TAS-Based Incremental Hybrid Decode-Amplify-Forward Relaying for Physical Layer Security Enhancement

Youhong Feng, *Student Member, IEEE*, Shihao Yan, *Member, IEEE*, Zhen Yang, Nan Yang, *Member, IEEE*, and Wei-Ping Zhu, *Senior Member, IEEE*

***Abstract*—In this paper, a transmit antenna selection (TAS)-based incremental hybrid decode-amplify-forward (IHDAF) scheme is proposed to enhance physical layer security in cooperative relay networks. Specifically, TAS is adopted at the source in order to reduce the feedback overhead. In the proposed TAS-based IHDAF scheme, the network transmits signals to the destination adaptive select direction transmission mode, AF mode or DF mode depending on the capacity of the source-relay link and source-relay link. In order to fully examine the benefits of the proposed TAS-based IHDAF scheme, we first derive its secrecy outage probability (SOP) in a closed-form expression. We then conduct asymptotic analysis on the SOP, which reveals the secrecy performance floor of the proposed TAS-based IHDAF scheme when no channel state information is available at the source. Theoretical analysis and simulation results demonstrate that the proposed TAS-based IHDAF scheme outperforms the selective decode-and-forward (SDF), the incremental decode-and-forward (IDF), and the noncooperative direction transmission (DT) schemes in terms of the SOP and effective secrecy throughout, especially when the relay is close to the destination. Furthermore, the proposed TAS-based IHDAF scheme offer a good trade-off between complexity and performance compare with using all antennas at the source.**

***Index Terms*—Physical layer security, cooperative communications, transmit antenna selection, secrecy outage probability.**

I. Introduction

RECENTLY, physical layer security [1–4] as a complementary and alternative cryptographic method to defend against eavesdroppers from information-theoretic perspective has drawn numerous research interests. Physical layer security offers two major advantages relative to the traditional cryptographic method. First, physical layer security is not conditional on the limited computational ability of eavesdroppers, which indicates that the achieved level of secrecy will not be compromised even in the presence of an eavesdropper with unlimited computational capabilities. Second, physical layer security techniques can be used to provide direct secure data transmission, which implies that physical layer security has a high scalability for the decentralized nature of the network [2]. In addition, we note that physical layer security is complementary to the traditional cryptographic techniques (e.g., it can be used to facilitate the distribution of cryptographic keys). To improve the physical-layer security of wireless communications, multiple-input multiple-out (MIMO) architectures [1, 5–9] and cooperative relays [3, 10–15] have been investigated in the context of physical layer security. For example, when the channel state information (CSI) of the eavesdropper is known to the transmitter, the secrecy capacity achieved by beamforming was examined for multiple-input single-output (MISO) wiretap channels [1] and MIMO wiretap channels [8] by considering multiple eavesdroppers. When the CSI of the eavesdropper is unknown to the transmitter, beamforming with artificial noise is desirable in MISO or MIMO wiretap channels due to its robustness [5, 9]. As shown in the literature, such beamforming techniques can effectively improve the secrecy performance of wiretap channels [5, 9]. However, these beamforming methods require precise CSI of the main channel, which incurs high feedback overhead and computational cost of signal processing. Moreover, the front-end and the radio frequency (RF) modules of a multi-antenna transmitter have a complex hardware structure, which are expensive to implement. To avoid the high feedback overhead and complex hardware structure, transmit antenna selection (TAS) has been applied at the multi-antenna transmitter to enhance physical layer security [6]. TAS offers the following benefits relative to beamforming in the context of physical layer security. First, it requires less feedback overhead and a single RF chain, which leads to the fact that the feedback overhead and the computational complexity of TAS is much lower than that of beamforming. Second, the index of the selected transmit antenna, which is returned from the destination to the transmitter over the feedback channel, is meaningless to the eavesdropper which cannot be exploited to improve her eavesdropping capability [7].

Manuscript received October 10, 2016; revised February 19, 2017 and May 13, 2017. The editor coordinating the review of this paper and approving it for publication was Y.-W. P. Hong.

This work was partially supported by the National Natural Science Foundation of China (No. 61671252, 61571233, 61501251), the Key Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 14KJA510003), and the Australian Research Council Discovery Project (DP150103905).

Y. Feng and Z. Yang are with the Key Laboratory of Ministry of Education in Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: {2013010213, yangz}@njupt.edu.cn). Y. Feng is also with the College of Physics and Electronic information Engineering, Anhui Normal University, Wuhu 241000, China.

S. Yan and N. Yang are with the Research School of Engineering, Australian National University, Canberra, ACT, Australia (emails: {shihao.yan, nan.yang}@anu.edu.au).

W.-P. Zhu is with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada (e-mail: weiping@ece.concordia.ca). He is also an Adjunct Professor with the School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China.

Apart from the aforementioned studies, which have examined physical layer security of point-to-point MIMO systems, the physical layer security of relay-aided networks has also drawn increasing attention [3, 10–15]. This is due to the fact that wireless relaying has been recognized as an effective means to improve the coverage and reliability of mobile networks. In this context, the secrecy performance of cooperative transmissions, such as decode-and-forward (DF) [10, 11, 16] and amplify-and-forward (AF) [12, 13, 15, 17], has been examined in the literature. The secrecy performance of DF relay selection scheme was examined by considering different combining techniques and different CSI assumptions in [15] and [16] , respectively. Meanwhile, the authors of [17] analyzed the secrecy performance of dual-hop AF relaying systems by taking into account the availability of direct link over Rayleigh fading channels, in which two linear processing schemes (i.e., zero-forcing and maximal ratio transmission) at the relay were proposed to enhance the security of the considered system. In the AF scheme, the relay simultaneously amplifies the information and noise, which leads to the propagation of noise and interference. In the DF scheme, the relay first decodes the received signals and then retransmits the recovered signals to the destination, which often imposes a higher signal processing burden on the relay. Another drawback of DF scheme is that the relay may forward signals with decoding errors to the destination. Motivated by the aforementioned benefits of TAS, the impact of antenna selection at the multi-antenna relay on the secrecy performance of one-way and two-way cooperative relaying networks was studied in [13] and [14], respectively.

More recently, in [11], the secrecy outage probabilities (SOPs) of the selective decode-and-forward (SDF) and the incremental decode-and-forward (IDF) schemes were analysed, where no CSI is available and TAS is performed at the source. In the SDF scheme, the relay operates in DF mode regardless of whether the information from the source can be successfully decoded at the destination. In the IDF scheme, the relay operates in DF mode only when the source's information cannot be decoded at the destination in the direction transmission (DT) mode but can be correctly decoded at the relay. As shown in [18], the IDF and SDF schemes achieve the same performance without considering physical layer security. Meanwhile, the analysis in [11] shows that IDF scheme outperforms the SDF scheme in the context of physical layer security while the secrecy performance of these two schemes is not desirable (i.e., their SOPs are very high) when the relay is close to the destination.

In order to achieve the benefits offered by both the DF and AF schemes, a new adaptive hybrid relaying scheme (without considering security), in which the relay switches between AF and DF modes based on its decoding capability, was proposed in [19]. In addition, a similar hybrid relaying scheme for multiple relays was proposed and the performance gain in terms of achieving a lower symbol error probability was analyzed in [20]. In order to enhance the information transmission security, the authors of [21] proposed an incremental hybrid decode-amplify (IHDAF) scheme based on the signal-to-noise ratio (SNR) thresholds at the relay and destination in a single-antenna communication scenario. In this IHDAF scheme, the relay operates in the AF mode when neither the destination nor the relay can decode the information from the source directly. It is shown in [21] that the IHDAF scheme significantly outperforms both the SDF and IDF schemes as it achieves a lower outage probability or bit error rate. However, the IHDAF scheme has never been utilized to achieve physical layer security and its secrecy performance relative to the SDF and IDF schemes has never been studied. The lack of the secrecy performance study of the hybrid cooperative transmissions in the literature and how to further improve the secrecy performance of SDF and IDF schemes when the relay is close to the destination motivate this work. Our main contributions are summarized as follows:

- In the present work, for the first time, we propose a TAS-based IHDAF scheme to enhance physical layer security in cooperative relay networks. In this scheme the source transmits signals directly to the destination when such signals can be successfully decoded and the relay keeps silent. Otherwise, the source transmits signals to the destination with the aid of a relay, which operates in either DF or AF mode, depending whether or not the relay can decode the source's signals. In addition, an efficient TAS scheme is adopted at the source, aiming to avoid high feedback overhead, high hardware complexity, and complicated cooperations.
- In order to fully examine the secrecy performance of the proposed scheme, we first derive a closed-form expression for its SOP. For the sake of comparison, we also examine the secrecy performance of the traditional IDF, SDF, and DT schemes in our considered system model (multi-antenna communication scenario with TAS scheme). Our examination shows that the proposed scheme significantly outperforms the (TAS-based) IDF, SDF, and DT schemes in terms of achieving a lower SOP, especially when the relay is close to the destination. We also conduct asymptotic analysis on the SOP of the proposed scheme with the SDF and IDF schemes as benchmarks. This asymptotic analysis discloses the SOP floor of the proposed scheme that is lower than or equal to that of the SDF and IDF schemes, which analytically confirms the advantages of our proposed scheme.
- We also examine the effective secrecy throughput (EST) of the proposed scheme by incorporating the different time slots incurred in the direct and cooperative transmissions. Our examination reveals that the proposed scheme achieves a higher EST relative to other schemes. In order to study the efficiency of the proposed scheme in terms of the feedback overhead, we compare it with a codebook-based beamforming (CB) scheme. Surprisingly, our study indicates that our proposed scheme can outperform the CB scheme with less feedback overhead and fewer RF chains.

