_1, \cdots, g'_Q]^T$, we arrive at the secrecy capacity of the cooperative beamforming mode as follows:

$$\mathcal{C}_{\text{Beam}}^{\text{secure}} = \frac{1}{2}\log_2\left(\frac{1 + \gamma_{\text{RD}} \|\mathbf{g}\|^2}{1 + \gamma_{\text{RE}}(|\mathbf{g}^H\mathbf{g}'|/\|\mathbf{g}\|)^2}\right) \tag{8}$$

where we assume the identical average SNR of RE links, i.e., $\gamma_{\text{RE}_1} = \cdots = \gamma_{\text{RE}_K} = \gamma_{\text{RE}}$. Finally, if the secrecy capacity (8) is higher than the target secrecy rate, i.e., $\mathcal{C}_{\text{Beam}}^{\text{secure}} > r_{\text{sc}}$, the transmission is successful.

E. VFD Mode for SR and RD Transmission

In the VFD mode for SR and RD transmission, Alice transmits an information packet to a single receiving relay node, while a single activated transmitting relay node relays a packet to Bob. We assume the ith relay node is the receiving relay node, and the jth relay node is the transmitting relay node. Here, the received signals at the ith relay node, Bob, and Eve are given, respectively, by

$$y_{\mathcal{R}_i} = h_{\text{SR}_i} x_{\mathcal{A}} + h_{\text{RR}_{ji}} x_j + n_i \tag{9}$$

$$y_{\mathcal{B}} = h_{\text{RD}_j} x_j + n_{\mathcal{B}}, \tag{10}$$

$$y_{\mathcal{E}} = h_{\text{SE}} x_{\mathcal{A}} + h_{\text{RE}_j} x_j + n_{\mathcal{E}} \tag{11}$$

where $x_{\mathcal{A}}$ and x_j are the packet transmitted from Alice and that from the jth relay node, respectively. The associated complex-valued Additive white Gaussian noises (AWGNs) at the ith relay node, Bob, and Eve are represented by n_i, $n_{\mathcal{B}}$ and $n_{\mathcal{E}}$, respectively.

In our VFD mode, the receiving and the transmitting relay nodes are selected under the assumption that both the relay nodes share a common packet in their buffers. Thus, the receiving relay node can calculate $h_{\text{RR}_{ji}} x_j$ in (9) to eliminate IRI via using SIC as follows:

$$\begin{aligned} \bar{y}_{\mathcal{R}_i} &= y_{\mathcal{R}_i} - h_{\text{RR}_{ji}} x_j & (12)\\ &= h_{\text{SR}_i} x_{\mathcal{A}} + n_i. & (13) \end{aligned}$$

Here, we assume that the receiving relay node has the knowledge of the RR channel of $h_{\text{RR}_{ji}}$ by overhearing the pilot signal transmitted from the transmitting relay node to the central coordinator (Bob).[2] Hence, the capacity of the receiving relay node and that of Bob are represented by (1) and (4), respectively.

Furthermore, since each mode of our protocol is designed to be information-theoretically secure, Eve does not have any chance to intercept a packet x_j stored in the jth relay node's buffer. In the VFD mode, the Eve's capacity for the SE link and that for the RE link between the jth relay node and Eve are formulated, respectively, by

$$\mathcal{C}_{\text{VFD,SE}} = \frac{1}{2}\log_2\left(1 + \frac{\gamma_{\text{SE}}|h_{\text{SE}}|^2}{1 + \gamma_{\text{RE}_j}|h_{\text{RE}_j}|^2}\right) \tag{14}$$

$$\mathcal{C}_{\text{VFD,RE}_j} = \frac{1}{2}\log_2\left(1 + \frac{\gamma_{\text{RE}_j}|h_{\text{RE}_j}|^2}{1 + \gamma_{\text{SE}}|h_{\text{SE}}|^2}\right). \tag{15}$$

Hence, our VFD mode has the benefits of imposing increased interference on signals received at Eve. From (1) and (14), the secrecy capacity of the link between Alice and the receiving relay node in the VFD mode is given by

$$\mathcal{C}_{\text{VFD,SR}_i}^{\text{secure}} = \frac{1}{2}\log_2\left(\frac{1 + \gamma_{\text{SR}_i}|h_{\text{SR}_i}|^2}{1 + \frac{\gamma_{\text{SE}}|h_{\text{SE}}|^2}{1+\gamma_{\text{RE}_j}|h_{\text{RE}_j}|^2}}\right). \tag{16}$$

