10.1109/ACCESS.2022.3151792, IEEE Access

Date of publication xxxx 00, 2021, date of current version xxxx 00, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.DOI

Impact of Outdated CSI on the Secure Communication in Untrusted In-Band Full-Duplex Relay Networks

JIN-TAEK LIM[1], (Member, IEEE), TAEHOON KIM[2], (Member, IEEE), and INKYU BANG[3], (Member, IEEE)

[1]Agency for Defense Development, Daejeon 34186, Republic of Korea (e-mail: jtlim@add.re.kr)
[2]Department of Computer Engineering, Hanbat National University, Daejeon 34158, Republic of Korea (e-mail: thkim@hanbat.ac.kr)
[3]Department of Information and Communication Engineering, Hanbat National University, Daejeon 34158, Republic of Korea (e-mail: ikbang@hanbat.ac.kr)

Corresponding authors: Taehoon Kim and Inkyu Bang

This work was partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1G1A1101176) and was partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1F1A1069934).

ABSTRACT To provide reliable connectivity in recent and future wireless communication systems, it is necessary to deploy several relay nodes. Further, a full-duplex (FD) technique has been in the spotlight since it can significantly improve spectral efficiency, and thus recent studies in relaying networks have considered FD relays. In relaying networks, confidentiality between the source and destination nodes from the relay node should be carefully kept, especially, when the relay node is not fully trusted, so-called *untrusted* relay node. To this end, in this paper, we consider physical-layer security taking into account an untrusted FD relay node. We investigate a secure relaying protocol against the untrusted relay node where the destination generates artificial noise to prevent the untrusted relay from decoding the source information. We derive the analytical expression of the lower bound of the ergodic secrecy rate ($\bar{R}$). We find two main factors affecting the secrecy performance: residual self-interference (RSI) at the FD-available nodes (i.e., relay and destination), and outdated channel state information (CSI) at the destination. Thereafter, we evaluate their effects on $\bar{R}$ and suggest the algorithm for finding the sub-optimal artificial noise power level at the destination for maximizing $\bar{R}$. Through simulations, we have verified our mathematical derivation and have shown that our secure relaying protocol can achieve near-optimal secrecy performance. Numerical results imply that the artificial noise power level should be carefully considered when the channel is severely outdated and RSI is irresistible.

INDEX TERMS Physical-layer security, untrusted relay, full-duplex, outdated channel state information, artificial noise.

I. INTRODUCTION

Conventionally, security in wireless communications is conducted through cryptographic techniques on the network layers by using secret key distribution, which rely on the computational complexity (e.g., prime factorization). However, it will encounter unprecedented challenges with the rapid development of quantum computing which is believed to be capable of solving complex computational problems substantially faster than classical computing [1]. Motivated by this, physical layer security (PLS) has been considered one of the primary alternative cryptographic techniques, which exploits the fundamental characteristics of wireless medium to achieve perfect secrecy without keys or computational complexity [2], [3].

Nowadays, with best compatibility and applicability, the PLS technology has been extended and investigated in cooperative relaying networks. There have been recent studies on the impact of nodes cooperation on the secrecy capacity, following the pioneering works of [4], [5]. Under one eavesdropper, PLS communication in two-hop wireless relaying network was investigated in [4]. Park et al. developed three types of jamming signal[1] power allocation methods to minimize the outage probability of the secrecy rate, according to the channel information available at the destination. Moreover, in [5], Liu et al. investigated the PLS system where there are one source, one destination, one eavesdropper, and multiple decode-

[1]In this paper, we use 'artificial noise' and 'jamming signal' interchangeably as the same meaning.

and-forward relays with optimal relay selection method and power allocation. However, the relaying scheme in [4], [5] is sub-optimal in the sense that it ignores the impact of the buffer state information at the relay node. In [6], they proposed a buffer-aided full-duplex (FD) relay with finite buffer and showed a significant average secrecy end-to-end throughput improvement. In order to further improve the secrecy capacity, the PLS communication study where a multi-antenna cooperative jammer is employed to improve secret communication in the presence of a multi-antenna eavesdropper was also conducted with different secrecy rate optimization techniques in [7].

Studies previously mentioned only considered relay to be reliable. However, in some applications, relays can have different classes of security clearance [8]. For example, in the network of a government, a military, or a financial institution, not all nodes are supposed to have the access to information, albeit they help the information transfer as relay nodes with agreed protocols in the network. In this sense, researches for such a special node, called untrusted relay, are being actively conducted [8]–[10]. In [8], He et al. considered the untrusted relay channel and proved that the untrusted relay may help the source and the destination to communicate despite being subjected to the secrecy constraint, and that cooperation with the untrusted relay is beneficial. The untrusted multi-antenna relay in three nodes scenario was also investigated in [9]. Meanwhile, these untrusted relay researches raised the new trade-off issue for the artificial noise power level. For example, [10] showed that controlling the artificial noise power level under a wireless energy harvesting untrusted node is very important from the point of view of PLS performance.

One candidate which also influences the optimal artificial noise level is the time-varying nature of channels. In PLS relaying network, the time-varying fading channels causes the channel state information (CSI) to become outdated [11]–[15]. In particular, if the receiver which wants to decode the artificial noise does not know the exact CSI through the artificial noise sent, it can not perfectly filter out the artificial noise from the received signal, resulting in residual jamming interference (RJI). This RJI can significantly deteriorate the PLS performance. The outdated CSI inevitably occurs in a real relay environment, and researches that does not reflect it is only an ideal condition. The quality of CSI on the performance of relay selection schemes in cooperative communications was firstly investigated in [11], [12]. In the presence of outdated CSI, [13] investigated the on-off scheme to help perform secure transmission and presented the design of wiretap coding parameters. Moreover, based on the study of [10], the optimal control of the artificial noise power level under outdated CSI were derived to maximize the secrecy performance of wireless powered untrusted relay networks in [14], [15].

Another factor affecting the optimal artificial noise level can arise in the application of FD system. In the next generation wireless system, the duplex modes of a node is being expanded to FD system. Half-duplex (HD) mode nodes can receive and forward the radio signal in different time/frequency slots. In contrast, FD nodes can exchange radio signal simultaneously in the same time/frequency slots. The FD technology itself doubles the frequency efficiency by simultaneously transmitting and receiving, but if it is applied to the relay and destination, the time slots can be effectively used, leading to doubling the reception rate of the destination (the transmission rate of the source). Generally, the performance of FD systems is limited by the residual self interference (RSI) in receive antenna. This RSI from the signal transmission can deteriorate the performance of the PLS system, resulting in a need to control the artificial noise power level. Hence, the FD mode has received a lot of attention in the PLS research community [16]–[22]. [16], [17] designed joint information beamforming and jamming beamforming to guarantee both transmit security and receive security for a FD base-station. In [18], [19], secure communications in FD relaying systems was investigated to enhance PLS performance. A robust resource allocation framework to improve the PLS performance in the presence of an active FD eavesdropper was proposed in [20]. [21], [22] investigated the user-fairness relay selection problem for decode-and-forward FD relay networks where multiple users cooperate with multiple relays.

In this paper, we want to propose the two-hop relaying PLS system combined with FD technology in the practical environment. Our proposal can greatly improve the PLS performance. However, it has a challenge that both the effect of RJI and RSI must be analyzed from the side of the PLS performance. Despite such an importance, to the best of our knowledge, studies including the influence of RJI and RSI have not yet been conducted. To summarize our problem; a destination-assisted cooperative jamming strategy is adopted to maintain information confidentiality from the untrusted relay. Because we consider a real two-hop relaying system, the outdated CSI is modeled by the well-known channel correlation model [11]. Moreover, for FD operations in relay/destination nodes, the resulting RSI is modeled as a complex Gaussian distribution model [21]. Under these settings, we find out the sub-optimal jamming signal power level, $\tilde{\zeta}$, according to the amount of RSI and RJI. The main contributions of this paper are summarized as follows.

1) In consideration of a FD relay-to-destination outdated link, we derive the analytical expressions of important metric for the secrecy performance; the lower-bound of the ergodic secrecy rate (ESR), $\bar{R}_{LB}$, in the closed form.

2) From the derived analytical expression, we suggest the algorithm iteratively finding the values of $\tilde{\zeta}$ optimizing $\bar{R}_{LB}$. We also show that the proposed methods achieve near-optimal secrecy performances with much lower time complexity, compared to an exhaustive search based on Monte Carlo simulation.

3) Our simulation results show that ζ is a dominant determinant for improving ESR.

