Abstract—This letter proposes a novel hybrid half-/full-duplex relaying scheme to enhance the relay channel security. A source node (Alice) communicates with her destination node (Bob) in the presence of a buffer-aided full-duplex relay node (Rooney) and a potential eavesdropper (Eve). Rooney adopts two different relaying, namely randomize-and-forward and decode-and-forward relaying strategies, to improve the security of the legitimate system. In the first relaying strategy, Rooney uses a codebook different from that used at Alice. In the second relaying strategy, Rooney and Alice use the same codebooks. In addition, Rooney switches between half-duplex and full-duplex modes to further enhance the security of the legitimate system. The numerical results demonstrate that our proposed scheme achieves a significant average secrecy end-to-end throughput improvement relative to the conventional bufferless full-duplex relaying scheme.

Index Terms—Buffer, full-duplex, relay, security.

I. INTRODUCTION

The use of buffers to enhance secrecy rates has been investigated recently in, e.g., [1], [2]. In [1], Huang and Swindlehurst investigated the physical (PHY) layer security of a buffer-aided half-duplex (HD) relay channel. The authors proposed an adaptive link selection scheme for time slot assignments between the source and relay nodes. However, the proposed scheme is suboptimal in the sense that it ignores the impact of the buffer state information at the relay node. Reference [1] assumed that there is no direct link between the source node and both the legitimate destination node and the potential eavesdropping node. Unlike [1], we consider a buffer-aided full-duplex (FD) relay with finite buffer. In [2], the authors proposed two secure cooperative schemes for a wireless relay channel with buffered relay and source nodes. In contrast to [2], we assume an FD relay node with a reliable power supply.

Recently, the authors of [3] investigated the PHY-layer security of a single-input single-output antenna eavesdropper (SISOSE) wiretap channel with bufferless FD single-antenna relay node. Similar to [1], Reference [3] assumed that there is no direct link between the source node and its destination. In [4], the authors proposed three relay selection schemes for FD heterogeneous networks in the presence of multiple cognitive radio eavesdroppers. The relay selection schemes are based on the availability of the network’s channel state information (CSI) at the secondary information source.

The contributions of this letter are summarized as follows:

- We propose a novel hybrid HD/FD relaying scheme and two decoding strategies at the relay node to enhance the security of the legitimate system. Our proposed scheme exploits the exact buffer state information at the relay node and the secrecy rates of all links.
- We derive the system secrecy rate and average end-to-end secure throughput. Moreover, we convert the throughput-maximization problem into a standard linear program.

Notation: \( I_B \) denotes the identity matrix whose size is \( B \times B \). \( C^{M \times N} \) denotes the set of all complex matrices of size \( M \times N \) and \( \mathbb{C} \) denotes the set of all complex numbers. \((\cdot)^*\) denotes Hermitian operation.

II. MAIN ASSUMPTIONS

We consider a wireless network composed of one source node (Alice), one eavesdropping node (Eve), one FD relay node (Rooney), and one destination node (Bob). All nodes are equipped with a single antenna [3]. Alice is always backlogged with data packets to transmit. We assume that the distance between Alice and Bob is large enough due to shadowing and large distances such that the direct link between them is completely disconnected as in, e.g., [1], [3], Eve eavesdrops both Alice’s and Rooney’s transmissions. Time is slotted into discrete equal-size time slots. The duration of a time slot is \( T \) seconds and the channel bandwidth is \( W \) Hz.

We assume fixed secrecy-rate transmissions since in real systems the data is packetized and arrives in packets from the upper layers. Therefore, in a given time slot, the legitimate transmitting nodes transmit fixed-length packets of size \( b_s \) bits over one time slot duration. Since the transmission time is \( T \) seconds and the bandwidth is \( W \) Hz, the transmission secrecy rate is \( R_s = \frac{b_s}{WT} \) bits/sec/Hz.