Notation: Scalar variables are denoted by italic symbols; Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively; $X \sim \mathit{CN}(\mu, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable X with mean μ and covariance σ^2; $\Pr[\cdot]$ is the probability; $f_X(\cdot)$

and $F_X(\cdot)$ represent the probability density function (PDF) and cumulative distribution function (CDF) of the random variable X, respectively.

II. System Model and TAS-based IHDAF Scheme

A. System Model

In this work, we consider a half-duplex relay network as illustrated in Fig. 1, in which an N_{S}-antenna source (S) communicates with an N_{D}-antenna destination (D) with the aid of a single-antenna relay (R) in the presence of an N_{E}-antenna eavesdropper (E). We clarify that the communication between S and D can be conducted via both the direct link and relay link. In this network, we assume that only the receiver knows the CSI of corresponding channels (i.e., R knows the CSI of the S-R link, D knows the CSI of the R-D and S-D links, and E knows the CSI of the S-E and R-E links). We also assume that the feedback capability of each legitimate link (i.e., S-D, R-D, and S-R) is limited and the receiver cannot feed back the full CSI of each link to the corresponding transmitter (i.e., the transmitter does not know the CSI of each link). Furthermore, we consider a passive eavesdropping scenario, in which E does not feed back the CSI of the S-E and R-E links and thus such CSI is unknown to other nodes. Meanwhile, in this work we consider a multi-antenna E, who applies maximal radio combining (MRC) to maximize the probability of the successful eavesdropping.[1] We note that multiple antennas may not be available at the relay in this system due to the constraints by the hardware size or implementing cost. Therefore, this system is generally applicable to many practical wireless communication scenarios. For example, in the emerging Internet of Things the far departed nodes may exchange information with the aid of a single-antenna relay [22]. In addition, this system can be found in device-to-device (D2D) communication scenarios where a single-antenna relay assists two multi-antenna devices to communication with each other [11, 21–25]. Furthermore, we consider the similar scenario adopted in [4, 11, 16, 17, 26], where both the direct links S-D and S-E are assumed to be existent, and E can intercept the data from both the S and R.

We denote $\mathbf{H} \in \mathcal{C}^{N_D \times N_S}$ as the channel matrix between S and D, and $\mathbf{G} \in \mathcal{C}^{N_E \times N_S}$ as the channel matrix between S and E. The entries of $\mathbf{H}$ and $\mathbf{G}$ are independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance. In this network, we adopt the TAS scheme at S, in which the antenna that maximizes the instantaneous SNR of the S-D link is selected as active [6]. As such, the index of the selected antenna, n^* is determined by[2]

$$n^* = \arg \max_{1 \le n \le N_S} \|\mathbf{h}(n)\|, \tag{1}$$

where $\mathbf{h}(n)$ denotes the nth column of $\mathbf{H}$. We highlight that the strongest antenna selected by the TAS scheme is equivalent to a random source antenna for E, since this antenna is solely determined by $\mathbf{H}$, which is uncorrelated with $\mathbf{G}$. Thus, E cannot exploit any diversity benefits from multiple source antennas [11]. Furthermore, using TAS method at the multi-antenna transmitter can enhance security and reduce hardware complexity [7]. Also, we assume that MRC is adopted at D to maximize the quality of the received signal.

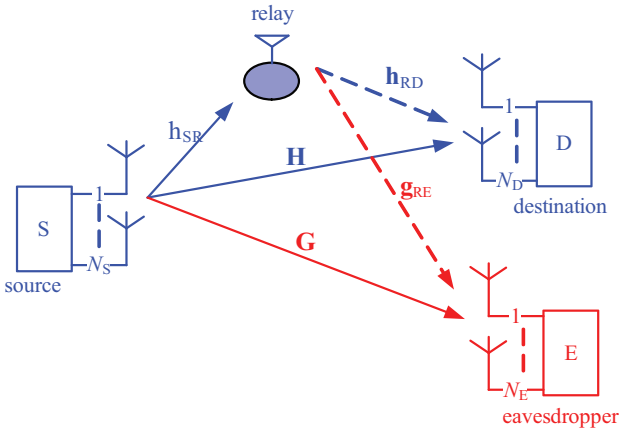


Fig. 1. The illustration of a half-duplex cooperative relay network in the presence of an N_E-antenna eavesdropper.

B. TAS-based IHDAF Scheme for Physical Layer Security

The operation of the TAS-based IHDAF scheme in the considered network is shown in Fig. 2 [21]. With this scheme, the network operates in two phases, namely, the broadcast phase and the cooperative phase. In the broadcast phase, as represented by the solid lines in Fig. 1, if the capacity of the S-D link exceeds the codeword rate R_c, the network adopts DT mode and R keeps silent. Otherwise, the network operates in the cooperative phase (i.e., as represented by the dash lines in Fig. 1) and R helps the transmission from S to D. Differing from the conventional IDF scheme, R operates in either the DF mode or the AF mode, according to the capacity of the S-R link. Specifically, if the capacity of the S-R link, C_{SR}, exceeds the codeword rate R_c, R operates in the DF mode and thus, decodes the received signal and retransmits it towards D. Otherwise, R operates in the AF mode to amplify and forward the received signal to D.

In the considered network, the TAS-based IHDAF scheme can be interpreted as follows: S is equipped with N_{S} antennas and employs a TAS scheme, in which D selects the *strongest* antenna (among the N_{S} available antennas) which maximizes the instantaneous SNR of S-D link, and then informs the index of the strongest antenna through an open error-free feedback

[1] It is noted that, in this work we consider a multi-antenna E, who knows the CSI of the S-E and R-E links, and then applies MRC to maximize the probability of the successful eavesdropping. As such, this multi-antenna E can also be interpreted as multiple colluding Es that cooperatively decode the desired information. Therefore, the operation of the proposed scheme does not change in order to address physical layer security in the colluding eavesdropping scenario.

[2] Here, D selects the "strongest" antenna (among the N_S available antennas at S) which maximizes the instantaneous SNR of S-D link, and then informs the index of the strongest antenna through an open error-free feedback channel to S.

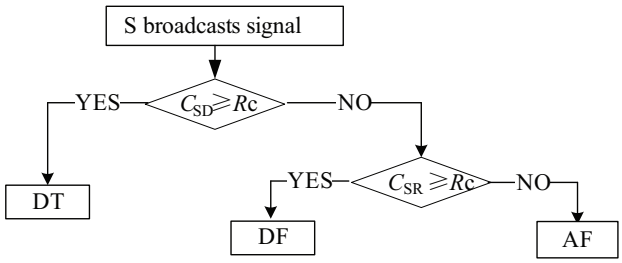


Fig. 2. Signal processing diagram of the TAS-based IHDAF scheme in cooperative relay networks

channel to S. Then D decides whether it can decode the information sent from S according to the instantaneous SNR of the S-D link. If yes, D informs R to keep silent and S to adopt the DT mode. Otherwise, D informs R to be active and R to choose either the DF mode or the AF mode, according to the capacity of the S-R link.

We now formulate the broadcast phase and the cooperation phase of the TAS-based IHDAF scheme in the presence of eavesdropping as follows:

1) Broadcast phase: When the coded confidential information x is sent by S, the signal received at R, D, and E are given by

$$y_{\text{SR}} = \sqrt{k_{\text{SR}}P}\, h_{\text{SR}}\, x + n_{\text{R}}, \tag{2}$$

$$\mathbf{y}_{\text{SD}} = \sqrt{k_{\text{SD}}P}\, \mathbf{h}\, x + \mathbf{n}_{\text{D}}, \tag{3}$$

and

$$\mathbf{y}_{\text{SE}} = \sqrt{k_{\text{SE}}P}\, \mathbf{g}\, x + \mathbf{n}_{\text{E}}, \tag{4}$$

respectively, where h_{SR} denotes the channel coefficient from the selected transmit antenna of S to R, i.e., $h_{\text{SR}} \triangleq \mathbf{h}_{\text{SR}}(n^*)$, $\mathbf{h}$ is an $N_{\text{D}} \times 1$ vector representing the channel coefficients from the selected transmit antenna of S to D, i.e., $\mathbf{h} \triangleq \mathbf{H}(:, n^*)$, and $\mathbf{g}$ is an $N_{\text{E}} \times 1$ vector representing the channel coefficients from the selected transmit antenna of S to E, i.e., $\mathbf{g} \triangleq \mathbf{G}(:, n^*)$. In (2)–(4), P is the transmit power of S, and we denote $k_{mn} = K\left(\frac{d_0}{d_{mn}}\right)^v$ as the path-loss between nodes m and n, d_{mn} is the distance between the m and n, where $m \in \{\text{S}, \text{R}\}$, $n \in \{\text{R}, \text{D}, \text{E}\}$, and $m \neq n$ [27], d_0 is a reference distance, v is the path loss exponent, and $K = \left(\frac{\lambda}{4\pi d_0}\right)^2$ is the free-space path loss at d_0, where λ is the wavelength. We also denote n_{R}, $\mathbf{n}_{\text{D}}$ and $\mathbf{n}_{\text{E}}$ as the additive white Gaussian noise (AWGN) at R, D, and E, respectively. We assume that $n_{\text{R}} \sim CN(0, \sigma_{\text{R}}^2)$, $\mathbf{n}_{\text{D}} \sim CN(\mathbf{0}, \sigma_{\text{D}}^2 \mathbf{I}_{N_{\text{D}}})$, and $\mathbf{n}_{\text{E}} \sim CN(\mathbf{0}, \sigma_{\text{E}}^2 \mathbf{I}_{N_{\text{E}}})$.