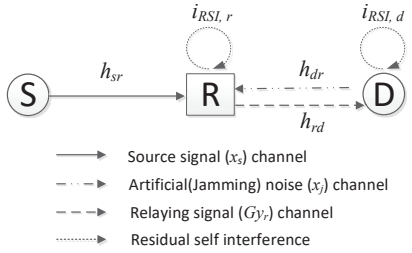


FIGURE 1. System model

II. SYSTEM MODEL

Fig. 1 shows the system model of a secure FD relaying network consisting of a source, an untrusted relay, and a destination. In this paper, we assume that the direct link between the source and destination is unavailable due to a blockage or long distance. Each node is equipped with a single receive antenna and a single transmit antenna. A source operates in a half-duplex mode with only transmission, while an untrusted relay and a destination operate in a full-duplex mode. The channel between nodes i and j is denoted by h_{ij}, and follows a complex Gaussian distribution with zero-mean and variance λ_{ij}, such that $h_{ij} \sim \mathcal{CN}(0, \lambda_{ij})$. Here, $i, j \in \{s, r, d\}$ and the subscripts, s, r, and d, represent the source, untrusted relay, and destination, respectively. The channel power gain $|h_{ij}|^2$ follows an exponential distribution with mean λ_{ij}, of which the probability density function (PDF) is given by

$$f_{|h_{ij}|^2}(x) = \frac{1}{\lambda_{ij}} e^{-\frac{x}{\lambda_{ij}}}, \quad x \geq 0. \tag{1}$$

In addition, we consider a quasi-static frequency nonselective channel, where the channel is constant over the duration of a single time slot and changes every time slot with correlation [14], [15]. The baseband noise for node i is denoted n_i, and is assumed to follow a complex additive white Gaussian noise (AWGN) with zero-mean and variance σ^2, i.e., $n_i \sim \mathcal{CN}\left(0, \sigma^2\right)$.

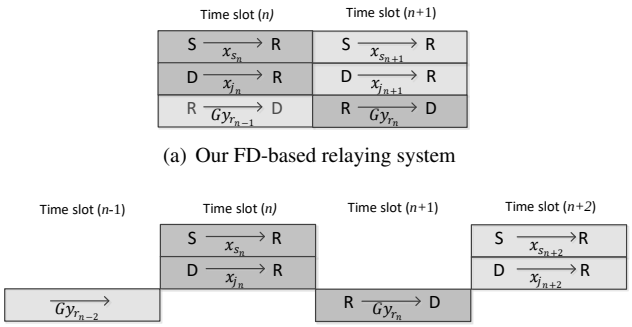
A. RESIDUAL SELF INTERFERENCE MODELING

In FD mode operations, to avoid excessive interference, each relay and destination node applies several stages of self-interference cancellation. Moreover, the antenna isolation techniques such as implementing a solid physical barrier between a transmit and a receive antenna, utilizing directional antennas and exploiting antenna polarization greatly mitigate the transmit power leakage especially via the LOS path. However, notwithstanding all efforts, there still exists the RSI denoted as $i_{RSI,i}$.

In modeling $i_{RSI,i}$, the Gaussian assumption from the central limit theorem holds in practice due to the various sources of imperfections in the interference cancellation process.

So, $i_{RSI,i}$ can be assumed to be independent to other signals and follows a complex Gaussian distribution with zero mean and variance κP_i^{ν}, such that $i_{RSI,i} \sim \mathcal{CN}(0, \kappa P_i^{\nu})$, where two constants, $\kappa > 0$ and $\nu \in [0, 1]$, depend on the interference cancellation scheme at relay and destination [21].

P_i is the maximum transmit power, but, for the simplicity, we assume that $P_i = P$ for all i in this paper.



(a) Our FD-based relaying system

(b) General HD-based relaying system

FIGURE 2. Illustration for relaying single data (x_{s_n})

B. PROPOSED FD-BASED TWO-HOP RELAYING SCHEME

As illustrated in Fig. 2 (a), single source information is transmitted over two consecutive time slots (n-th and $(n+1)$-th) in our proposed system. In this system, the untrusted relay has a different security clearance from the source and destination, so there is the desire for them to maintain information confidentiality from the untrusted relay. Therefore, in the n-th time slot, the source and the destination transmit source information, x_{s_n}, and a jamming signal, x_{j_n}, to the untrusted relay, respectively. At the same time slot, the untrusted relay with the in-band full-duplex mode sends the previous amplified source information, $Gy_{r_{n-1}}$. This might deteriorate the receiving quality of x_{s_n} and x_{j_n} with i_{RSI,r_n}. In the $(n+1)$-th time slot, the untrusted relay amplifies the received signal, y_{r_n}, up to amplifying factor, G, and forwards it to the destination, Gy_{r_n}, and the destination transmits the next jamming signal, $x_{j_{n+1}}$, simultaneously. This also result in $i_{RSI,d_{n+1}}$ at the receive antenna of destination. Unlike the general HD-based two-phase relaying system in Fig. 2 (b), our FD-based relaying system can transmit each single source information in consecutive time slots, so that the reception rate of the destination can be nearly doubled.

C. OUTDATED CHANNEL MODELING

Note that the relay-to-destination link generally varies between the first and second time slot because of the time difference [11]–[13]. Considering the outdated characteristic of the wireless channel, the relationship between h_{dr_n} and $h_{rd_{n+1}}$ can be modeled as follows [11].

$$h_{dr_n} = \rho h_{rd_{n+1}} + \sqrt{1-\rho^2} w \tag{2}$$

where w is a circularly symmetric complex Gaussian random variable with the same variance as $h_{rd_{n+1}}$, i.e., $w \sim \mathcal{CN}(0, \lambda_{rd})$, and is independent from $h_{rd_{n+1}}$. In addition, ρ is a correlation coefficient between h_{dr_n} and $h_{rd_{n+1}}$, which is modelled using Jakes' autocorrelation model [23]

given by $\rho = J_0(2\pi f_d T_s)$. Here, $J_0(\cdot)$ denotes the zeroth order Bessel function of the first kind, f_d is the maximum Doppler frequency on relay-to-destination link, and T_s is the time slot length. Then, ρ can easily be estimated from knowledge of f_d and T_s.

III. PERFORMANCE ANALYSIS

A. SECRECY RATE

From now on, for the clarity, the subscript letter for indexing the time slot, n, will be omitted. Also, an untrusted relay will be referred to simply as a relay. Then, the received signal at the relay, y_r, is represented by

$$y_r = \sqrt{P} h_{sr} x_s + \sqrt{\zeta P} h_{dr} x_j + i_{RSI,r} + n_r. \quad (3)$$

Here, x_s and x_j are a source signal and an artificial jamming noise signal, respectively. They have normalized power, i.e., $\mathbb{E}[|x_s|^2] = \mathbb{E}[|x_s|^2] = 1$. And, ζ is a scaling factor used to determine the power level of the jamming signal, e.g., $0 \le \zeta \le 1$. Then, the jamming power can be determined by ζP. The signal-to-interference-plus-noise ratio (SINR) at the relay for detecting x_s, Γ_r, is obtained as

$$\begin{aligned}\Gamma_r &= \frac{|h_{sr}|^2}{\zeta(\rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2) + \kappa P^{\nu-1} + 1/\gamma} \\ &= \frac{X}{\zeta\rho^2 Y + \zeta(1-\rho^2)Z + \kappa P^{\nu-1} + 1/\gamma}\end{aligned} \quad (4)$$

where $\gamma = \frac{P}{\sigma^2}$ denotes the transmit signal-to-noise ratio (SNR). And, $X = |h_{sr}|^2$, $Y = |h_{rd}|^2$, and $Z = |w|^2$ are the exponential RVs with means λ_{sr}, λ_{rd}, and λ_{rd}, respectively.

During the second time slot, the relay amplifies the received signal by a factor G and forwards it to the destination. Thus, the amplifying factor, G, is given by

$$G = \sqrt{\frac{P}{P|h_{sr}|^2 + \zeta P|h_{dr}|^2 + \kappa P^{\nu} + \sigma^2}} \quad (5)$$

where $|h_{dr}|^2 = \rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2$.

Then, the received signal at the destination, y_d, is obtained as

$$\begin{aligned}y_d &= G h_{rd} y_r + i_{RSI,d} + n_d \\ &= G h_{rd}(\sqrt{P} h_{sr} x_s + \sqrt{\zeta P} h_{dr} x_j + i_{RSI,r} + n_r) \\ &\quad + i_{RSI,d} + n_d\end{aligned} \quad (6)$$

Because x_j is the jamming noise sent by the destination during the first time slot, the destination can eliminate it by subtracting $G\sqrt{\zeta P}\rho h_{rd}^2 z$ from y_d. After the jamming noise has been cancelled, the received signal at the destination can be rewritten as

$$\begin{aligned}\hat{y}_d &= y_d - G\sqrt{\zeta P}\rho h_{rd}^2 x_j \\ &= G(\sqrt{P} x_s h_{sr} + i_{RSI,r} + n_r) h_{rd} \\ &\quad + G\sqrt{\zeta P}\sqrt{1-\rho^2} h_{rd} w x_j + i_{RSI,d} + n_d\end{aligned} \quad (7)$$

where $G\sqrt{\zeta P}\sqrt{1-\rho^2} h_{rd} w x_j$ denotes the residual jamming signal, which cannot be perfectly cancelled because of the outdated CSI of the relay-to-destination link.