Similarly, from (4) and (15), the secrecy capacity of the link between the transmitting relay node and Bob in the VFD mode is expressed by

$$\mathcal{C}_{\text{VFD,RD}_j}^{\text{secure}} = \frac{1}{2}\log_2\left(\frac{1 + \gamma_{\text{RD}_j}|h_{\text{RD}_j}|^2}{1 + \frac{\gamma_{\text{RE}_j}|h_{\text{RE}_j}|^2}{1+\gamma_{\text{SE}}|h_{\text{SE}}|^2}}\right). \tag{17}$$

Finally, our VFD mode is successful if the following relationship is satisfied:

$$\min\{\mathcal{C}_{\text{VFD,SR}_i}^{\text{secure}}, \mathcal{C}_{\text{VFD,RD}_j}^{\text{secure}}\} > r_{\text{sc}}. \tag{18}$$

Since the VFD mode is capable of achieving a doubled transmission rate compared to the HD modes, the VFD mode is given the highest priority to be activated in our selection algorithm.

Note that the average power consumption in each SR or RD transmission of our scheme is maintained constant, which is the same as that of the conventional relaying schemes that dispense with buffering or beamforming.

III. Proposed Selection Algorithm

As mentioned above, the VFD mode is put the highest priority among the five modes since the VFD mode achieves the doubled transmission rate. The three conditions that have to be satisfied in our VFD mode are summarized as follows:

(A1) The receiving relay node and the transmitting relay node have to be different. This corresponds to the VFD con-

[2] In the proposed scheme, a packet used in SIC, i.e., x_j of (12), is successfully shared among the relay nodes through the broadcast and full-duplex modes, hence free from any error propagation, while SIC in conventional MIMO and NOMA systems typically suffer from the detrimental effects of such error propagation due to mis-demodulation of x_j. Furthermore, the potential channel estimation errors of the RR channel may induce a residual SIC error in (12). However, even when the SNR of the RR channel is low, the associated effects may not be high owing to low IRI.

cept [11, 22, 23] that there is one relay node to receive a packet while another relay node transmits another packet simultaneously.

(A2) The receiving relay node and the transmitting relay node have to share a packet in their buffers. Owing to this, our single-antenna-based SIC of (12) becomes realistic.

(A3) Both the secure transmissions from Alice and the transmitting relay have to be successful, i.e., the inequality of (18) has to be satisfied.

Here, let us denote $\mathcal{L}$ as the set of relay pairs (i, j) that satisfy (A1)–(A3).

A. Case of $\mathcal{L} \neq \varnothing$

In this case, the VFD mode is activated. Among all the relay pairs in $\mathcal{L}$, the relay node that stores the highest number of packets in its buffer is selected as the transmitting relay node. If multiple candidates of the transmitting relay node exist, the relay node that achieves a higher secrecy capacity $\mathcal{C}^{\text{secure}}_{\text{VFD},\text{RD}_j}$ of (17) is selected as the transmitting relay node. Let us denote the index of the selected transmitting relay node as $\hat{j}$.

Then, the index $\hat{i}$ of the receiving relay node is selected from the subset $(\hat{i}, \hat{j}) \in \mathcal{L}$, such that the secrecy capacity of the VFD mode is maximized.

B. Case of $\mathcal{L} = \varnothing$

If there is no relay pair to activate the VFD mode, i.e., $\mathcal{L} = \varnothing$, one out of the four HD modes is activated based on CSI and BSI. Here, we introduce a parameter ω, which is used for characterizing our algorithm to select one out of the four HD modes, where $0 \leq \omega \leq L$. For example, when ω is high, i.e., $\omega > 0.5L$, the average packet delay tends to be low at the cost of the increased secrecy outage probability. More specifically, to avoid the detrimental of the buffer overflow and empty buffer state, we classify our algorithm based on BSI and ω into three as follows.

1) $\max\limits_{\forall i \in \mathcal{I}}\{L - \psi_i\} > \max\limits_{\forall j \in \mathcal{J}}\{\omega + \psi_j\}$*:* In this case, either the unicast mode for SR transmission or the broadcast modes is activated. More specifically, the broadcast mode is activated if multiple SR links are available. Otherwise, the unicast mode is activated for SR transmission.

2) $\max\limits_{\forall j \in \mathcal{J}}\{\omega + \psi_j\} \geq \max\limits_{\forall i \in \mathcal{I}}\{L - \psi_i\}$*:* In this case, either the unicast mode for RD transmission or the cooperative beamforming mode is activated. If multiple RD links are available in an outage and their buffers contain a common packet, the cooperative beamforming mode is activated. Otherwise, a single strongest RD link is selected, which corresponds to the unicast mode for RD transmission.