We assume that E adopts MRC to combine her received signals from different antennas. Based on (2), (3), and (4), the instantaneous SNRs of the S-R, S-D, and S-E links are given by

$$\rho_{\text{SR}} = |h_{\text{SR}}|^2 \Omega_{\text{SR}} = |h_{\text{SR}}|^2 \frac{k_{\text{SR}}P}{\sigma_{\text{R}}^2}, \tag{5}$$

$$\tilde{\rho}_{\text{SD}} = ||\mathbf{h}||^2 \Omega_{\text{SD}} = ||\mathbf{h}||^2 \frac{k_{\text{SD}}P}{\sigma_{\text{D}}^2}, \tag{6}$$

and

$$\rho_{\text{SE}} = ||\mathbf{g}||^2 \Omega_{\text{SE}} = ||\mathbf{g}||^2 \frac{k_{\text{SE}}P}{\sigma_{\text{E}}^2}, \tag{7}$$

respectively, where Ω_{mn} is the average SNR of the $m-n$ link. Then, the channel capacity between m and n is written as

$$C_{mn} = \log_2(1 + \rho_{mn}). \tag{8}$$

Given the target information transmit rate as R_c in bits per channel use (bpcu), transmission outage occurs when C_{mn} falls below R_c [11, 28].

2) Cooperation phase: We note that R operates in either the DF mode or the AF mode in the TAS-based IHDAF Scheme. According to Shannon's channel theorem, R can successfully decode x with an ignorable error probability when $C_{SR} > R_c$ (i.e., when R operates in the DF mode) [3]. As such, when R operates in the DF mode, the signals received at D and E are written as

$$\mathbf{y}_{\text{RD}} = \sqrt{k_{\text{RD}}P}\, \mathbf{h}_{\text{RD}}\, x + \mathbf{n}_{\text{RD}}, \tag{9}$$

$$\mathbf{y}_{\text{RE}} = \sqrt{k_{\text{RE}}P}\, \mathbf{g}_{\text{RE}}\, x + \mathbf{n}_{\text{RE}}, \tag{10}$$

where $\mathbf{h}_{\text{RD}} \in \mathcal{C}^{N_{\text{D}} \times 1}$ and $\mathbf{g}_{\text{RE}} \in \mathcal{C}^{N_{\text{E}} \times 1}$ represent the channel coefficient vector from R to D and that from R to E, respectively. The entries of $\mathbf{h}_{\text{RD}}$ and $\mathbf{g}_{\text{RE}}$ are i.i.d. complex Gaussian random variables with zero mean and unit variance. When R operates in the AF mode, the signals received at D and E can be written as

$$\mathbf{y}_{\text{RD}} = \beta\, \mathbf{h}_{\text{RD}}\, y_{SR} + \mathbf{n}_{\text{RD}}, \tag{11}$$

$$\mathbf{y}_{\text{RE}} = \gamma \sqrt{k_{\text{RE}}P}\, \mathbf{h}_{\text{RE}}\, y_{\text{SR}} + \mathbf{n}_{\text{RE}}, \tag{12}$$

where the amplification coefficients β and γ are given by $\beta = \frac{\sqrt{k_{\text{RD}}P}}{\sqrt{k_{\text{RD}}P|h_{\text{SR}}|^2 + \sigma_{\text{R}}^2}}$ and $\gamma = \frac{\sqrt{k_{\text{RE}}P}}{\sqrt{k_{\text{RE}}P|h_{\text{SR}}|^2 + \sigma_{\text{R}}^2}}$, respectively [29]. Then, the instantaneous SNRs of the R-D and R-E links are given by $\rho_{\text{RD}} = ||\mathbf{h}_{\text{RD}}||^2 \Omega_{\text{RD}}$ and $\rho_{\text{RE}} = ||\mathbf{h}_{\text{RD}}||^2 \Omega_{\text{RE}}$, respectively, where $\Omega_{\text{RD}} = \frac{k_{\text{RD}}P}{\sigma_{\text{D}}^2}$ and $\Omega_{\text{RE}} = \frac{k_{\text{RE}}P}{\sigma_{\text{E}}^2}$ denote the average SNR of the R-D and that of R-E links, respectively. In the cooperation phase, D combines the signals from both the direct link and R link using MRC. This leads to the capacity at D in the DF mode and in the AF mode as [11, 21]

$$C_{\text{SRD}}^{\text{DF}} = \log_2(1 + \rho_{\text{SRD}}^{DF}) = \log_2(1 + \tilde{\rho}_{\text{SD}} + \rho_{\text{RD}}), \tag{13}$$

$$C_{\text{SRD}}^{\text{AF}} = \log_2\left(1 + \rho_{\text{SRD}}^{AF}\right) = \log_2\left(1 + \tilde{\rho}_{\text{SD}} + \frac{\rho_{\text{SR}}\rho_{\text{RD}}}{\rho_{\text{SR}} + \rho_{\text{RD}} + 1}\right), \tag{14}$$

where ρ_{SRD}^{DF} and ρ_{SRD}^{AF} represent the instantaneous SNRs at D for the DF mode and AF mode, respectively. Similarly, the capacities at E in the DF mode and in the AF mode are given by

$$C_{\text{SRE}}^{\text{DF}} = \log_2(1 + \rho_{\text{SRE}}^{DF}) = \log_2(1 + \rho_{\text{SE}} + \rho_{\text{RE}}), \tag{15}$$

$$C_{\text{SRE}}^{\text{AF}} = \log_2\left(1 + \rho_{\text{SRE}}^{AF}\right) = \log_2\left(1 + \rho_{\text{SE}} + \frac{\rho_{\text{SR}}\rho_{\text{RE}}}{\rho_{\text{SR}} + \rho_{\text{RE}} + 1}\right), \tag{16}$$

where ρ_{SRE}^{DF} and ρ_{SRE}^{AF} represent the instantaneous SNRs at E for the DF and AF modes, respectively.

C. Performance Metric

In [1, 30], the notion of SOP was introduced in the quasi-static Rayleigh fading wiretap channel. If the CSI of the legitimate link is assumed to be perfectly known by S, the overall codeword rate R_c can be dynamically chosen as $R_c = C_b$, where C_b is the instantaneous capacity of the legitimate link. We note that perfect secrecy cannot be always guaranteed in the passive eavesdropping scenario since there exists a possibility that some messages transmitted by S are leaked to E, and for this reason we define a secrecy rate R_s, which is usually fixed. The difference between R_c and R_s, i.e., $R_e = R_c - R_s$, is the redundant rate that provides secrecy against eavesdropping. The SOP is thus defined as $\Pr\{C_b - R_s < C_e\}$, where C_e is the instantaneous capacity of E's channel [11]. Note that the transmission outage does not occur when the value of R_c is chosen to be equal to C_b. However, we now study a special case where S does not know the CSI about both D and E. In this scenario, since C_b is not known, to study the secrecy performance, we must choose a fixed overall codeword rate R_c and a fixed rate redundancy R_e, yielding a fixed secure rate $R_s = R_c - R_e$. Therefore, the SOP is the union of two events, i.e., C_b falls below R_c or R_e falls below C_e, which is expressed as [11]

$$P_{so} = \Pr\{(C_b < R_c) \cup (C_e > R_e)\}, \tag{17}$$

where $\Pr(C_b < R_c) \triangleq P_b$ denotes the probability of the reliability outage event, and $\Pr(C_e < R_e) \triangleq P_e$ refers to the secrecy outage event [11].

III. Exact Secrecy Outage Probability Analysis of TAS-based IHDAF Scheme

In this section, we present a comprehensive analysis on the SOP for cooperative relay networks with perfect and outdated CSI.

A. Preliminaries

In practical systems, the TAS phase may exceed the coherent time of the channel. As a result, the main channel may have already changed since the moment when S receives the feedback of the optimal antenna index due to the time-varying nature of the wireless channel. In this case, the optimal antenna is selected based on the outdated CSI. Let $\mathbf{h}(t-\tau)$ denote the τ time-delayed version of current CSI (i.e., $h(t)$). The relationship between $\mathbf{h}(t-\tau)$ and $\mathbf{h}(t)$ can be modeled as $\mathbf{h}(t) = \sqrt{\rho}\mathbf{h}(t-\tau) + \sqrt{1-\rho}\mathbf{e}(t)$ [31, 32], where $\mathbf{e}(t) \sim CN(0, \mathbf{I}_{N_D})$ denotes the channel error vector and $\rho = [J_0(2\pi f t)]^2$ is the correction coefficient between $\mathbf{h}(t-\tau)$ and $\mathbf{h}(t)$, with f as the maximum Doppler frequency and $J_0(\cdot)$ as the zeroth-order Bessel function of the first kind [33, Eq. (8.411)].