Then, the SINR at the destination can be expressed as (8) where $c_1 = \frac{1}{\gamma}\left(1 + \frac{\kappa(\zeta P)^{\nu}}{\sigma^2}\right)$, $c_2 = \frac{1}{\gamma}\left(1 + \frac{\kappa P^{\nu}}{\sigma^2}\right) + \frac{\zeta\rho^2}{\gamma}\left(1 + \frac{\kappa(\zeta P)^{\nu}}{\sigma^2}\right)$, $c_3 = \frac{\zeta}{\gamma}(1-\rho^2)\left(1 + \frac{\kappa(\zeta P)^{\nu}}{\sigma^2}\right)$, $c_4 = \zeta(1-\rho^2)$, and $c_5 = \frac{1}{\gamma^2}\left(1 + \frac{\kappa P^{\nu}}{\sigma^2}\right)\left(1 + \frac{\kappa(\zeta P)^{\nu}}{\sigma^2}\right)$.

To maintain information security against the relay, the legitimate link must achieve a higher data rate than the wiretap link. In other words, if $\Gamma_d < \Gamma_r$, the mutual information between the source and destination becomes zero [24]. Therefore, the achievable instantaneous secrecy rate can be defined as the difference between the rate of the legitimate link and that of the wiretap link [3].

$$R \triangleq \left[\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+ \quad (9)$$

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

B. ERGODIC SECRECY RATE

The ESR is an useful metric such as in a delay-tolerant application. This indicates the average secrecy rate at which the relay fails to decode the secret information [10].

We can obtain the ESR by taking the expectation of (9) over three random variables, X, Y, and Z.

$$\begin{aligned}\bar{R} &= \mathbb{E}_{X,Y,Z}[R] \\ &= \int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\left[\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+ \\ &\quad \times f_X(x) f_Y(y) f_Z(z) dx dy dz.\end{aligned} \quad (10)$$

Although the triple integral expressions in (10) can be evaluated numerically, it is not yet possible to find a closed-form expression. Thus, we derive the tight lower-bound of the ergodic secrecy rate, which can be written as

$$\begin{aligned}\bar{R} &= \mathbb{E}\left[\left[\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+\right] \\ &\overset{(a)}{\ge} \left[\frac{1}{\ln 2}\left(\mathbb{E}[\ln(1+\Gamma_d)] - \mathbb{E}[\ln(1+\Gamma_r)]\right)\right]^+ \\ &\overset{(b)}{\ge} \left[\frac{1}{\ln 2}\left(\ln(1+\exp(\mathbb{E}[\ln\Gamma_d])) - \mathbb{E}[\ln(1+\Gamma_r)]\right)\right]^+ \\ &\overset{(c)}{\ge} \left[\frac{1}{\ln 2}\left(\ln(1+\exp(\underbrace{\mathbb{E}[\ln\Gamma_d{}']}_{\mathcal{L}_1})) - \underbrace{\mathbb{E}[\ln(1+\Gamma_r)]}_{\mathcal{L}_2}\right)\right]^+ \\ &\triangleq \bar{R}_{LB}\end{aligned} \quad (11)$$

where inequality (a) comes from the fact that $\mathbb{E}[\max(X_1, X_2)] \ge \max(\mathbb{E}[X_1], \mathbb{E}[X_2])$, and inequality (b) comes from Jensen's inequality with the convexity of $\ln(1+t\exp(x))$ for $t > 0$. For the inequality (c), we replace $|G|^2$ with $|G'|^2 = \frac{P}{PX+\zeta P(\rho^2|h_{rd}|^2+(1-\rho^2)|w'|^2)+\kappa P^{\nu}+\sigma^2}$ in Γ_d. Then, we can obtain $\Gamma_d{}' = \frac{XY}{c_1\lambda_{sr}+c_2 Y+c_3\lambda_{rd}+c_4 ZY+c_5}$

$$\Gamma_d = \frac{|h_{sr}|^2|h_{rd}|^2}{(\kappa P^{\nu-1}+1/\gamma)|h_{rd}|^2+\zeta(1-\rho^2)|w|^2|h_{rd}|^2+\frac{1/\gamma+\kappa\zeta^\nu P^{\nu-1}}{|G|^2}} = \frac{XY}{c_1X+c_2Y+c_3Z+c_4ZY+c_5} \tag{8}$$

instead of Γ_d. [2] With a tight simplified form, the closed form expression for the lower-bound of the ESR can be obtained from the following proposition.

Proposition 1: The lower-bound of ESR can be expressed as

$$\bar{R}_{LB}(\zeta) = \frac{1}{\ln 2}[\ln(1+\exp(\mathcal{L}_1))-\mathcal{L}_2]^+ \tag{12}$$

In (12), $\mathcal{L}_1$ and $\mathcal{L}_2$ are defined in (13) and (14), respectively.

$$\mathcal{L}_1 = \ln\left(\frac{\lambda_{sr}\lambda_{rd}}{c_5'}\right) - 2\phi - e^{\frac{c_2'}{\lambda_{rd}c_4'}}\left[G_{4\,2}^{1\,4}\left(\lambda_{rd}^2c_4'\middle|\begin{matrix}0,0,1,1\\1,0\end{matrix}\right) - \sum_{i=0}^{\infty}\frac{(-1)^i c_2'^{\,i+1}}{(\lambda_{rd}c_4')^{i+1}i!}G_{4\,3}^{1\,4}\left(\lambda_{rd}c_2'\middle|\begin{matrix}-i,0,1,1\\1,0,-i-1\end{matrix}\right)\right] \tag{13}$$

where ϕ is the Euler's constant [25, 4.331.1], $c_5' = c_5 + c_1\lambda_{sr} + c_3\lambda_{rd}$, $c_2' = c_2/c_5'$ and $c_4' = c_4/c_5'$, and $G_{p\,q}^{m\,n}\left(z\middle|\begin{matrix}a_1,...,a_p\\b_1,...,b_q\end{matrix}\right)$ is the Meijer G function.

$$\mathcal{L}_2 = \mathcal{I}_1 - \mathcal{I}_2 \tag{14}$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ are defined in (18) and (16), respectively, with $\mu_1 = \lambda_{sr}$, $\mu_2 = \zeta\rho^2\lambda_{rd}$, $\mu_3 = \zeta(1-\rho^2)\lambda_{rd}$, $C = \kappa P^{\nu-1}+1/\gamma$, $\mathrm{Ei}(x) = -\int_{-x}^{\infty}\frac{e^{-t}}{t}dt$ is the exponential integral, and $g_1(\cdot)$, $g_2(\cdot)$, and $g_3(\cdot)$ are defined in Lemma 4 of Appendix C [15].

Proof: See Appendix A. ■

C. ALGORITHM FOR FINDING THE SUB-OPTIMAL JAMMING POWER LEVEL, $\tilde{\zeta}$

From inspecting (12), we suggest the following lemma.

Lemma 1: With high SNR assumption ($\frac{1}{\gamma^2} \cong 0$), $\bar{R}_{LB}(\zeta)$ is an unimodal function (especially, an *increasing* or *increasing and then decreasing* function for $0 \le \zeta \le 1$). So, it has one peak at $\tilde{\zeta}$.

Proof: See Appendix B. ■

Then, the extremum of an unimodal function can always be found through the well-known divide-and-conquer algorithms [26] such as Golden-section searching algorithm and Fibonacci searching algorithm. Through the Golden-section algorithm (Algorithm 1), we present the way to iteratively find $\tilde{\zeta}$ for our system. This proposed algorithm has the complexity as $\mathcal{O}(\log(1/\epsilon))$ where ϵ is the accuracy.