3) $\mathcal{I} = \mathcal{J} = \varnothing$*:* In this case, there is neither available SR nor RD link, and hence the transmission is counted as an outage event.

IV. Performance Results

In this section, the achievable performance of the proposed scheme is compared with those of the existing benchmark schemes, i.e., the BSB max-ratio scheme [7] and the conventional max-ratio scheme [6]. Let us introduce the SNRs of $\xi_{\text{SR}} = \gamma_{\text{SR}}/\gamma_{\text{SE}}$, and $\xi_{\text{RD}} = \gamma_{\text{RD}}/\gamma_{\text{RE}}$. Additionally, the initial buffer state is set to empty one in each Monte Carlo simulation. Also, we assumed the symmetric channel scenario of $\gamma_{\text{SR}} = \gamma_{\text{RD}} = 40$ dB, and the ratios of $\xi_{\text{SR}} = \xi_{\text{RD}} = 5$.[3]

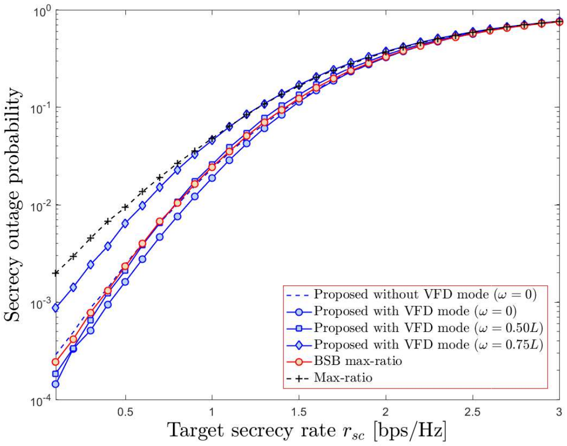
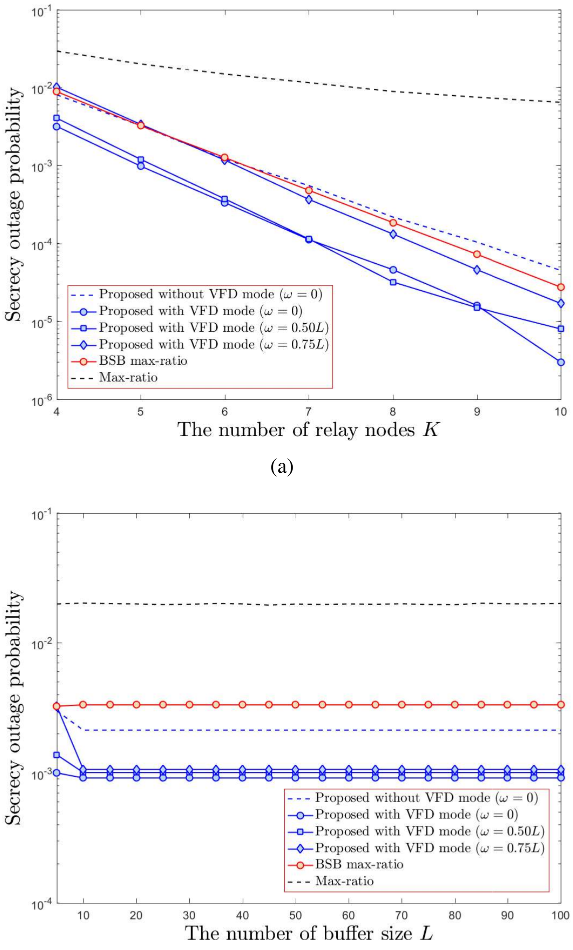


Fig. 1. Secrecy outage probabilities of the proposed scheme with and without the VFD mode, the conventional max-ratio, and the BSB max-ratio scheme, where we considered the system parameters of $(K, L) = (3, 5)$, and the target secrecy rate was varied from $r_{\text{sc}} = 0.1$ to 3.0 bps/Hz.

First, we investigated the effects of ω on the performance of the proposed scheme, where we considered $\omega = 0, 0.50L, 0.75L$. Fig. 1 compares the secrecy outage probabilities of the proposed scheme with and without the VFD mode, where the target secrecy rate was varied from $r_{\text{sc}} = 0.1$ to 3.0 bps/Hz. As seen in Fig. 1, the proposed scheme with the VFD mode ($\omega = 0$) achieved the lowest secrecy outage probability, which is achieved at the cost of a higher delay, as shown later. Upon increasing ω in the proposed scheme with the VFD mode, the secrecy outage probability monotonically increased.