We denote $\tilde{X} = \tilde{\rho}_{\text{SD}} = ||\mathbf{h}(t)||^2\Omega_{\text{SD}}$ and $X = \rho_{\text{SD}} = ||\mathbf{h}(t-\tau)||^2\Omega_{\text{SD}}$ as the current SNR and the time-delayed SNR, respectively. The PDF of the $\tilde{\rho}_{\text{SD}}$ is given by [34]

$$f_{\tilde{X}}(\tilde{x}) = \int_0^\infty f_{\tilde{X}|X}(\tilde{x}|x) f_X(x) dx, \tag{18}$$

where $f_{\tilde{X}|X}(\cdot)$ denotes the PDF of $\tilde{\rho}_{\text{SD}}$ conditioned on ρ_{SD}, given by [35]

$$f_{\tilde{X}|X}(\tilde{x}|x) = \frac{1}{(1-\rho)\Omega_{SD}} \left(\frac{\tilde{x}}{\rho x}\right)^{\frac{N_D-1}{2}} e^{-\frac{\rho x + \tilde{x}}{(1-\rho)\Omega_{SD}}} \times \mathbf{I}_{N_D-1}\left(\frac{2\sqrt{\rho x \tilde{x}}}{(1-\rho)\Omega_{SD}}\right), \tag{19}$$

and $I_n(\cdot)$ is the $n-$th modified Bessel function of the first kind [33, Eq. (8.406.1)]. The PDF of X is given by [31]

$$f_X(x) = \frac{N_{\text{S}}}{(N_{\text{D}}-1)!} \sum_{i=0}^{N_{\text{S}}-1} (-1)^i \binom{N_{\text{S}}-1}{i} e^{-\frac{(i+1)x}{\Omega_{\text{SD}}}} \times \sum_{j=0}^{i(N_{\text{D}}-1)} \frac{\xi_{ji} x^{j+N_{\text{D}}-1}}{\Omega_{\text{SD}}^{j+N_{\text{D}}}}, \tag{20}$$

where $\xi_{ji} = \sum_{x=a}^{b} \frac{\xi_{j(i-1)}}{(j-x)!}$, with $a = \max\{0, j-(N_{\text{D}}-1)\}$, $b = \min\{j, (i-1)(N_{\text{D}}-1)\}$, $\xi_{j0} = \xi_{0i} = 1$, $\xi_{j1} = \frac{1}{j!}$, and $\xi_{1i} = i$. Substituting (20) and (19) into (18), we can respectively obtain the PDF and CDF of $\tilde{X}$ as

$$f_{\tilde{X}}(\tilde{x}) = \frac{N_{\text{S}}}{(N_{\text{D}}-1)!} \sum_{i=0}^{N_{\text{S}}-1} \sum_{j=0}^{i(N_{\text{D}}-1)} \sum_{k=0}^{j} \Xi(i,j,k,\Omega_{\text{SD}}) \times \tilde{x}^{k+N_{\text{D}}-1} e^{-\frac{(i+1)\tilde{x}}{(i(1-\rho)+1)\Omega_{\text{SD}}}}, \tag{21}$$

and

$$F_{\tilde{X}}(\tilde{x}) = \frac{N_{\text{S}}}{(N_{\text{D}}-1)!} \sum_{i=0}^{N_{\text{S}}-1} \sum_{j=0}^{i(N_{\text{D}}-1)} \sum_{k=0}^{j} \Xi(i,j,k,\Omega_{\text{SD}}) \times \frac{\Gamma_1\left(k+N_D, \frac{(i+1)\tilde{x}}{(i(1-\rho)+1)\Omega_{\text{SD}}}\right)}{\left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\text{SD}}}\right)^{k+N_D}}, \tag{22}$$

with

$$\Xi(i,j,k,\Omega_{\text{SD}}) = \binom{N_{\text{S}}-1}{i}\binom{j}{k} \frac{(j+N_D-1)!}{(k+N_D-1)!} \frac{(-1)^i \xi_{ji} \rho^k (1-\rho)^{j-k}}{(i(1-\rho)+1)^{j+k+N_D} \Omega_{\text{SD}}^{k+N_{\text{D}}}}, \tag{23}$$

where $\Gamma_1(\alpha, x) = \int_0^x e^{-t} t^{\alpha-1} dt$ is the lower incomplete Gamma function [33, Eq. (8.350.1)].

In the case of $\rho = 1$, which corresponds to the case with $\tau = 0$, i.e., perfect feedback without delay, (21) is identical to (20) and (22) is identical to $F_{\tilde{X}}(\tilde{x})|_{\rho=1} = \left[1 - \frac{\Gamma(N_D, \frac{\tilde{x}}{\Omega_{SD}})}{\Gamma(N_D)}\right]^{N_S}$.

B. Secrecy Outage Probability Analysis for Outdated CSI

In this section, we analyze the SOP of the proposed TAS-based IHDAF scheme. As shown in Fig. 2, in the cooperative phase of the proposed TAS-based IHDAF scheme, R adaptively selects AF mode or DF mode due to the incremental nature of the proposed scheme (which is different from the SDF and IDF schemes). As such, to derive the overall SOP of the proposed TAS-based IHDAF scheme, we have to consider the following three mutually exclusive events. i) The information transmitted from S is successfully decoded by D in the DT

mode, where R keeps silent. ii) S's transmission failed at D in the DT mode, but R decoded it correctly and operates in DF mode to retransmit it to D. iii) Neither D nor R can decode the information from S correctly i.e., the capacities of both the S-R link and the S-D link are lower than R_c, and then R operates in the AF mode to amplify and forward the information to D. As per the rules of the proposed TAS-based IHDAF scheme (as shown in Fig. 2), the probability that S operates in the DT mode is $\Pr\{C_{\rm SD}\geq R_c\}$, the probability that R operates in the DF mode is $\Pr\{C_{\rm SR}\geq R_c\}\Pr\{C_{\rm SD}<R_c\}$, and the probability that R operates in the AF mode is $\Pr\{C_{\rm SR}<R_c\}\Pr\{C_{\rm SD}<R_c\}$. Then, the SOPs of the three mutually exclusive events are given by

$$P_{out}^{\rm DT} = \Pr\{(C_{\rm SD} < R_c) \cup (C_{\rm SE} \geq R_e)|(C_{\rm SD} \geq R_c)\} \times \Pr\{C_{\rm SD} \geq R_c\}, \quad (24)$$

$$P_{out}^{\rm DF} = \Pr\{(C_{\rm SRD}^{\rm DF} < R_c) \cup (C_{\rm SRE}^{\rm DF} \geq R_e)|(C_{\rm SD} < R_c, C_{\rm SR} \geq R_c)\} \times \Pr\{C_{\rm SD} < R_c, C_{\rm SR} \geq R_c\}, \quad (25)$$

and

$$P_{out}^{\rm AF} = \Pr\{(C_{\rm SRD}^{\rm AF} < R_c) \cup (C_{\rm SRE}^{\rm AF} \geq R_e)|(C_{\rm SD} < R_c, C_{\rm SR} < R_c)\} \times \Pr\{C_{\rm SD} < R_c, C_{\rm SR} < R_c\}, \quad (26)$$

respectively. Therefore, we can express the SOP of the TAS-based IHDAF scheme as

$$P_{\rm IHDAF} = P_{out}^{\rm DT} + P_{out}^{\rm DF} + P_{out}^{\rm AF}. \quad (27)$$

In the following, we sequentially derive the expressions for $P_{out}^{\rm DT}$, $P_{out}^{\rm DF}$, and $P_{out}^{\rm AF}$ in Theorem 1, Theorem 2, and Theorem 3, respectively.

***Theorem** 1:* The SOP in the first sub-case (i.e., the SOP of DT mode without considering the cooperation transmission mode of R) is given by

$$P_{out}^{\rm DT} = \frac{\Gamma(N_{\rm E}, \frac{T_e}{\Omega_{\rm SE}})}{\Gamma(N_{\rm E})}\Bigg[1 - \sum_{i=0}^{N_{\rm S}-1}\sum_{j=0}^{i(N_{\rm D}-1)}\sum_{k=0}^{j}\frac{N_{\rm S}\Xi(i,j,k,\Omega_{\rm SD})}{(N_{\rm D}-1)!} \times \frac{\Gamma_1\left(k+N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)}{\left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)^{k+N_D}}\Bigg], \quad (28)$$

where $T = 2^{R_c} - 1$ and $T_e = 2^{R_e} - 1$, and $\Gamma(\alpha, x) = \int_x^{+\infty} e^{-t}t^{\alpha-1}dt$ is the upper incomplete gamma function [33, Eq. (8.350.2)], and $\Gamma(y) = \int_0^{+\infty} e^{-t}t^{y-1}dt$ is the gamma function [33, Eq. (8.310.1)].

Proof: Following (24), we have

$$\begin{aligned} &P_{out}^{\rm DT} \\ &= \Pr\{(C_{\rm SD} < R_c) \cup (C_{\rm SE} \geq R_e)|(C_{\rm SD} \geq R_c)\}\Pr\{C_{\rm SD} \geq R_c\} \\ &= \Pr\{C_{\rm SE} \geq R_e|(C_{\rm SD} \geq R_c)\}\Pr\{C_{\rm SD} \geq R_c\} \\ &= \Pr\{C_{\rm SE} \geq R_e\}\left(1 - \Pr\{C_{\rm SD} < R_c\}\right), \end{aligned} \quad (29)$$

where we have applied the fact that $\Pr\{(C_{\rm SD} < R_c)|(C_{\rm SD} \geq R_c)\} = 0$ and $C_{\rm SE} \geq R_e$ is independent of $C_{\rm SD} \geq R_c$.

According to the discussion in Section-II, from E's point of view, the optimum TAS scheme for D will be a random TAS for E, as the main channel and E' channel are uncorrelated. Then, based on (7), we can obtain the CDFs of $\rho_{\rm SE}$ [29]. (i.e., $F_{\rho_{\rm SE}}(x) = \left[1 - \frac{\Gamma(N_E, \frac{x}{\Omega_{SE}})}{\Gamma(N_E)}\right]$). As such, we can achieve

$$\Pr\{C_{\rm SE} \geq R_e\} = \Pr\{\log_2(1+\rho_{\rm SE}) \geq R_e\} = \frac{\Gamma(N_{\rm E}, \frac{T_e}{\Omega_{\rm SE}})}{\Gamma(N_{\rm E})}. \quad (30)$$

In additional, based on (6) and (22), we can achieve

$$\begin{aligned} \Pr\{C_{\rm SD} < R_c\} &= \Pr\{\log_2(1+\tilde{\rho}_{\rm SD}) < R_c\} \\ &= \sum_{i=0}^{N_{\rm S}-1}\sum_{j=0}^{i(N_{\rm D}-1)}\sum_{k=0}^{j}\frac{N_{\rm S}\Xi(i,j,k,\Omega_{\rm SD})}{(N_{\rm D}-1)!} \\ &\quad \times \frac{\Gamma_1\left(k+N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)}{\left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)^{k+N_D}}. \end{aligned} \quad (31)$$

Substituting (30) and (31) into (29), we achieve the desired result in (28). ■

***Remark** 1:* In the case of single receive antenna and TAS based on perfect feedback, i.e., $N_{\rm D} = 1$ and $\rho = 1$, we can obtain the corresponding SOP from (28) as

$$P_{out}^{\rm DT} = \frac{\Gamma(N_{\rm E}, \frac{T_e}{\Omega_{\rm SE}})}{\Gamma(N_{\rm E})}\left[1 - \left(1 - e^{-\frac{T}{\Omega_{\rm SD}}}\right)^{N_{\rm S}}\right], \quad (32)$$

which is a generalization of [11, Eq. (33)]. In other words, [11, Eq. (33)] can be regarded as a special cases of Theorem 1 in (28).