Algorithm 1 A Golden-section searching algorithm for $\tilde{\zeta}$

$\zeta_1 \leftarrow 0$, $\zeta_4 \leftarrow 1$
$\tilde{\zeta}_{prev} \leftarrow 0$, $\tilde{\zeta} \leftarrow 1$
while $|\tilde{\zeta} - \tilde{\zeta}_{prev}| > \epsilon$ **do**
  $\zeta_2 \leftarrow \zeta_4 - \frac{\sqrt{5}-1}{2}(\zeta_4-\zeta_1)$
  $\zeta_3 \leftarrow \zeta_1 + \frac{\sqrt{5}-1}{2}(\zeta_4-\zeta_1)$
  $\tilde{\zeta}_{prev} \leftarrow \tilde{\zeta}$
  if $\bar{R}_{LB}(\zeta_2) \le \bar{R}_{LB}(\zeta_3)$ **then**
    $\zeta_1 \leftarrow \zeta_2$
  else
    $\zeta_4 \leftarrow \zeta_3$
  end if
  $\tilde{\zeta} \leftarrow \frac{\zeta_1+\zeta_4}{2}$
end while

IV. SIMULATIONS AND DISCUSSIONS

In this section, we show the impact of the channel correlation coefficient (ρ) (i.e. related to RJI cancellation level) and RSI cancellation level parameters (κ, ν) on the determination of the jamming power level (ζ). For the environment, we consider the transmit SNR as $\gamma = 70$ dB[3]. In the generation of wireless channels, we define the channel power gain between the nodes i and j as $|h_{ij}|^2 = \frac{v_{ij}}{d_{ij}^m}$, where v_{ij} reflects a small-scale fading, which is an exponential random variable with mean $\lambda_{ij} = 1$, d_{ij} is the distance between two nodes, and m is a path-loss exponent. Here, we set $d_{sr} = d_{rd} = 5$ m and $m = 2.7$. We obtain the two ESRs; the exact ESR, $\bar{R}$, by Monte Carlo Simulation and the lower bound of ESR, $\bar{R}_{LB}$, by our (12). The Monte Carlo simulation for $\bar{R}$ is performed 10^6 times, and the truncation error of the infinite sum in (12) is set to 10^{-3}. Moreover, the optimal jamming power level, ζ^*, is found by an exhaustive method based on Monte Carlo simulation, and the sub-optimal jamming power level, $\tilde{\zeta}$ is calculated by Algorithm 1. The searching interval for the exhaustive method and the accuracy of Algorithm 1, ϵ, are set to 0.02.

A. EFFECT OF (ρ, κ, AND ν) ON ERGODIC SECRECY RATE AND OPTIMAL JAMMING POWER LEVEL

Fig. 3 shows the variation of $\bar{R}$ and $\bar{R}_{LB}$ according to ζ given $\nu = 0$ (best case for SI cancellation model). As shown in subfigures (a) and (b), $\bar{R}$ and $\bar{R}_{LB}$ are unimodal functions with respect to ζ. Therefore, there exist the optimal value of ζ for maximizing them.

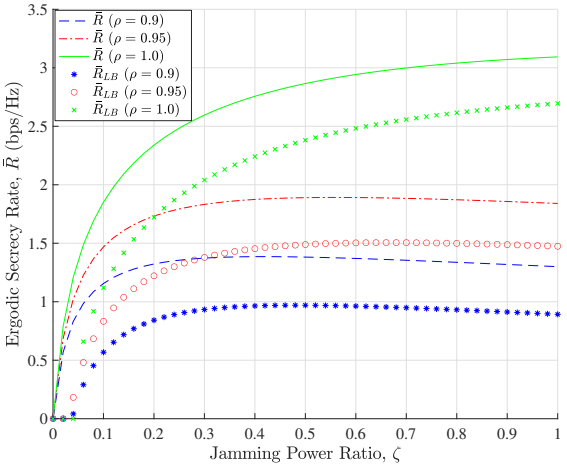
In subfigure (a), $\bar{R}$ and $\bar{R}_{LB}$ show similar graph trends, but there is a significant gap between them. This gap is originated from the fact that κ is not sufficiently small with large RSI, leading to a small $|G|^2$ This makes the LB approximation deviating in (11). However, the values of ζ at which the maximum point appears in both cases do

[2] The background of this derivation is that, since κP^ν, $\frac{1}{\gamma}$, and $\frac{1}{|G|^2}$ (the typical value of $|G|^2$ in AF relaying is generally large.) are sufficiently small, $\frac{1}{\gamma|G|^2}(1+\kappa P^\nu)$ occupies a small proportion in Γ_d. Thus, we can assume that $|w|^2$ in $1/|G|^2$ is independent of the other $|w|^2$ of $\zeta(1-\rho^2)|h_{rd}|^2|w|^2$ in Γ_d, as indicated by $|w'|^2$. From the same reason, we can take Jensen's inequality for $|h_{sr}|^2$ and $|w'|^2$ with the tight bound.

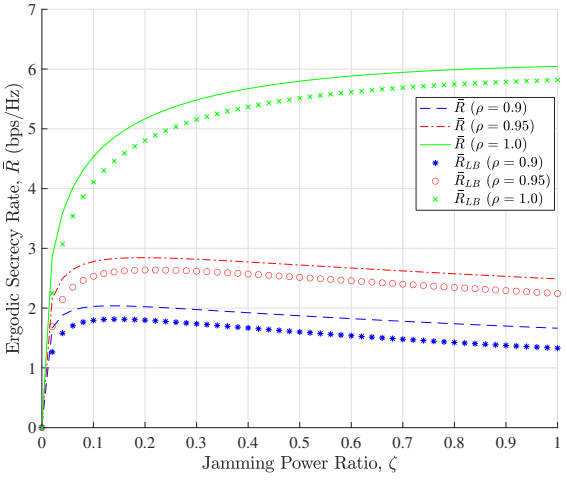
[3] 70 dB is not a large value for the transmit SNR ($\frac{P}{\sigma^2}$). the noise power, σ^2, is N_0B where N_0 is the noise power density and B is the signal bandwidth. For example, if we set $(P)_{\mathrm{dBm}} = 27$ (typical cellular phone transmission power), $(N_0)_{\mathrm{dbm/Hz}} = -174$ (typical noise power density), and $(B)_{\mathrm{Hz}} = 10^7$, the transmit SNR is calculated as 122 dB.

$$\mathcal{I}_1 = \begin{cases} \sum_{i=1}^{3} \frac{(\mu_i)^2}{\prod_{\substack{j\neq i \\ j=1}}^{3}(\mu_i-\mu_j)} \left(\ln C - e^{\frac{C}{\mu_i}} \mathrm{Ei}\left(-\frac{C}{\mu_i}\right)\right), & \text{if } \mu_1 \neq \mu_2 \neq \mu_3 \\ \frac{1}{\mu} g_2(\mu, C) - \left(\frac{\mu_i}{\mu-\mu_i}\right)^2 g_1(\mu_i, C) + \frac{\mu\mu_i^2}{(\mu-\mu_i)^2} \frac{1}{2\mu-\mu_i} g_1\left(\frac{\mu\mu_i}{2\mu-\mu_i}, C\right), & \text{if } \mu_i \neq \mu_j = \mu_k = \mu \\ \quad + \frac{\mu_i^2}{\mu-\mu_i} \frac{1}{2\mu-\mu_i} g_2\left(\frac{\mu\mu_i}{2\mu-\mu_i}, C\right) - \frac{\mu_i}{\mu(\mu-\mu_i)} g_2\left(\frac{\mu\mu_i}{2\mu-\mu_i}, C\right), & \text{for all } (i,j,k) \\ \left(1-\frac{1}{\mu}\right) g_2(\mu, C) + \frac{1}{2\mu^2} g_3(\mu, C), & \text{if } \mu_1 = \mu_2 = \mu_3 = \mu. \end{cases} \tag{15}$$

$$\mathcal{I}_2 = \begin{cases} \sum_{i=2}^{3} \frac{(\mu_i)^2}{\prod_{\substack{j\neq i \\ j=2}}^{3}(\mu_i-\mu_j)} \left(\ln C - e^{\frac{C}{\mu_i}} \mathrm{Ei}\left(-\frac{C}{\mu_i}\right)\right), & \text{if } \mu_2 \neq \mu_3 \\ \frac{1}{\mu} g_2(\mu, C), & \text{if } \mu_2 = \mu_3 = \mu. \end{cases} \tag{16}$$