A. Relay’s Model

Rooney has an FD capability and is equipped with a finite data buffer to store Alice’s data. The buffer can store up to \( Q_R \) packets. The number of packets in the buffer is \( Q_R, 0 \leq Q_R \leq Q \). If Rooney transmits data from his buffer, he employs a randomize-and-forward (RF) relaying strategy where he uses a codebook different from that used by Alice. The advantage of this relaying strategy is that Eve cannot combine the data transmitted by Alice and Rooney. Thus, the achievable secrecy rate is enhanced [5]. If Rooney’s buffer is empty, while it is still feasible to operate in the FD mode, Alice and Rooney transmit the data cooperatively using a secrecy rate that is based on the minimum of the two-hop transmission rates. The transmitted packet is delivered to Bob directly without being stored in Rooney’s buffer.

In summary, we have three main transmission schemes: 1) RF-FD where the FD capability is utilized in the RF mode; 2)
DF-FD where the FD capability is utilized in the DF mode; and 3) HD mode where either Alice or Rooney transmits when FD transmissions are insecure.

B. Channel Model

Each link experiences block flat-fading where a channel coefficient remains unchanged during one time slot duration and changes independently from one time slot to another. We denote the channel coefficient between Node \( n_1 \) and Node \( n_2 \) in time slot \( t \) by \( h_{n_1n_2}(t) \), where \( n_1, n_2 \in \{ A, B, E, R \} \) denote Alice, Bob, Eve, and Rooney, respectively. The complex random variable \( h_{n_1n_2}(t) \) is independent and identically distributed (i.i.d.) from one time slot to another with zero mean and variance \( \sigma_{n_1n_2}^2 \). Each link is also corrupted by an additive white Gaussian noise (AWGN) process with zero mean and variance \( \kappa_m \) Watts/Hz. In a given time slot, all nodes are assumed to have complete and perfect CSI [3]. This is reasonable when all nodes are active (non-hostile). The CSI is obtained through channel estimation and feedback. It is assumed that the average transmit power at Node \( n_1 \) is \( P_{n_1} \) Watts [1].

C. Received Signal-to-Interference-Plus-Noise Ratios

In this subsection, we analyze the received signal-to-interference-plus-noise ratios (SINRs) at all nodes.

1) FD mode: The received SINR at Rooney is given by

\[
\gamma_{R,FD}(t) = \frac{|h_{AR}(t)|^2 P_A}{|h_{RR}(t)|^2 P_R + \kappa R W}
\]

where \( |h_{RR}(t)| \in \mathbb{C} \) is the residual self-interference at Rooney after interference cancelation. The term \( |h_{RR}(t)|^2 P_R \) in the denominator of (1) represents the self-interference power. Thus, the received SINR at Rooney is degraded due to self-interference caused by the FD operation, which, in turn, decreases the secrecy rate of the Alice-Rooney link. This demonstrates the benefit of HD modes when the self-interference power is high. The received SINR at Bob is given by

\[
\gamma_{RB}(t) = \frac{|h_{RB}(t)|^2 P_R}{\kappa B W}
\]

In the RF-FD mode, the data signal transmitted by Alice, \( x_A(t) \), and the data signal transmitted by Rooney, \( x_R(t) \), are two independent signals. In the DF-FD mode, we assume \( x_R(t) = x_A(t-1) \).\(^1\) The latter case resembles an inter-symbol interference (ISI) channel.

2) HD mode: If Rooney operates in the HD mode, \( x_R(t) = 0 \). Assuming Alice only transmits, the SINR at Rooney is given by

\[
\gamma_{AR,HD}(t) = \frac{|h_{AR}(t)|^2 P_A}{\kappa R W}
\]

In addition, the received SINR at Eve is thus

\[
\gamma_{AE,HD}(t) = \frac{|h_{AE}(t)|^2 P_A}{\kappa E W}
\]

If Rooney only transmits, the SINR at both Bob and Eve are

\[
\gamma_{RB,HD}(t) = \frac{|h_{RB}(t)|^2 P_R}{\kappa B W}, \gamma_{RE,HD}(t) = \frac{|h_{RE}(t)|^2 P_R}{\kappa E W}
\]\n
\(^1\)The data processing delay is assumed to be one data symbol.