***Theorem** 2:* The SOP for the DF relaying cooperative transmission mode is given by (33), as shown at the top of the next page.

Proof: The proof is presented in Appendix A. ■

***Remark** 2:* In the case of single receive antenna and TAS based on perfect feedback, i.e., $N_{\rm D} = 1$ and $\rho = 1$, we can obtain the corresponding SOP by (25), which is a generalization of [11, Eq. (35)]. In other words, [11, Eq. (35)] can be regarded as a special cases of Theorem 2.

As neither D nor R received the message from S correctly, instead of remaining silent during the cooperation phase in the IDF scheme [11], the proposed TAS-based IHDAF scheme will employ AF relaying cooperation to improve the system secrecy performance. In this case, the SOP of the third sub-case can be given by

$$P_{out}^{\rm AF} = \Pr\{(C_{\rm SRD}^{\rm AF} < R_c) \cup (C_{\rm SRE}^{\rm AF} > R_e)|(C_{\rm SD} < R_c, C_{\rm SR} < R_c)\} \times \Pr\{C_{\rm SD} < R_c, C_{\rm SR} < R_c\}, \quad (39)$$

where $C_{\rm SRD}^{\rm AF}$ and $C_{\rm SRD}^{\rm AF}$ are, respectively, the capacity at D and that at E when R employs the AF relaying cooperation. We present our new result concerning the SOP in the following theorem (See Appendix B for its proof).

***Theorem** 3:* The SOP for the AF relaying cooperative transmission mode is given by

$$P_{out}^{\rm AF} = (P_{out}^{\rm AF1} + P_{out}^{\rm AF2} - P_{out}^{\rm AF1}P_{out}^{\rm AF2})\Pr\{C_{\rm SD} < R_c, C_{\rm SR} < R_c\}, \quad (40)$$

$$P_{out}^{\text{DF}} = \Big[\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\} + \Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\} \Pr\{C_{\text{SD}} < R_c\} - \Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\} \Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\} \Big] \Pr\{C_{\text{SR}} \geq R_c\}, \tag{33}$$

where

$$\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\} = F_{\tilde{\rho}_{\text{SD}}}(T) - \sum_{n=0}^{N_{\text{D}}-1} \Pi_1\bigg(n, \frac{1}{\Omega_{\text{RD}}}\bigg), \tag{34}$$

and

$$\Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\} = \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})} + \sum_{n=0}^{N_{\text{E}}-1} \Pi_2\bigg(n, \frac{1}{\Omega_{\text{RE}}}\bigg), \tag{35}$$

with

$$\Pi_1\left(n, \frac{1}{\Omega_{\text{RD}}}\right) = \begin{cases} \sum_{i=0}^{N_{\text{S}}-1} \sum_{j=0}^{i(N_{\text{D}}-1)} \sum_{k=0}^{j} \sum_{n_1=0}^{n} \binom{n}{n_1} (-1)^{n_1} \Xi\left(i,j,k,\Omega_{\text{SD}}\right) \frac{N_{\text{S}} e^{-\frac{T}{\Omega_{\text{RD}}}}}{\Gamma(N_{\text{D}}) \Omega_{\text{RD}}^{n} n!} \\ \quad \times \frac{T^{n-n_1} \Gamma_1\left(k+N_{\text{D}}+n_1, (\frac{i+1}{(i(1-\rho)+1)\Omega_{\text{SD}}} - \frac{1}{\Omega_{\text{RD}}})T\right)}{\left(\frac{i+1}{(i(1-\rho)+1)\Omega_{\text{SD}}} - \frac{1}{\Omega_{\text{RD}}}\right)^{k+N_{\text{D}}+n_1}}, & \text{if } \frac{i+1}{(i(1-\rho)+1)\Omega_{\text{SD}}} \neq \frac{1}{\Omega_{\text{RD}}} \\ \sum_{i=0}^{N_{\text{S}}-1} \sum_{j=0}^{i(N_{\text{D}}-1)} \sum_{k=0}^{j} \sum_{n_1=0}^{n} \binom{n}{n_1} (-1)^{n_1} \Xi\left(i,j,k,\Omega_{\text{SD}}\right) \frac{N_{\text{S}} e^{-\frac{T}{\Omega_{\text{RD}}}}}{\Gamma(N_{\text{D}}) \Omega_{\text{RD}}^{n} n!} \frac{T^{n+k+N_{\text{D}}}}{n+k+N_{\text{D}}}, & \text{if } \frac{i+1}{(i(1-\rho)+1)\Omega_{\text{SD}}} = \frac{1}{\Omega_{\text{RD}}} \end{cases} \tag{36}$$

$$\Pi_2\left(n, \frac{1}{\Omega_{\text{RE}}}\right) = \begin{cases} \frac{e^{-\frac{T_e}{\Omega_{\text{RE}}}}}{\Gamma(N_{\text{E}}) \Omega_{\text{SE}}^{N_{\text{E}}} \Omega_{\text{RE}}{}^{n} n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^{k} T_e^{n-k} \frac{\Gamma_1\left(N_{\text{E}}+k, \left(\frac{1}{\Omega_{\text{SE}}} - \frac{1}{\Omega_{\text{RE}}}\right) T_e\right)}{\left(\frac{1}{\Omega_{\text{SE}}} - \frac{1}{\Omega_{\text{RE}}}\right)^{N_{\text{E}}+k}}, & \text{if } \frac{1}{\Omega_{\text{SE}}} \neq \frac{1}{\Omega_{\text{RE}}} \\ \frac{e^{-\frac{T_e}{\Omega_{\text{RE}}}}}{\Gamma(N_{\text{E}}) \Omega_{\text{SE}}^{N_{\text{E}}} \Omega_{\text{RE}}{}^{n} n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^{k} \frac{T_e^{N_{\text{E}}+n}}{N_{\text{E}}+k}, & \text{if } \frac{1}{\Omega_{\text{SE}}} = \frac{1}{\Omega_{\text{RE}}} \end{cases} \tag{37}$$

and

$$F_{\tilde{\rho}_{\text{SD}}}(T) = \sum_{i=0}^{N_{\text{S}}-1} \sum_{j=0}^{i(N_{\text{D}}-1)} \sum_{k=0}^{j} \frac{N_{\text{S}}\, \Xi(i,j,k,\Omega_{\text{SD}}) \Gamma_1\left(k+N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\text{SD}}}\right)}{(N_{\text{D}}-1)! \left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\text{SD}}}\right)^{k+N_D}}. \tag{38}$$

---

where

$$P_{out}^{\text{AF1}} = \frac{\eta_1}{1 - e^{-\frac{T}{\Omega_{\text{SR}}}}} + \frac{e^{-\frac{T}{\Omega_{\text{SR}}}} \sum_{n=0}^{N_{\text{D}}-1} \Pi_1\left(n, \frac{1}{\Omega_{\text{RD}}}\right) - \eta_3}{\left(1 - e^{-\frac{T}{\Omega_{\text{SR}}}}\right) F_{\tilde{\rho}_{\text{SD}}}(T)}, \tag{41}$$

and

$$P_{out}^{\text{AF2}} = \frac{\eta_2 \left[\frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})} - 1\right] + \left[1 - e^{-\frac{T}{\Omega_{\text{SR}}}} \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})}\right]}{1 - e^{-\frac{T}{\Omega_{\text{SR}}}}} + \frac{\eta_4 - e^{-\frac{T}{\Omega_{\text{SR}}}} \sum_{n=0}^{N_{\text{E}}-1} \Pi_2\left(n, \frac{1}{\Omega_{\text{RE}}}\right)}{1 - e^{-\frac{T}{\Omega_{\text{SR}}}}}, \tag{42}$$

with

$$\eta_1 = \sum_{m=0}^{N_{\text{D}}-1} \frac{\frac{1}{\Omega_{\text{SR}}} (\frac{1}{\Omega_{\text{RD}}})^{m}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RD}}})^{m+1}} + \frac{(\frac{1}{\Omega_{\text{RD}}})^{N_{\text{D}}}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RD}}})^{N_{\text{D}}}} - e^{-\frac{T}{\Omega_{\text{SR}}}}, \tag{43}$$

$$\eta_2 = \sum_{m=0}^{N_{\text{E}}-1} \frac{\frac{1}{\Omega_{\text{SR}}} (\frac{1}{\Omega_{\text{RE}}})^{m}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RE}}})^{m+1}} + \frac{(\frac{1}{\Omega_{\text{RE}}})^{N_{\text{E}}}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RE}}})^{N_{\text{E}}}}, \tag{44}$$

$$\eta_3 = \left[\sum_{m=0}^{N_{\text{D}}-1} \sum_{n=0}^{m} \frac{\frac{1}{\Omega_{\text{SR}}} (\frac{1}{\Omega_{\text{RD}}})^{m}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RD}}})^{m+1}} + \sum_{n=0}^{N_{\text{D}}-1} \frac{(\frac{1}{\Omega_{\text{RD}}})^{N_{\text{D}}}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RD}}})^{N_{\text{D}}}}\right] \times \Pi_1\left(n, \frac{1}{\Omega_{\text{RD}}} + \frac{1}{\Omega_{\text{SR}}}\right), \tag{45}$$

and

$$\eta_4 = \left[\sum_{m=0}^{N_{\text{E}}-1} \sum_{n=0}^{m} \frac{\frac{1}{\Omega_{\text{SR}}} (\frac{1}{\Omega_{\text{RE}}})^{m}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RE}}})^{m+1}} + \sum_{n=0}^{N_{\text{E}}-1} \frac{(\frac{1}{\Omega_{\text{RE}}})^{N_{\text{E}}}}{(\frac{1}{\Omega_{\text{SR}}} + \frac{1}{\Omega_{\text{RE}}})^{N_{\text{E}}}}\right] \times \Pi_2\left(n, \frac{1}{\Omega_{\text{RE}}} + \frac{1}{\Omega_{\text{SR}}}\right). \tag{46}$$

Finally, substituting (28), (33), and (40) into (27), the SOP of the proposed TAS-based IHDAF scheme can be achieved as in (47), as shown at the top of the next page.