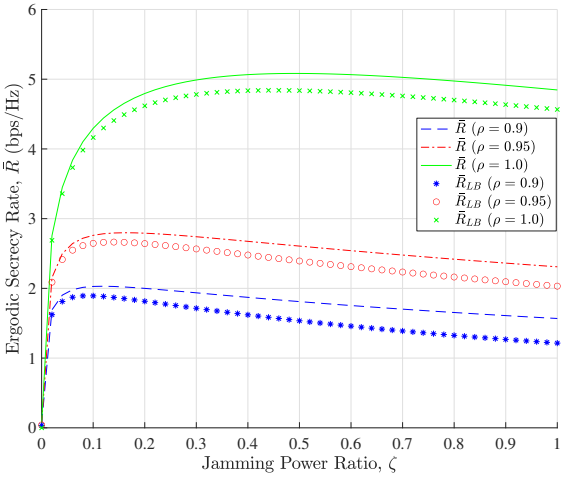


(a) $\kappa = 10^{-4}$

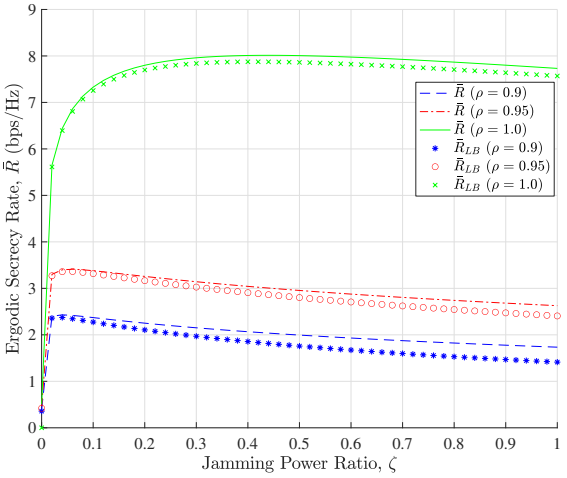


(b) $\kappa = 10^{-5}$

FIGURE 3. Variation of ($\bar{R}$ and $\bar{R}_{LB}$) according to ζ with $\nu = 0$



(a) $\kappa = 10^{-4}$



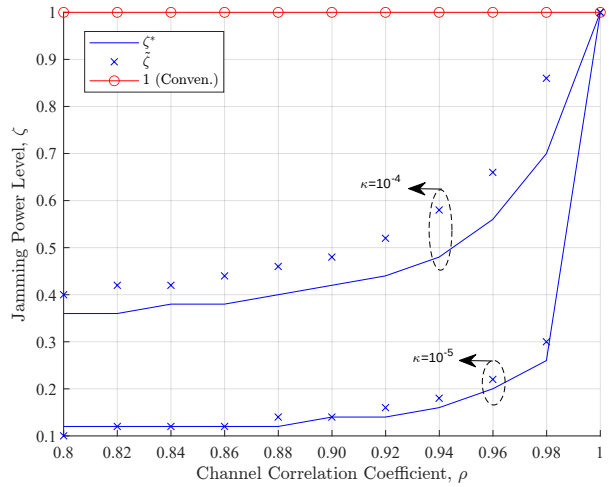
(b) $\kappa = 10^{-5}$

FIGURE 4. Variation of ($\bar{R}$ and $\bar{R}_{LB}$) according to ζ with $\nu = 1$

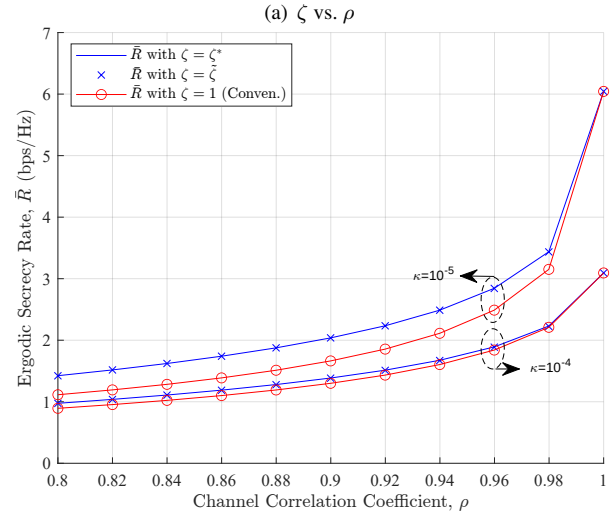
not differ significantly (we can check it in the subfigure (a) of Fig. 5). This means that has sufficient accuracy over the optimal value, i.e. $\zeta^* \cong \tilde{\zeta}$. When $\rho = 1$, the perfect jamming signal cancellation is possible (RJI is zero) and FD RSI become insignificant, so it is advantageous to transmit the jamming signal with the maximum power. However, when ρ decreases and the channel starts to be outdated, RJI increases, then reducing ζ is optimal in terms of ESR.

In the case of subfigure (b) with $\kappa = 10^{-5}$, the difference between $\bar{R}$ and $\bar{R}_{LB}$ are reduced because the RSI is further lowered. In addition, the overall ESR performance is improved due to the reduced RSI. It can be also discovered that the accuracy of $\tilde{\zeta}$ increases as $\bar{R}$ and $\bar{R}_{LB}$ become tighter.

Fig. 4 shows the variation of $\bar{R}$ and $\bar{R}_{LB}$ according to ζ given $\nu = 1$ (worst case for SI cancellation model). Overall, $\bar{R}$ and $\bar{R}_{LB}$ tend to be more consistent than when ν is 0. As ν is increased, it needs to optimize the ESR through the

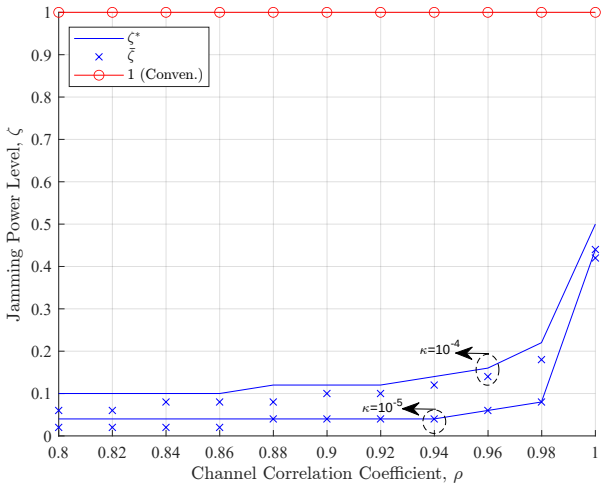


(a) ζ vs. ρ

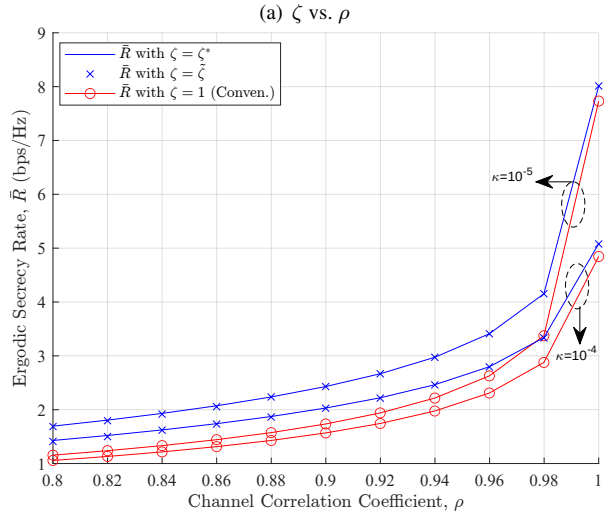


(b) $\bar{R}$ vs. ρ

FIGURE 5. Comparison of three schemes for $\bar{R}$ according to ρ with $\nu = 0$



(a) ζ vs. ρ



(b) $\bar{R}$ vs. ρ

FIGURE 6. Comparison of three schemes for $\bar{R}$ according to ρ with $\nu = 1$

adjustment of ζ even when $\rho = 1.0$ (RSI has the form, $\frac{\kappa(\zeta P)^{\nu}}{\sigma^2}$). One insightful point is that both Fig. 4 (a) and (b) represents the higher ESR performance than $\nu = 0$ case. The cause of this phenomenon is that the increased RSI (due to low SI cancellation capability) causes a steeper drop of $\log(1 + \Gamma_r)$ than that of $\log(1 + \Gamma_d)$ ($\Gamma_d > \Gamma_r$ with jamming interference cancellation). This means that, *if the SI cancellation capability of the FD relay and the FD destination are the same, increasing the RSI of the FD relay can help improve the performance of the ESR.*

B. COMPARISON OF PROPOSED METHOD AND CONVENTIONAL METHOD OVER ERGODIC SECRECY RATE

Fig. 5 shows the performance evaluation in terms of $\bar{R}$ against the channel correlation coefficient, ρ with $\nu = 0$; (a) ζ^*, $\tilde{\zeta}$, and $\zeta = 1$, (b) $\bar{R}$ under ζ^*, $\tilde{\zeta}$, and $\zeta = 1$. We plot the conventional ('Conven.') scheme, $\zeta = 1$, for the performance comparison, which only uses the full jamming power, to evaluate the effect of jamming power control [10], [14], [15]. We plot $\bar{R}$, the real performance metric, not $\bar{R}_{LB}$, to check the sub-optimal degree of $\tilde{\zeta}$.