III. SECRECY RATES

In this section, we investigate the nodes’ achievable data rates (without secrecy constraints) and the legitimate links secrecy rates. The achievable rate at Rooney is

\[
\mathcal{R}_{AR,M}(t) = \log_2 (1 + \gamma_{R,M}(t))
\]

where \( M \in \{ HD, FD \} \) denotes the duplex mode at Rooney. On the other hand, the achievable rate at Bob is

\[
\mathcal{R}_{RB}(t) = \log_2 (1 + \gamma_B(t))
\]

Hereinafter, we omit the time index from the rate expressions.

A. FD Mode

In the RF-FD relay mode, the signals received by Eve from Alice and Rooney are independent. The secrecy rate region is obtained as follows

1) If Eve assumes Rooney’s transmission as noise and only decodes Alice’s transmission, the SINR and the achievable rate at Eve are given, respectively, by

\[
\gamma_{AE,FD} = \frac{|h_{AE}(t)|^2 P_A}{|h_{RE}(t)|^2 P_R + \kappa E W}, \quad \mathcal{R}_{AE} = \log_2 (1 + \gamma_{AE,FD})
\]

Hence, the secrecy rate of Alice is upper-bounded as

\[
\mathcal{R}_{sec,FD}^A \leq \left[ \mathcal{R}_{AR,FD} - \mathcal{R}_{AE} \right]^+
\]

where \([x]^+ = \max(x, 0)\).

2) If Eve assumes Alice’s transmission as noise and only decodes Rooney’s transmission, the SINR and achievable rate at Eve are given, respectively, by

\[
\gamma_{RE,FD} = \frac{|h_{RE}(t)|^2 P_R}{|h_{AE}(t)|^2 P_A + \kappa E W}, \quad \mathcal{R}_{RE} = \log_2 (1 + \gamma_{RE,FD})
\]

Hence, the secrecy rate of Rooney is upper-bounded as

\[
\mathcal{R}_{sec,FD}^R \leq \left[ \mathcal{R}_{RB} - \mathcal{R}_{RE} \right]^+
\]

3) If Eve employs a joint-typicality receiver, she can decode a sum rate

\[
\mathcal{R}_{E,sum} = \log_2 \left( 1 + \frac{|h_{AE}|^2 P_A + |h_{RE}|^2 P_R}{\kappa E W} \right)
\]

Hence, the sum secrecy rate is upper-bounded as [6]

\[
\mathcal{R}_{sec,FD}^A + \mathcal{R}_{sec,FD}^R \leq \left[ \mathcal{R}_{AR,FD} + \mathcal{R}_{RB} - \mathcal{R}_{E,sum} \right]^+
\]

The rate pair \((\mathcal{R}_{sec,FD}^A, \mathcal{R}_{sec,FD}^R)\) should satisfy the conditions in (9), (11), and (13).

In the DF-FD case, and assuming one symbol duration delay, the end-to-end rate of the system is given by [3]

\[
\mathcal{R}_{AB} = \min\{\mathcal{R}_{AR,FD}, \mathcal{R}_{RB}\}
\]

In addition, Eve’s rate is given by [3]

\[
\mathcal{R}_E = \frac{1}{B} \log_2 \det \left( I_B + \frac{1}{\kappa E W} H^* H \right)
\]

where \( B = [W T] \) is the codeword length and \( H \in \mathbb{C}^{(B+1) \times B} \) is a Toeplitz matrix whose first column is \( [h_{AE}^*, h_{RE}^*, 0, \ldots, 0]^* \). The system secrecy rate is given by

\[
\mathcal{R}_{AB}^s = [\mathcal{R}_{AB} - \mathcal{R}_E]^+
\]
In our proposed scheme, we give priority to the RF-  

transmits or Rooney only transmits. Depending on the values  

Rooney operates in the RF-HD mode and either Alice only  

will not be stored at Rooney’s queue and, hence, Rooney’s  

codebooks are used; 2) Alice and Rooney transmit the data  

S

1

, the DF-FD mode is used.  

Remark: In our proposed scheme, we give priority to the RF-  

enhanced secrecy rate. The RF-FD mode cannot be used when  

Q

R

= 0. However, we can still make use of the FD capability  

via the DF-FD mode. When FD transmissions are infeasible  

due to secrecy constraints, we resort to the HD mode.  