***Remark** 3:* Following a similar procedure to derive the SOP of the proposed TAS-based IHDAF scheme, we can obtain the SOPs of the IDF and SDF schemes as benchmarks to demonstrate the secrecy performance of our proposed TAS-based IHDAF scheme. A thorough comparison among these three schemes is provided in Section V.

IV. Asymptotic Secrecy Outage Probability and Effective Secrecy Throughput of TAS-based IHDAF Scheme

In this section, we first analytically determine the asymptotic SOP of the proposed TAS-based IHDAF scheme with the SDF and IDF schemes as benchmarks, aiming to theoretically reveal the benefits of the proposed scheme. In addition, we adopt a new performance metric EST (i.e., effective secrecy throughput) to examine the secrecy performance of the cooperative and DT schemes by taking into account the

$$P_{\text{IHDAF}} = \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})\big(1 - F_{\tilde{\rho}_{\text{SD}}}(T)\big)}{\Gamma(N_{\text{E}})} + e^{-\frac{T}{\Omega_{\text{SR}}}}\Bigg(F_{\tilde{\rho}_{\text{SD}}}(T) + \sum_{n=0}^{N_{\text{D}}-1}\Pi_1\big(n, \frac{1}{\Omega_{\text{RD}}}\big)\big[\frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})} + \sum_{n=0}^{N_{\text{E}}-1}\Pi_2\big(n, \frac{1}{\Omega_{\text{RE}}}\big) - 1\big]\Bigg)$$
$$- F_{\tilde{\rho}_{\text{SD}}}(T)\Bigg(\big[1 - \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})}\big]\eta_2 - \big[1 - \frac{e^{-\frac{T}{\Omega_{\text{SR}}}}\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})}\big] + e^{-\frac{T}{\Omega_{\text{SR}}}}\sum_{n=0}^{N_{\text{E}}-1}\Pi_2\big(n, \frac{1}{\Omega_{\text{RE}}}\big) - \eta_4\Bigg) + \frac{1}{1 - e^{-\frac{T}{\Omega_{\text{SR}}}}}$$
$$\times\Bigg(F_{\tilde{\rho}_{\text{SD}}}(T)\eta_1 + e^{-\frac{T}{\Omega_{\text{SR}}}}\sum_{n=0}^{N_{\text{D}}-1}\Pi_1\big(n, \frac{1}{\Omega_{\text{RD}}}\big) - \eta_3\Bigg)\Bigg(\big[1 - \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})}\big]\big[\eta_2 - e^{\frac{T}{\Omega_{\text{SR}}}}\big] + e^{-\frac{T}{\Omega_{\text{SR}}}}\sum_{n=0}^{N_{\text{E}}-1}\Pi_2\big(n, \frac{1}{\Omega_{\text{RE}}}\big) - \eta_4\Bigg). \quad (47)$$

different time slots required by these schemes. Furthermore, we examine the tradeoff between the secrecy performance and required feedback overhead in the considered system model by comparing our proposed scheme with the CB (i.e., codebook-based beamforming) scheme. Finally, we discuss the impact of outdated CSI and the optimal antenna selection on the secrecy performance of the proposed scheme.

A. Asymptotic Secrecy Outage Probability

In this subsection, we examine the asymptotic SOP of the proposed TAS-based IHDAF scheme with the SDF and IDF schemes as benchmarks to obtain further insights.

***Corollary** 1:* In the case of $P/\sigma_{\text{E}}^2 \to 0$, we have

$$\lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{IHDAF}} < \lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{IDF}} = \lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{SDF}}. \quad (48)$$

Proof: When $P/\sigma_{\text{E}}^2 \to 0$, following (29), (33), and (39), we obtain the SOP of the proposed TAS-based IHDAF scheme as

$$\lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{IHDAF}} = \Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\}\Pr\{C_{\text{SR}} > R_c\} + \Pr\{(C_{\text{SRD}}^{\text{AF}} < R_c)|(C_{\text{SD}} < R_c, C_{\text{SR}} < R_c)\} \times \Pr\{C_{\text{SD}} < R_c, C_{\text{SR}} < R_c\}. \quad (49)$$

Likewise, according to [18] and following (29) and (33), we obtain the SOP of the proposed TAS-based SDF and IDF schemes for $P/\sigma_{\text{E}}^2 \to 0$ as

$$\lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{IDF}} = \lim_{\frac{P}{\sigma_{\text{E}}^2}\to 0} P_{\text{SDF}} = \Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\}\Pr\{C_{\text{SR}} > R_c\} + \Pr\{(C_{\text{SD}} < R_c)|(C_{\text{SD}} < R_c, C_{\text{SR}} < R_c)\} \times \Pr\{C_{\text{SD}} < R_c, C_{\text{SR}} < R_c\}. \quad (50)$$

We note that the only difference between (49) and (50) is that $C_{\text{SRD}}^{\text{AF}}$ in (49) is replaced by C_{SD} in (50). We recall that $C_{\text{SRD}}^{\text{AF}} > C_{\text{SD}}$ due to $C_{\text{SRD}}^{\text{AF}} = \log_2\big(1 + \tilde{\rho}_{\text{SD}} + \frac{\tilde{\rho}_{\text{SD}}\rho_{\text{RD}}}{\tilde{\rho}_{\text{SD}}+\rho_{\text{RD}}+1}\big)$ and $C_{\text{SD}} = \log_2\big(1 + \tilde{\rho}_{\text{SD}}\big)$. As such, we achieve the desired result in (48). ∎

***Remark** 4:* Corollary 1 indicates that the proposed TAS-based IHDAF scheme achieves a lower SOP than the SDF and IDF schemes when $P/\sigma_{\text{E}}^2 \to 0$, which analytically discloses the advantages of the proposed scheme. We note that this conclusion is still valid for reasonable small but non-zero values of P/σ_{E}^2 (e.g., 0 dB), which will be verified in Section V. Based on Corollary 1, we also conclude that the performance gain of proposed scheme over SDF and IDF schemes becomes more prominent as N_{S} increases when N_{S} is relatively small. This is due to the fact that $C_{\text{SRD}}^{\text{AF}} - C_{\text{SD}} = \log_2\Big(1 + \frac{\tilde{\rho}_{\text{SD}}\rho_{\text{RD}}}{(\tilde{\rho}_{\text{SD}}+\rho_{\text{RD}}+1)}\frac{1}{(1+\tilde{\rho}_{\text{SD}})}\Big)$ increases with N_S when $\rho > 0$ and the number of antennas at S is relatively small.

***Corollary** 2:* When $P/\sigma_D^2 \to \infty$, we have

$$\lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{IHDAF}} = \lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{IDF}} < \lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{SDF}}. \quad (51)$$

Proof: Following (31), we have

$$\lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} \Pr\{C_{\text{SD}} < R_c\} = \lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} \sum_{i=0}^{N_{\text{S}}-1}\sum_{j=0}^{i(N_{\text{D}}-1)}\sum_{k=0}^{j}\frac{N_{\text{S}}\Xi(i,j,k,\Omega_{\text{SD}})}{(N_{\text{D}}-1)!} \times \frac{\Gamma_1\Big(k + N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\text{SD}}}\Big)}{\Big(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\text{SD}}}\Big)^{k+N_D}} = 0. \quad (52)$$

Based on the above equality, the value of (25) and (26) tend to be zero, and thus we have

$$\lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{IHDAF}} = \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})}. \quad (53)$$

As per [11, Eq. (42)], we also have

$$\lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{IDF}} = \frac{\Gamma(N_{\text{E}}, \frac{T_e}{\Omega_{\text{SE}}})}{\Gamma(N_{\text{E}})} < \lim_{\frac{P}{\sigma_{\text{D}}^2}\to\infty} P_{\text{SDF}}. \quad (54)$$

Comparing (53) with (54), we complete the proof. ∎

***Remark** 5:* Corollary 2 indicates that for $P/\sigma_{\text{D}}^2 \to \infty$ the proposed TAS-based IHDAF scheme achieves a lower SOP than the SDF scheme, which is the same as that of the IDF scheme. This also demonstrates the advantage of the proposed scheme. In addition, as per (53) we note that the SOP of the proposed scheme for $P/\sigma_{\text{D}}^2 \to \infty$ does not depend on the SNR of S-D link.

B. Effective Secrecy Throughput

Following the definition of EST adopted in [11, 36], which is the product of the secrecy rate and the secure transmission probability, the EST of the proposed scheme is given by

$$T_{\text{IHDAF}} = Rs(1 - P_{DT}^{out}) \quad (55a)$$
$$+ \frac{Rs}{2}P_{DT}^{out}\Pr\{C_{\text{SR}} \geq R_c\}(1 - P_{DF}^{out}) \quad (55b)$$
$$+ \frac{Rs}{2}P_{DT}^{out}\Pr\{C_{\text{SR}} < R_c\}(1 - P_{AF}^{out}), \quad (55c)$$

where $P_{DT}^{out} = \Pr\{(C_{\rm SD} < R_c) \cup (C_{\rm SE} \geq R_e)\}$, $P_{DF}^{out} = \Pr\{(C_{\rm SRD}^{\rm DF} < R_c) \cup (C_{\rm SRE}^{\rm DF} \geq R_e)\}$, and $P_{AF}^{out} = \Pr\{(C_{\rm SRD}^{\rm AF} < R_c) \cup (C_{\rm SRE}^{\rm AF} \geq R_e)\}$. We note that only one time slot is required for the DT mode while two times slots are used in the AF and DF mode, which is the reason why we have R_s in (55a) but $R_s/2$ in (55b) and (55c). Based on (55), we will numerically examine the EST of the proposed scheme in Section V.