In subfigure (a), the lines represent ζ^* while the markers indicate $\tilde{\zeta}$. The RJI deteriorates the reception of information at the destination when the channel is severely outdated. Therefore, it is better to reduce ζ as ρ decreases. Although there is a little difference between ζ^* and $\tilde{\zeta}$ with decreasing ρ, $\bar{R}$ under them match quite well as shown in subfigure (b). The reason why ζ^* and $\tilde{\zeta}$ for $\kappa = 10^{-4}$ are higher than those for $\kappa = 10^{-5}$ is the same as the analysis of Fig. 3 and Fig. 4.

In subfigure (b), the secrecy performances of three different schemes are compared. According to ρ, $\bar{R}$ under ζ^* is used for the blue line while $\bar{R}$ under $\tilde{\zeta}$ is used for the blue marker. $\bar{R}$ for all schemes decrease as ρ decreases because of a large RJI. We confirm that the proposed schemes achieve near-optimal $\bar{R}$, and outperform conventional schemes from proper adjustment of ζ against the change in ρ. These results confirm that there is a little difference between the applications of ζ^* and $\tilde{\zeta}$.

Fig. 6 shows the performance evaluation in terms of $\bar{R}$ against the channel correlation coefficient, ρ with $\nu = 1$; (a) ζ^*, $\tilde{\zeta}$, and $\zeta = 1$, (b) $\bar{R}$ under ζ^*, $\tilde{\zeta}$, and $\zeta = 1$. When ζ is properly adjusted, the amount of the performance improvement is higher than that of $\nu = 0$ case, This

explains why the adjustment of ζ is the effective way when the negative impact of FD can not be ignored.

V. CONCLUSIONS

We studied the secrecy performances of untrusted FD relay and FD destination networks under outdated CSI. To keep information secret from an untrusted relay, a destination-assisted jamming strategy is used. When the CSI of the relay-to-destination link is outdated and the FD mode is used in relay and destination, the destination cannot perfectly cancel out the RJI and the significant RSI occurs, causing significant deterioration of the secrecy performance. To assess the impact of RSI and RJI on the secrecy performance, we derived the analytical expressions of the lower bound for ergodic secrecy rate, and proposed the algorithm for finding the sub-optimal jamming power level. Our simulation and numerical results demonstrated the accuracy of our analysis and provide some useful observations. For instance, the jamming power level was an important determinant for improving the secrecy performance under outdated CSI and interference cancellation level. In addition, it was also found that the secrecy performance tends to be maximized when the RSI is above a certain level. Finally, we confirmed that the proposed scheme can be used to achieve near-optimal ergodic secrecy rate.

APPENDIX A A PROOF OF PROPOSITION 1

In the lower-bound of the ergodic secrecy rate (11), $\mathcal{L}_1$ can be derived as follows.

$$\begin{aligned}\mathcal{L}_1 &= \mathbb{E}\left[\ln\left(\frac{XY}{c_1\lambda_{sr}+c_2Y+c_3\lambda_{rd}+c_4ZY+c_5}\right)\right] \\ &= \underbrace{\mathbb{E}[\ln(XY)]}_{\mathcal{K}_1} - \underbrace{\mathbb{E}[\ln(c_2'Y+c_4'ZY+1)]}_{\mathcal{K}_2} - \ln(c_5')\end{aligned} \tag{17}$$

where $c_5' = c_5+c_1\lambda_{sr}+c_3\lambda_{rd}$, $c_2' = c_2/c_5'$ and $c_4' = c_4/c_5'$.

From [25, 4.331.1], $\mathcal{K}_1$ can be calculated as

$$\mathcal{K}_1 = \ln(\lambda_{sr}\lambda_{rd}) - 2\phi. \tag{18}$$

Moreover, $\mathcal{K}_2$ can be rewritten as

$$\begin{aligned}\mathcal{K}_2 &= \mathbb{E}[\ln(YZ'+1)] \\ &= \mathbb{E}[\ln(S+1)]\end{aligned} \tag{19}$$

where $Z' = c_4'Z + c_2'$ has the PDF of $f_{Z'}(x) = \frac{1}{c_4'\lambda_{rd}}\exp\left(-\frac{x-c_2'}{c_4'\lambda_{rd}}\right)$. Then, the PDF of S, which is the product of two exponential RVs, can be expressed as

$$f_S(s) = \int_{c_2'}^{\infty} \frac{1}{\lambda_{rd}^2 c_4' t} e^{-\frac{s}{\lambda_{rd}t} - \frac{t-c_2'}{\lambda_{rd}c_4'}} dt. \tag{20}$$

Now, we can rewrite (19) as (21) shown at the top of the next page, where (a) comes from the fact that $\ln(1+x) = G_{2\,2}^{1\,2}\left(x\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)$ and (b) comes from [25, 7.813.1]. (c) is established through the series expansion of the exponential function. Lastly, by applying [25, 7.813.1] and [25, 7.811.2], we can derive the equality (d).

In (11), $\mathcal{L}_2$ can be derived from the following procedure.

$$\mathcal{L}_2 = \mathbb{E}[\ln(1+\Gamma_r)] = \mathcal{I}_1 - \mathcal{I}_2 \tag{22}$$

where $\mathcal{I}_1 = \mathbb{E}\big[\ln\big(|h_{sr}|^2 + \zeta(\rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2) + \kappa P^{\nu-1} + 1/\gamma\big)\big]$ and $\mathcal{I}_2 = \mathbb{E}\big[\ln\big(\zeta(\rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2) + \kappa P^{\nu-1} + 1/\gamma\big)\big]$. Let us define $X_1 = |h_{sr}|^2$, $X_2 = \zeta\rho^2|h_{rd}|^2$, and $X_3 = \zeta(1-\rho^2)|w|^2$ are the exponential RVs with means $\mu_1 = \lambda_{sr}$, $\mu_2 = \zeta\rho^2\lambda_{rd}$, and $\mu_3 = \zeta(1-\rho^2)\lambda_{rd}$, respectively. In addition, let us replace $\kappa P^{\nu-1} + 1/\gamma$ with C. With those simplified notations, we note that $\mathcal{I}_1 = \mathbb{E}\left[\ln\left(\sum_{i=1}^3 X_i + C\right)\right]$ and $\mathcal{I}_2 = \mathbb{E}\left[\ln\left(\sum_{i=2}^3 X_i + C\right)\right]$. Then, with the expression 2) of Lemma 5 in [15], we can derive $\mathcal{I}_1$ and $\mathcal{I}_2$ as (18) and (16), respectively. Finally, with $\mathcal{L}_1$ and $\mathcal{L}_2$, we can obtain the lower-bound of the ergodic secrecy rate as (12).

APPENDIX B A PROOF OF LEMMA 1

To prove Lemma 1, let's rewrite (11) as

$$\begin{aligned}\bar{R}_{LB} &= \left[\frac{1}{\ln 2}\left(\ln(1+\exp(\mathcal{L}_1)) - \mathcal{L}_2\right)\right]^+ \\ &= \left[\frac{1}{\ln 2}Q(\zeta)\right]^+.\end{aligned} \tag{23}$$

If $Q(\zeta)$ is an unimodal function, so is $\bar{R}_{LB}$. Therefore, we will prove that $Q(\zeta)$ is an unimodal function.

We prove it by the fact that, If $\frac{\partial Q(\zeta)}{\partial\zeta} = 0$ has a single positive real root and $\frac{\partial Q(\zeta)}{\partial\zeta}\Big|_{\zeta=0} \geq 0$, then $Q(\zeta)$ *increases* or *increases and then decreases* for $0 \leq \zeta \leq 1$ (if a positive real root is larger than 1, then $Q(\zeta)$ is an *increasing* function; otherwise, an *increasing and then decreasing* function)

Before starting proof, we need to check out the signs of $\frac{\partial\mathcal{L}_1}{\partial\zeta}$, $\frac{\partial\mathcal{L}_2}{\partial\zeta}$, $\frac{\partial^2\mathcal{L}_1}{\partial\zeta^2}$ and $\frac{\partial^2\mathcal{L}_2}{\partial\zeta^2}$.