B. Rooney’s Buffer  

From the described scheme in Section IV-A, Rooney: 1)  

neither receives nor transmits data packets, 2) receives one  

packet, 3) transmits one packet, or 4) receives one packet  

and transmits one packet in the same time slot. Hence, the  

Markov chain of Rooney’s queue can be modeled as a birth-  

death process. When the queue is in State 0 < n ≤ Q  

packets, the probability of the queue state decreasing by 1  

is given by  

b

n

= Pr(S

0

= 0, S

3

= 1, S

5

= 0)µn  

+ Pr(S

0

= 0, S

3

= 0, S

5

= 1)k1µn+k2  

where k1 = Pr(S

0

= 0, S

3

= 0, S

5

= 1) = k2 = Pr(S

0

= 0, S

3

= 0, S

5

= 1), and b

n

is the transition probability from State n + 1 to State n.  

When the queue is in State 0 ≤ n < Q packets, the probability  

of the queue state increasing by 1 is given by  

a

n

= Pr(S

0

= 0, S

3

= 1, S

5

= 0)αn  

+ Pr(S

0

= 0, S

3

= 0, S

5

= 1)k3αn+k3  

where k3 = Pr(S

0

= 0, S

3

= 0, S

5

= 1) = 0, and a

n

is the transition probability from State n to State n + 1.  

Analyzing the Markov chain of Rooney’s queue, the local  

balance equations are given by  

ζ

n

αn = ζ

n+1b

n+1 , 0 ≤ n ≤ Q − 1  

where ζ

n

denotes the probability of having n packets at  

Rooney’s queue. Using the balance equations successively, the  

stationary distribution of ζ

n

is given by  

ζ

n

= ζ0  

αm b

m+1  

m=0  

(22)  

where ζ0 = (1 + ∑

m=1  

αm b

m+1  

Q−1  

−1 ) is obtained using the  

normalization condition ∑

n=0  

ζ

n

= 1.  

Based on the above description, the average secure end-to-  

dend throughput in packets/slot, denoted by µ, is given by  

µ = ∑

n=1  

b

n

ζ

n

+ Pr(S

= 1) + Pr(S

= 0, S

= 1)  

(23)  

+ (Pr(S

= 1) − Pr(S

= 1) + Pr(S

= 0, S

= 1))ζ0  

Our aim is to maximize µ via optimizing {αm}Q−1  

m=1. The optimization problem is given by  

max :  

0≤αm≤1  

m=1  

µ  

(24)  

The formulation of this optimization problem is nonconvex in  

{αm}Q−1  

m=1. Next, we employ a change of variables and convert  

the problem to a linear program.  

Letting φ

=  

m=0  

b

m+1  

−1 , and substituting with the value  

of ζ0, we can rewrite ∑

m=1  

b

n

ζ

n

as follows  

∑

n=1  

(b

n

φ

= ∑  

k1 + k2)φ

− k1  

n=1  

(αmφ

)  

(25)
In the following, we write \( \sum_{n=1}^{Q-1} (a_n \phi_n) \) as a linear function of \( \{ \phi_n \}_{n=1}^{Q-1} \). Since \( \phi_n = \prod_{m=0}^{n-1} \frac{a_m}{b_m} \), we have the following relation between \( \phi_n \) and \( \phi_{n-1} \):

\[
\frac{\phi_n}{\phi_{n-1}} = \frac{a_{n-1}}{b_n} = \frac{k_1 \alpha_{n-1} + k_3}{k_1 \alpha_n + k_2}
\]

(26)

Therefore, we get the following recurrence relation between \( \phi_n \alpha_n \) and \( \phi_{n-1} \alpha_{n-1} \):

\[
\phi_n \alpha_n = -\phi_{n-1} \alpha_{n-1} - \frac{k_3}{k_1} \phi_n + \frac{k_1 + k_2}{k_1} \phi_{n-1}
\]

(27)

Letting \( d = \frac{k_3}{k_1} \) and \( e = \frac{k_1 + k_2}{k_1} \), then

\[
\phi_n \alpha_n = -\phi_{n-1} \alpha_{n-1} - d \phi_n + e \phi_{n-1}
\]

(28)

Since \( \phi_n = \prod_{m=0}^{n-1} \frac{a_m}{b_m} \), \( \forall n \geq 1 \), we have

\[
\phi_1 = \frac{a_0}{b_1} = \frac{(k_1 + k_3)}{k_1
\]