C. Tradeoff between Secrecy Performance and Feedback Overhead

In this work, we adopt TAS in the proposed scheme due the following three aspects.

- In some communication scenario, such as Internet of Things and Device-to-Device communications, the system may only support a few bits feedback overhead due to limited resources, which leads to that the techniques (e.g., beamforming) that require high feedback overhead are not applicable. Considering such limited feedback overhead, we adopt TAS in this work since it only requires $\lceil \log N_{\rm S} \rceil$ bits feedback overhead.
- In the context of physical layer security, TAS can enable legitimate nodes to achieve a high diversity gain while does not offer benefits to E (i.e., the eavesdropper). This is due to the fact that the strongest antenna selected in TAS is equivalent to a random source antenna for E based on the valid assumption that legitimate links are independent of the eavesdropping links.
- A multi-antenna transmitter suffers from a complex hardware structure (e.g., multiple RF chains), which are expensive to implement. We adopt TAS at the multi-antenna S in order avoid this complex hardware structure since TAS only requires one active RF chain.

In practice, if only the feedback overhead is the bottleneck of the system, another transmission scheme, namely, CB(i.e.,codebook-based beamforming) scheme, was proposed in [31, 37]. In this CB scheme, all transmit antennas at the source are active and the required feedback overhead is determined by the number of codebook vectors available to select. Specifically, in this scheme a pre-designed codebook of N unit-norm vectors is known to both the transmitter and receiver. Then, the receiver selects the best codebook vector (using it as a beamforming vector) that maximizes the SNR of the channel based on the known CSI and feeds back the index of the selected vector through an open error-free feedback channel to the transmitter. As such, the amount of feedback overhead required by the CB scheme is $\lceil \log N \rceil$. Here, we adopt this CB scheme as a benchmark to study the efficiency of the proposed scheme in terms of the tradeoff between its achieved secrecy performance and the required feedback overhead. In order to guarantee a fair comparison between the proposed scheme and the CB scheme, we also assume that D selects the best codebook vector based on the S-D link and feeds back the its index to S. We refer to the IHDAF scheme with CB (instead of TAS) as the CB-IHDAF scheme while refer to the TAS-based IHDAF as TAS-IHDAF when comparing with CB-IHDAF. Particularly, we adopt two different codebooks in the CB scheme for comparison (i.e., $N = 4$ and $N = 16$). For $N = 4$, we adopt the codebook generated based on the Generalized Lloyd Algorithm (GLA) (also known as LBG algorithm) presented in [38]. For $N = 16$, we use a Grassmannian codebook proposed in [39]. We further refer to the CB-IHDAF scheme with $N = 4$ and $N = 16$ as CB($N = 4$)-IHDAF and CB($N = 16$)-IHDAF, respectively. We will compare the secrecy performance of the proposed scheme with that of the CB-IHDAF scheme in Section V to further demonstrate the advantages of our proposed scheme.

D. Discussion on Optimal Antenna Selection

As mentioned in Section II-A, the antenna selection given in (1) is not optimal. The optimal antenna selection should depend on the working mode of the proposed scheme. Specifically, the current selection is optimal when DT mode is active, the optimal selection should maximize $\rho_{\rm SRD}^{DF}$ (i.e., the SNR at D for DF mode) when DF mode is active at R, and the optimal selection should maximize $\rho_{\rm SRD}^{AF}$ (i.e., the SNR at D for AF mode) when AF mode is active at R. As such, the optimal selection not only depends on the S-D and S-R links, but also relates to the R-D link. Therefore, the optimal selection requires the cooperation between R and D (e.g., R has to feedback the CSI of the S-R link to D in order to enable this optimal selection), which costs extra resources (e.g., time slots, feedback overhead). In order to avoid such cost and to achieve an efficient scheme of low complexity, we adopt a sub-optimal selection scheme in the current work. However, we will examine the performance gap between the adopted sub-optimal selection and the optimal selection numerically in Section V.

V. Numerical Results

In this section, we provide numerical results to examine the secrecy performance of the proposed scheme. The SDF, IDF, and DT [3] schemes are also shown for comparison. We show that the proposed TAS-based IHDAF scheme outperforms other schemes by achieving a lower SOP and a higher EST, especially in the scenario where R is close to D. Moreover, Monte Carlo simulations are also performed to verify the analytical results given in this paper. In the simulation, we locate R on a straight line between S and D, which is a typical topology applied in relay networks. We set the path-loss factor as $\nu = 4$, and that the reference distance for the antenna far-field as $d_0 = 1\,$m. All nodes transmit at a carrier frequency of $f_c = 2.4$GHz, corresponding to a wavelength of $\lambda = 125$mm, $B = 10$MHz, and $N_0 = -174$dBn/Hz [11].

Fig. 3 plots the SOP versus the normalized distance between S and R (e.g., the value of δ) with different values of $N_{\rm D}$. In

[3]It is noted that the SOP of the non-cooperative DT scheme is given by $P_{DT}^{out} = \Pr\{(C_{SD} < R_c) \cup (C_{SE} > R_e)\} = N_{\rm S} \sum_{i=0}^{N_{\rm S}-1} \sum_{j=0}^{i(N_{\rm D}-1)} \sum_{k=0}^{j} \frac{\Xi(i,j,k,\Omega_{\rm SD})}{(N_{\rm D}-1)!} \frac{\Gamma_1\left(k+N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)}{\left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\rm SD}}\right)^{k+N_D}} \Big[1 - \frac{\Gamma(N_{\rm E}, \frac{T_e}{\Omega_{\rm SE}})}{\Gamma(N_{\rm E})}\Big] + \frac{\Gamma(N_{\rm E}, \frac{T_e}{\Omega_{\rm SE}})}{\Gamma(N_{\rm E})}$. Moreover, due to the multiplexing loss of the cooperative schemes, we also assume that the three cooperative schemes (i.e., the IDF, SDF and IHDAF shcemes) transmit with twice of the rate of the Non-cooperative scheme [11].

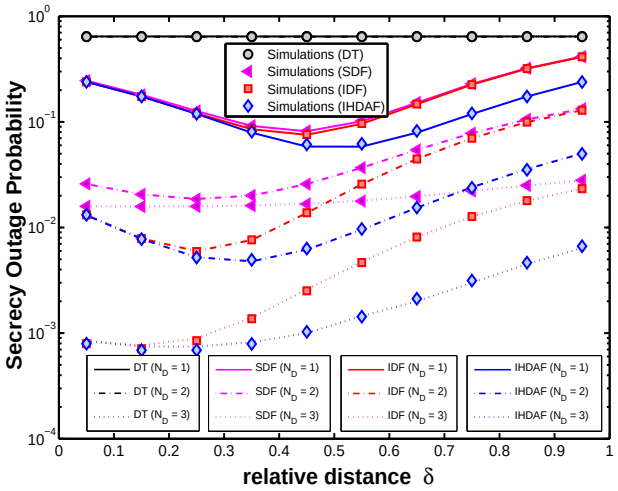


Fig. 3. Secrecy outage probability versus the normalized distance between S and R (i.e., δ) with $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$dB, $\Omega_{\rm SD} = 20$ dB, $R_e = 2$ bpcu, $R_c = 3.6$ bpcu, $\rho = 1$, $N_{\rm S} = 2$, and $N_{\rm E} = 4$.

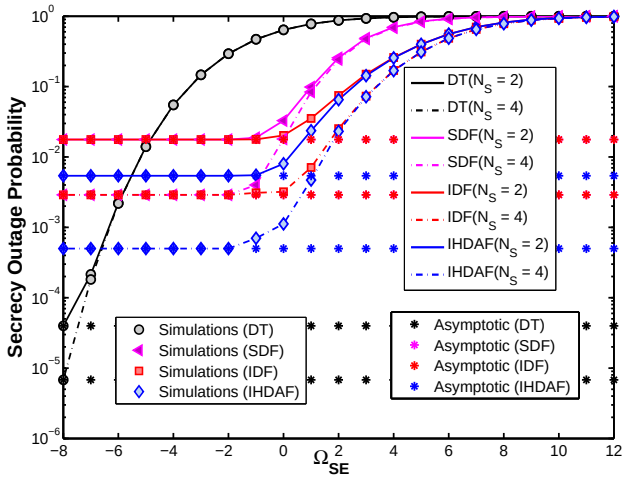


Fig. 4. Secrecy outage probability versus the SNR at E with $\Omega_{\rm SD} = 20$ dB, $R_e = 2$ bpcu, $R_c = 3.6$ bpcu, $\delta = 0.5$, $\rho = 1$, $N_{\rm D} = 2$, $N_{\rm E} = 4$, and $N_{\rm S} = 2, 4$.

this figure, we first observe that the simulation and analytical results match well for different values of δ and $N_{\rm D}$, which confirms the correctness of the derived analytical expression of the SOP. We also observe that all the SDF, IDF, and IHDAF schemes outperform the DT scheme in terms of achieving lower SOPs, illustrating the security benefits of exploiting cooperative relays to prevent eavesdropping attacks. Fig. 3 shows that the SOPs of all cooperative relaying schemes decrease as the normalized distance between S and R increases for $\delta > 0.5$, and the proposed IHDAF scheme achieves the best secrecy performance. Particularly, the IDF and the proposed IHDAF schemes outperform the SDF scheme in terms of achieving similar secrecy performance gain when $\delta < 0.2$, while the proposed scheme gains more prominent advantages when $\delta > 0.2$. This is due to the fact that when R is close to S, the average SNR of the S-R link is high and thus the probability of adopting AF mode in the proposed IHDAF scheme is low, which leads to marginal benefits in the proposed scheme relative to the IDF scheme. However, when R is far from S, the average SNR of the S-R link is low and the probability that the proposed scheme adopts AF mode (while the IDF scheme fails) is high, which results in the dramatic advantages of the proposed IHDAF scheme.