From differentiating $\mathcal{L}_1$ by ζ, we can obtain

$$\begin{aligned}\frac{\partial\mathcal{L}_1}{\partial\zeta} &= \frac{\partial\mathbb{E}[\ln\Gamma_d{}']}{\partial\zeta} \\ &= \int_0^\infty\int_0^\infty\int_0^\infty \frac{\partial\ln\Gamma_d{}'}{\partial\zeta} f_X(x)f_Y(y)f_Z(z)dxdydz. \\ &= \mathbb{E}\left[\frac{1}{\Gamma_d{}'}\frac{\partial\Gamma_d{}'}{\partial\zeta}\right] \\ &= \mathbb{E}\left[-\frac{d_3+d_4\nu\zeta^{\nu-1}+d_5(\nu+1)\zeta^\nu}{d_2+d_3\zeta+d_4\zeta^\nu+d_5\zeta^{\nu+1}}\right] \\ &\overset{(a)}{\leq} 0\end{aligned} \tag{24}$$

where $\Gamma_d{}' = \frac{d_1}{d_2+d_3\zeta+d_4\zeta^\nu+d_5\zeta^{\nu+1}}$ is rearranged as a function of ζ with $d_1 = XY$, $d_2 = \frac{X}{\gamma} + \frac{Y}{\gamma}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right) + \frac{1}{\gamma^2}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right)\left(1+\frac{\kappa(\zeta P)^\nu}{\sigma^2}\right)$, $d_3 = \frac{\rho^2 Y}{\gamma} + \frac{(1-\rho^2)Z}{\gamma} + (1-\rho^2)ZY$, $d_4 = \frac{\lambda_{sr}}{\gamma}\frac{\kappa P^\nu}{\sigma^2} + \frac{\kappa P^\nu}{\gamma^2\sigma^2}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right)$, $d_5 = \frac{Y\rho^2}{\gamma}\frac{\kappa P^\nu}{\sigma^2} + \frac{\lambda_{rd}(1-\rho^2)}{\gamma}\frac{\kappa P^\nu}{\sigma^2}$ and (a) holds from the fact that $d_1, d_2, d_3, d_4, d_5 \geq 0$, $0 \leq \nu \leq 1$ and $0 \leq \zeta \leq 1$. So, $\frac{\partial\mathcal{L}_1}{\partial\zeta} \leq 0$.

$$\mathbb{E}[\ln(S+1)] = \int_0^\infty \int_{c_2'}^\infty \frac{e^{-\frac{s}{\lambda_{rd}t}-\frac{t-c_2'}{\lambda_{rd}c_4'}}}{\lambda_{rd}^2 c_4' t} \ln(s+1) dt ds$$
$$\overset{(a)}{=} \int_0^\infty \int_{c_2'}^\infty \frac{e^{-\frac{s}{\lambda_{rd}t}-\frac{t-c_2'}{\lambda_{rd}c_4'}}}{\lambda_{rd}^2 c_4' t} G_{2\,2}^{1\,2}\left(s\middle|\begin{matrix}1,1\\1,0\end{matrix}\right) dt ds \overset{(b)}{=} \int_{c_2'}^\infty \frac{e^{-\frac{t-c_2'}{\lambda_{rd}c_4'}}}{\lambda_{rd}c_4'} G_{3\,2}^{1\,3}\left(\lambda_{rd}t\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right) dt$$
$$= \frac{c_2' e^{\frac{c_2'}{\lambda_{rd}c_4'}}}{\lambda_{rd}c_4'}\left[\int_0^\infty e^{-\frac{c_2' t}{\lambda_{rd}c_4'}} G_{3\,2}^{1\,3}\left(\lambda_{rd}c_2' t\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right) dt - \int_0^1 e^{-\frac{c_2' t}{\lambda_{rd}c_4'}} G_{3\,2}^{1\,3}\left(\lambda_{rd}c_2' t\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right) dt\right]$$
$$\overset{(c)}{=} \frac{c_2' e^{\frac{c_2'}{\lambda_{rd}c_4'}}}{\lambda_{rd}c_4'}\left[\int_0^\infty e^{-\frac{c_2' t}{\lambda_{rd}c_4'}} G_{3\,2}^{1\,3}\left(\lambda_{rd}c_2' t\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right) dt - \sum_{i=0}^\infty \frac{(-1)^i {c_2'}^i}{(\lambda_{rd}c_4')^i i!}\int_0^1 t^i G_{3\,2}^{1\,3}\left(\lambda_{rd}c_2' t\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right) dt\right]$$
$$\overset{(d)}{=} e^{\frac{c_2'}{\lambda_{rd}c_4'}}\left[G_{4\,2}^{1\,4}\left(\lambda_{rd}^2 c_4'\middle|\begin{matrix}0,0,1,1\\1,0\end{matrix}\right) - \sum_{i=0}^\infty \frac{(-1)^i {c_2'}^{i+1}}{(\lambda_{rd}c_4')^{i+1} i!} G_{4\,3}^{1\,4}\left(\lambda_{rd}c_2'\middle|\begin{matrix}-i,0,1,1\\1,0,-i-1\end{matrix}\right)\right]. \quad (21)$$

Then, let us check the sign of $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2}$ as

$$\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} = \frac{\partial^2 \mathbb{E}[\ln \Gamma_d{}']}{\partial \zeta^2} = \mathbb{E}\left[\frac{\partial}{\partial \zeta}\left(-\frac{d_3+d_4\nu\zeta^{\nu-1}+d_5(\nu+1)\zeta^\nu}{d_2+d_3\zeta+d_4\zeta^\nu+d_5\zeta^{\nu+1}}\right)\right] > 0. \quad (25)$$

For $\nu = 0$, $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} > 0$ can be easily found. So, we need to check that $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} > 0$ when $\nu = 1$. With complex algebraic manipulation, we can find out that $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} > 0$ if $(d_3+d_4)^2 - 2d_2d_5 > 0$. Then, with the high SNR assumption ($\frac{1}{\gamma^2} \cong 0$), $(d_3+d_4)^2 - 2d_2d_5 \cong (1-\rho^2)^2 Z^2 Y^2 > 0$. Therefore, $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} > 0$.

Likewise, we can prove that $\mathcal{L}_2(\zeta)$ is a decreasing and strictly convex function. If $\Gamma_r = \frac{d_6}{d_7+d_8\zeta}$ is rearranged as a function of ζ with $d_6 = X$, $d_7 = \kappa P^{\nu-1} + 1/\gamma$, $d_8 = \rho^2 Y + (1-\rho^2)Z$, $\mathcal{L}_1 = \mathbb{E}[\ln(\frac{d_6+d_7+d_8\zeta}{d_7+d_8\zeta})]$. Then, with differentiating $\mathcal{L}_2$ by ζ, we can easily check that $\frac{\partial \mathcal{L}_2}{\partial \zeta} \leq 0$ and $\frac{\partial^2 \mathcal{L}_2}{\partial \zeta^2} > 0$.

Now, we show that $\frac{\partial Q(\zeta)}{\partial \zeta} = 0$ has a single positive real root.

$$\frac{\partial Q}{\partial \zeta} = \frac{1}{1+e^{-\mathcal{L}_1}}\frac{\partial \mathcal{L}_1}{\partial \zeta} - \frac{\partial \mathcal{L}_2}{\partial \zeta}. \quad (26)$$

Since $\mathcal{L}_1 \geq 0$ and $\frac{\partial \mathcal{L}_1}{\partial \zeta} \leq 0$, $\frac{1}{1+e^{-\mathcal{L}_1}}$ is bounded between $\frac{1}{2}$ and 1. Previously, we showed that $\frac{\partial \mathcal{L}_1}{\partial \zeta} \leq 0$, $\frac{\partial \mathcal{L}_2}{\partial \zeta} \leq 0$ $\frac{\partial^2 \mathcal{L}_1}{\partial \zeta^2} > 0$ and $\frac{\partial^2 \mathcal{L}_2}{\partial \zeta^2} > 0$. So, it means that $\frac{\partial Q}{\partial \zeta}$ is bounded as follows.

$$\frac{\partial \mathcal{L}_1}{\partial \zeta} - \frac{\partial \mathcal{L}_2}{\partial \zeta} \leq \frac{\partial Q}{\partial \zeta} \leq \frac{1}{2}\frac{\partial \mathcal{L}_1}{\partial \zeta} - \frac{\partial \mathcal{L}_2}{\partial \zeta}. \quad (27)$$

If we can show that both $\frac{\partial \mathcal{L}_1}{\partial \zeta} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0$ and $\frac{1}{2}\frac{\partial \mathcal{L}_1}{\partial \zeta} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0$ for $\nu = 0, 1$ have a single positive root, then $\frac{\partial Q}{\partial \zeta} = 0$ has also the single positive root. Those root-finding equations can only have the form of a cubic equation at the most, under the value of ν, leading to the maximum three of positive roots. But, since $\lim_{\zeta\to\infty} \frac{\partial Q}{\partial \zeta} = 0^-$ and $\frac{\partial Q}{\partial \zeta}\Big|_{\zeta=0} \geq 0$ (we will show in the next stage), one or three positive roots are only possible. And, we show that three positive roots are impossible in the following cubic equation.