Furthermore, in Figs. 2(a) and 2(b), we investigated the effects of the number of the relay nodes K and the buffer size L on the secrecy outage probabilities, respectively. In Fig. 2(a), the number of buffer size was fixed to $L = 5$ while the number of relay nodes was varied from $K = 4$ to 10. As seen in Fig. 2(a), the proposed scheme with the VFD mode ($\omega = 0$) achieved the lowest secrecy outage probability for most of K values, which was followed by the proposed scheme with the VFD mode ($\omega = 50L$). Also, the proposed scheme with the VFD mode ($\omega = 0.75L$) exhibited a lower secrecy outage probability than the conventional max-ratio scheme. In Fig. 2(b), the number of relay nodes was given by $K = 5$ while the buffer size was varied from $L = 5$ to 100. From Fig. 2(b), it was found that the proposed scheme with the VFD mode ($\omega = 0$) exhibited the best performance in the entire L range.

[3] In this paper, we considered the high SNR (i.e., $\gamma_{\text{SR}} = \gamma_{\text{RD}} = 40$ dB) scenarios to confirm the ideal achievable performance limit. The investigations of further realistic scenarios, such as the low SNRs or the asymmetric channels, are left for future studies.



(b)

Fig. 2. Secrecy outage probabilities of the proposed scheme with and without the VFD mode, the conventional max-ratio, and the BSB max-ratio scheme for the target secrecy rate of $r_{\text{sc}} = 1.0$ bps/Hz; (a) $L = 5$ and (b) $K = 5$.

V. Conclusions

In this paper, we proposed the novel secure buffer-aided relay selection scheme with the aid of hybrid HD and VFD transmissions. The presence of our VFD mode contributes to imposing interference on Eve, hence increasing secrecy capacity. Our simulation results demonstrated that the proposed scheme exhibited a better secrecy outage probability compared to the benchmark schemes.

References

[1] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[2] S. Sugiura, "Secrecy performance of eigendecomposition-based FTN signaling and NOFDM in quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5872–5882, Sep. 2021.

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

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

[5] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, 2009.

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

[7] R. Nakai and S. Sugiura, "Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 431–444, 2019.

[8] C. Dong, 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 Transactions on Communications*, vol. 63, no. 3, pp. 667–682, 2015.

[9] 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, 2016.

[10] R. Nakai, M. Oiwa, K. Lee, and S. Sugiura, "Generalized buffer-state-based relay selection with collaborative beamforming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1245–1257, 2018.

[11] G. Srirutchataboon, J. Kochi, and S. Sugiura, "Performance analysis of hybrid buffer-aided cooperative protocol based on half-duplex and virtual full-duplex relay selections," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1862–1873, 2021.

[12] 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 Transactions on Communications*, vol. 59, no. 6, pp. 1707–1719, Jun. 2011.

[13] J. Kochi, R. Nakai, and S. Sugiura, "Performance evaluation of generalized buffer-state-based relay selection in NOMA-aided downlink," *IEEE Access*, vol. 7, pp. 173 320–173 328, Dec. 2019.

[14] N. Nomikos, T. Charalambous, D. Vouyioukas, R. Wichman, and G. K. Karagiannidis, "Integrating broadcasting and NOMA in full-duplex buffer-aided opportunistic relay networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9157–9162, Jun. 2020.

[15] J. Kochi, R. Nakai, and S. Sugiura, "Hybrid NOMA/OMA broadcasting-and-buffer-state-based relay selection," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1618–1631, Feb. 2021.

[16] N. Nomikos, T. Charalambous, D. Vouyioukas, and G. K. Karagiannidis, "When buffer-aided relaying meets full duplex and NOMA," *IEEE Wireless Communications*, vol. 28, no. 1, pp. 68–73, 2021.

[17] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET communications*, vol. 4, no. 15, pp. 1787–1791, 2010.

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

[19] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, 2014.

[20] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

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

[22] A. Ikhlef, J. Kim, and R. Schober, "Mimicking full-duplex relaying using half-duplex relays with buffers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 7, pp. 3025–3037, 2012.

[23] M. Oiwa and S. Sugiura, "Generalized virtual full-duplex relaying protocol based on buffer-aided half-duplex relay nodes," in *IEEE Global Communications Conference*, Dec. 2017, pp. 1–6.

[24] S. M. Kim and M. Bengtsson, "Virtual full-duplex buffer-aided relaying in the presence of inter-relay interference," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2966–2980, 2016.

[25] T. Mishina, M. Oiwa, R. Nakai, and S. Sugiura, "Buffer-aided virtual full-duplex cooperative networks exploiting source-to-relay broadcast channels," in *IEEE Vehicular Technology Conference*, Nov. 2019, pp. 1–5.