Hence,

\[
\phi_1 \alpha_1 = e \phi_1 - \beta, \quad \text{where} \quad \beta = \frac{(k_1 + k_3)}{k_1}
\]

(30)

Starting from (30), \( \phi_n \alpha_n \) is given by

\[
\phi_n \alpha_n = e \phi_n + \sum_{\ell=1}^{n-1} (-1)^{n-\ell} (e + d) \phi_\ell + (-1)^n \beta
\]

(31)

Substituting (31) into (23), we obtain the following linear-fractional program

\[
\begin{align*}
\max &: \quad \frac{c^T \phi + f}{1 + \phi} \\
\text{s.t.} &: \quad 0 \leq \frac{e^T \phi + g}{\phi} \leq 1, \forall n \in \{1, 2, \ldots, Q-1\} \\
&: \quad c_n^T \phi + g_Q = 0
\end{align*}
\]

(32)

where the superscript \( T \) denotes the vector transposition, \( \phi = [\phi_Q, \phi_{Q-1}, \ldots, \phi_2, \phi_1]^T \), \( c = -k_3 [- (k_1 + k_2)/k_1, e, -d, e, -d, \ldots, d ]^T + (k_1 + k_2) [0 , 1, 1, \ldots, 1]^T \),

\[
f = \begin{cases} 
\Pr(S_3 = 1) - \Pr(S_3' = 1) + \Pr(S_3' = 0, S_3 = 1), & \text{Q odd} \\
\Pr(S_3 = 1) - \Pr(S_3' = 1) + \Pr(S_3' = 0, S_3 = 1) - \beta, & \text{Q even}
\end{cases}
\]

\[
c_n = [0, \ldots, 0, e, -(e+d), (e+d), -(e+d), \ldots, d]^T, \quad g_n = (-1)^n \beta
\]

Note that \( \phi \) and \( c_n \) are \( Q \)-dimensional column vectors, while \( f \) and \( g_n \) are scalars. The linear-fractional program in (32) can be solved efficiently by converting it to a standard linear program [7, Page 151]. Then, we obtain \( \{ \alpha_n \}_{n=1}^{Q-1} \) as

\[
\alpha_n = \frac{c_n^T \phi + g_n}{\phi_n}, \forall n \in \{1, 2, \ldots, Q-1\}
\]

(33)

V. NUMERICAL SIMULATIONS AND CONCLUSIONS

In this section, we simulate the considered wireless network and show the benefits of our proposed scheme. The fading channels are assumed to be complex circularly-symmetric Gaussian random variables with zero mean and unit variance. In Fig. 1, we plot the average secure end-to-end throughput of our proposed scheme and the conventional bufferless FD scheme. In the conventional bufferless FD scheme, Alice and Rooney cooperatively transmit the data in each time slot using the DF relaying strategy. The parameters used to generate Fig. 1 are: \( \kappa_R = \kappa_B = \kappa_E = \kappa, \kappa, R_s = 1 \text{ bits/sec/Hz}, b_s = 1000 \text{ bits}, W = 1 \text{ MHz}, T = 1 \text{ msec}, P_A/(\kappa W) = P_R/(\kappa W) = 10 \text{ dB}, \) and \( \sigma^{2}_{RR} = 0.1 \).

REFERENCES

[1] 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, 2015.

[2] A. El Shafie and N. Al-Dhahir, “Secure communications in the presence of a buffer-aided wireless-powered relay with self-energy recycling,” IEEE Wireless Commun. Lett., vol. 5, no. 1, pp. 32–35, Feb. 2016.

[3] 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, 2015.

[4] N. N. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, “Secure full-duplex small-cell networks in a spectrum sharing environment,” IEEE Access, 2016, available [Online]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7500135.

[5] J. Mo, M. Tao, and Y. Liu, “Relay placement for physical layer security: A secure connection perspective,” IEEE Comm. Lett., vol. 16, no. 6, pp. 878–881, 2012.

[6] E. Teken and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2735–2751, June 2008.

[7] S. Boyd and L. Vandenberghe, Convex optimization. Cambridge University Press, 2004.