$$\frac{\partial \mathcal{L}_1}{\partial \zeta}\Big|_{\nu=1} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = \mathbb{E}\left[\frac{\partial}{\partial \zeta}\left(\ln \Gamma_d{}'\big|_{\nu=1} - \ln(1+\Gamma_r)\right)\right] = 0$$
$$\xrightarrow{\left(\frac{1}{\gamma^2}\cong 0\right)} 2d_5{d_8}^2\zeta^3 + [d_5d_6d_8 + d_4{d_8}^2 + d_3{d_8}^2]\zeta^2 + d_3d_6d_7 - d_2d_6d_8 = 0. \quad (28)$$

Now, let us differentiate (28) to show that the cubic equation has one positive real root.

$$\zeta(6d_5{d_8}^2\zeta + 2(d_5d_6d_8 + d_4{d_8}^2 + d_3{d_8}^2)) = 0. \quad (29)$$

(29) shows that the inflection points of (28) are $-\frac{-2(d_5d_6+d_4d_8+d_3d_8)}{6d_5d_8}$ and 0. Therefore, if the cubic equation has a negative value at $\zeta = 0$, (28) has one positive real root (i.e., $d_3d_6d_7 - d_2d_6d_8 < 0 \xrightarrow{\left(\frac{1}{\gamma^2}\cong 0\right)} 0 < \frac{X}{\gamma}(\rho^2 Y + (1-\rho^2)Z) + \frac{\rho^2 Y^2}{\gamma}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right)$).

Similarly, the existence of one positive real root can be proved for $\frac{1}{2}\frac{\partial \mathcal{L}_1}{\partial \zeta}\Big|_{\nu=1} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0$ case as well.

Now let's look at case $\frac{1}{2}\frac{\partial \mathcal{L}_1}{\partial \zeta}\Big|_{\nu=0} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0$.

$$\frac{1}{2}\frac{\partial \mathcal{L}_1}{\partial \zeta}\Big|_{\nu=0} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0 \xrightarrow{\left(\frac{1}{\gamma^2}\cong 0\right)} (d_3+d_5){d_8}^2\zeta^2 + (2d_3d_7d_8 - d_5d_6d_8 - d_3d_6d_8)\zeta + d_3d_6d_7 - 2d_2d_6d_8 = 0. \quad (30)$$

From the relationship between the roots and coefficients of the quadratic equation, we can obtain the condition to have one positive real root (i.e., $d_3d_6d_7 - 2d_2d_6d_8 < 0 \xrightarrow{\left(\frac{1}{\gamma^2}\cong 0\right)} 0 < \frac{2X}{\gamma}(\rho^2 Y + (1-\rho^2)Z) + \frac{Y}{\gamma}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right)(2\rho^2 Y + (1-\rho^2)Z)$).

Similarly, the existence of one positive real root can be proved for $\frac{\partial \mathcal{L}_1}{\partial \zeta}\Big|_{\nu=0} - \frac{\partial \mathcal{L}_2}{\partial \zeta} = 0$ case as well. Therefore, $\frac{\partial Q(\zeta)}{\partial \zeta} = 0$ has a single positive real root.

Lastly, we show that $\left.\frac{\partial Q}{\partial \zeta}\right|_{\zeta=0} \geq 0$ as follows

$$\left.\frac{\partial Q}{\partial \zeta}\right|_{\zeta=0} = \frac{1}{1+e^{-\mathcal{L}_1(0)}} \left.\frac{\partial \mathcal{L}_1}{\partial \zeta}\right|_{\zeta=0} - \left.\frac{\partial \mathcal{L}_2}{\partial \zeta}\right|_{\zeta=0}. \quad (31)$$

Since $\frac{1}{1+e^{-\mathcal{L}_1(0)}} \leq 0$ and $\frac{\partial \mathcal{L}_1}{\partial \zeta}, \frac{\partial \mathcal{L}_2}{\partial \zeta} \leq 0$, $\left.\frac{\partial Q}{\partial \zeta}\right|_{\zeta=0} \geq 0$ if $\left|\frac{\partial \mathcal{L}_2}{\partial \zeta}\right|_{\zeta=0} \geq \left|\frac{\partial \mathcal{L}_1}{\partial \zeta}\right|_{\zeta=0}$.

$\left|\frac{\partial \mathcal{L}_2}{\partial \zeta}\right|_{\zeta=0} \geq \left|\frac{\partial \mathcal{L}_1}{\partial \zeta}\right|_{\zeta=0}$ can be rewritten as follows

$$\left|\frac{1}{1+\Gamma_r}\frac{\partial \Gamma_r}{\partial \zeta}\right|_{\zeta=0} \geq \left|\frac{1}{\Gamma_d{}'}\frac{\partial \Gamma_d{}'}{\partial \zeta}\right|_{\zeta=0}. \quad (32)$$

With $\nu = 0$, it is typical to prove (32), so we only deal with $\nu = 1$. With complex algebraic manipulation, the inequality of (32) holds if $d_2 d_6 d_8 - d_3 d_6 d_7 - d_3 {d_7}^2 \geq 0$. Then, with high SNR assumption (i.e., $\frac{1}{\gamma^2} \cong 0$), $d_2 d_6 d_8 - d_3 d_6 d_7 - d_3 {d_7}^2 \cong \frac{X\lambda_{sr}}{\gamma}(\rho^2 Y + (1-\rho^2)Z) + \frac{XY^2\rho^2}{\gamma}\left(1+\frac{\kappa P^\nu}{\sigma^2}\right) \geq 0$. So, $\left.\frac{\partial Q}{\partial \zeta}\right|_{\zeta=0} \geq 0$ is proved.

REFERENCES

[1] J. -P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8-11, Jun. 2017.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless Communications: Vision and Potential Techniques," *IEEE Access*, vol. 33, pp. 70-75, 2019.

[3] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[4] K. H. Park, T. Wang, M. S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sep. 2013.

[5] 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.

[6] A. E. 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.

[7] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833-1847, May 2015.

[8] X. He and A. Yener, "Cooperation with an Untrusted Relay: A Secrecy Perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807-3827, Aug. 2010.

[9] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536-2550, May 2013.

[10] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199-2213, Mar. 2017.

[11] M. Chen, T. C.-K. Liu and X. Dong, "Opportunistic multiple relay selection with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 61, no. 3, pp. 1333-1345, Mar. 2012.

[12] K. S. Hwang, M. Ju and M.-S. Alouini, "Outage performance of opportunistic two-way amplify-and-forward relaying with outdated channel state information," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3635-3643, Sep. 2013.

[13] J. Hu, W. Yang, N. Yang, X. Zhou and Y. Cai, "On-off-based secure transmission design with outdated channel state information." *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6075-6088, Sep. 2015.

[14] K. Lee, J. -T. Lim, and H. -H. Choi, "Impact of outdated CSI on the secrecy performance of wireless-powered untrusted relay networks," *IEEE Trans. Inf. Forensics Security.*, vol. 15, pp. 1423-1433, Sep. 2019.

[15] J. -T. Lim, K. Lee, and Y. Han, "Secure communication with outdated channel state information via untrusted relay capable of energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11323-11337, Jul. 2020.

[16] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint Information- and Jamming-Beamforming for Physical Layer Security With Full Duplex Base Station," *IEEE Trans. Sig. Proc.*, vol. 62, no. 24, pp. 6391-6401, Dec. 2014.

[17] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-Layer Security for Full Duplex Communications With Self-Interference Mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329-340, Jan. 2016.

[18] J. -H. Lee, "Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525-528, Apr. 2015.

[19] A. E. Shafie, A. Sultan, and N. Al-Dhabir, "Physical-layer Security of a Buffer-Aided Full-Duplex Relaying System," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1856-1859, Sep. 2019.

[20] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust Resource Allocation to Enhance Physical Layer Security in Systems With Full-Duplex Receivers: Active Adversary," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 885-899, Feb. 2017.

[21] S. Atapattu, P. Dharmawansa, M. Di Renzo, C. Tellambura, and J. S. Evans, "Multi-user relay selection for full-duplex radio," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 955-972, Feb. 2019.

[22] S. Atapattu, N. Ross, T. Jing, Y. He, and J. S. Evans, "Physical-layer Security in Full-Duplex Multi-Hop Multi-User Wireless Network With Relay Selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1216-1232, Feb. 2019.

[23] W. C. Jakes, *Microwave Mobile Communication*, Wiley & Sons, 1974.

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

[25] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed., New York, NY, USA: Academic, 2015.

[26] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 2nd ed., MA: Addison-wesley, 1984.