Fig. 4 plots the SOP versus SNR at E for different number of transmit antennas at S. One can see from Fig. 4 that the SOPs of all the schemes decrease with the SNR at E, while our proposed IHDAF scheme achieves the best performance for $\Omega_{\rm SE} > -6$ dB. Fig. 4 also illustrates the secrecy performance of the proposed scheme relative to SDF and IDF schemes becomes more prominent as the number of antennas at S increases (i.e., from $N_{\rm S} = 2$ to $N_{\rm S} = 4$). This can be explained by Remark 4 in Section IV.

As mentioned in Section IV-D, in Fig. 5 we numerically examine the performance gap between the adopted sub-optimal antenna selection and the optimal antenna selection in the proposed scheme. Surprisingly, in this figure we observe that

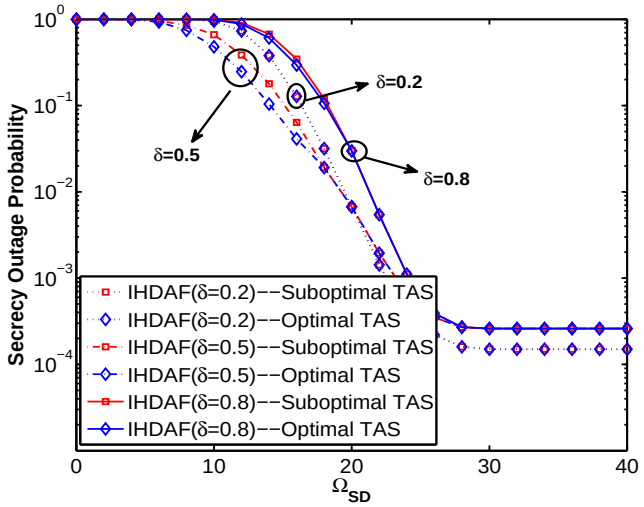


Fig. 5. Secrecy outage probability of the proposed TAS-based IHDAF scheme with sub-optimal and optimal antenna selections, with $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$ dB, $R_e = 2$ bpcu, $R_c = 3.6$ bpcu, $\delta = 0.2, 0.5, 0.8$, $\rho = 1$, $N_{\rm E} = 4$, $N_{\rm D} = 2$, and $N_{\rm S} = 2$.

this gap in terms of the difference in the achieved SOP is not significant. Specifically, this gap is negligible when $\Omega_{\rm SD}$ is relatively large, which is due to the fact that optimal selection will depend more on the S-D link when the S-D link becomes strong (e.g., the probability that the proposed scheme operates in the DT mode is high, for which our sub-optimal selection is optimal). Also, this gap is extremely small when δ is close to 0 or 1 (i.e., R is close to S or D). This is due to the fact that the cooperative link (i.e., S-R-D) is weak when one of the S-R and R-D links is weak (i.e., δ is close to 0 or 1) since the quality of the cooperative link is mainly determined by the link of the lower quality in relay networks, and thus the optimal selection will be mainly determined by the S-D link. These observations confirm the validness of the adopted sub-optimal antenna selection, which costs lower

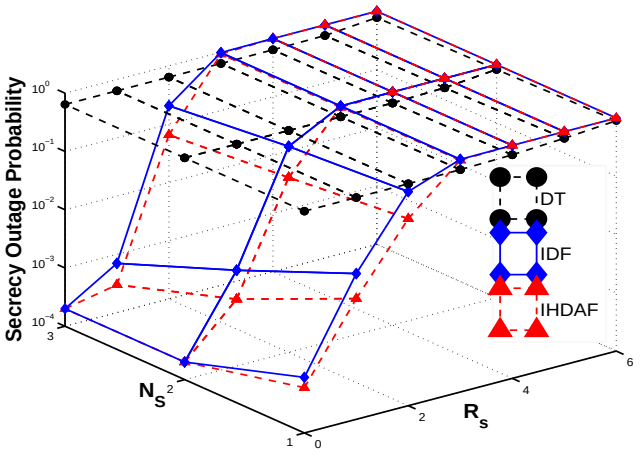


Fig. 6. Secrecy outage probability versus R_s for $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$dB, $\Omega_{\rm SD} = 20$ dB, $\delta = 0.5$, $\rho = 1$, $N_{\rm E} = 4$, $N_{\rm D} = 2$, and $R_e = 2$ bpcu.

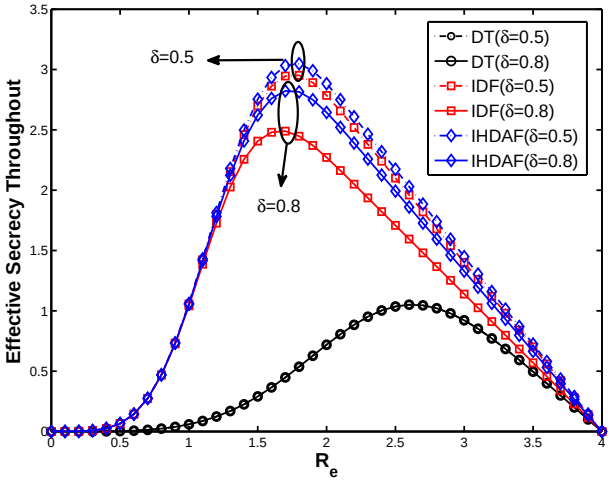


Fig. 7. Effective secrecy throughput of the IHDAF, IDF and DT schemes with $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$ dB, $\Omega_{\rm SD} = 20$ dB, $\delta = 0.5, 0.8$, $\rho = 1$, $N_{\rm E} = 4$, $N_{\rm D} = 2$, $N_{\rm S} = 2$, and $R_c = 4$ bpcu.

feedback overhead and cooperation complexity. The analysis of the above examples show that the IDF scheme always outperforms the SDF scheme. In the following simulations, only the simulation results for the proposed TAS-based IHDAF scheme, IDF and DT schemes are shown for better exposition.

Fig. 6 demonstrates the impact of the secrecy rate on the SOPs performance of the two cooperative relaying schemes and the DT scheme. In this figure, we observe that all the cooperative relaying schemes achieve higher secrecy rates for a fixed SOP. We also observe that the cooperative schemes outperform DT scheme when $R_s < 2.5$bpcu in terms of achieving lower SOPs. For a given equivocation rate (e.g., $R_e = 2$bpcu), the DT scheme may obtain a larger secrecy rate at the cost of a higher SOP. We noted that if there exists a maximum allowable SOP, the DT scheme may fail to provide secrecy transmission while the cooperative schemes can [9]. Finally, we observe that when $N_S = 1$, the proposed scheme still outperforms the IDF and DT schemes, which demonstrates that the advantage of the proposed scheme does not come from TAS.

Fig. 7 plots the EST of different schemes versus R_e. In this figure, we first observe that the cooperative schemes significantly outperform the DT scheme in terms of achieving a higher EST. This is due to the fact that the relay can aid the transmission between S and D when the DT fails, which demonstrates the benefits of relaying protocols. In addition, we observe that the proposed scheme can achieve a higher EST than other schemes. Specifically, the maximum EST of the proposed scheme is much higher than that of any other scheme, which is due to the fact that the proposed scheme takes into the advantages of both the AF and DF modes. Finally, we observe that the EST gain of the proposed scheme relative to the IDF scheme increases as the distance between S and R increases. This observation again confirms that the proposed scheme outperforms the IDF scheme, especially when R is close to D.

In Fig. 8 , we compare the SOP of the proposed scheme

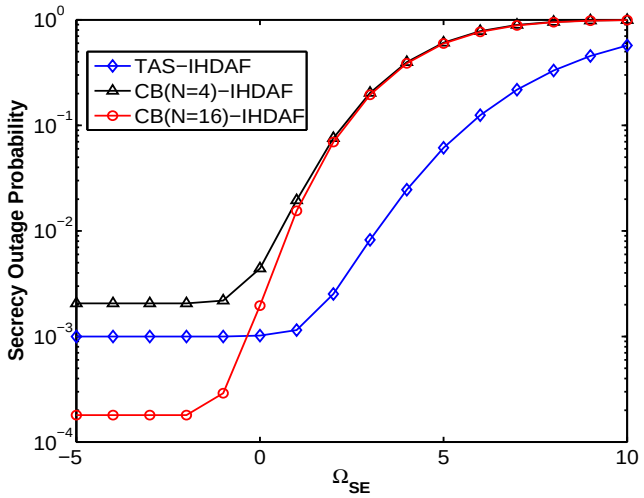


Fig. 8. Secrecy outage probability of the TAS-IHDAF, CB($N = 4$)-IHDAF, and CB($N = 16$)-IHDAF schemes with $R_e = 2$bpcu, $R_c = 3$ bpcu, $\Omega_{\rm SD} = 20$ dB, $\delta = 0.5$, $\rho = 1$, $N_{\rm S} = 4$, $N_{\rm D} = 1$, and $N_{\rm E} = 2$.

(TAS-IHDAF) with that of the CB-IHDAF scheme. In this figure, we first observe that the proposed TAS-IHDAF achieves a lower SOP than the CB($N = 4$)-IHDAF scheme. We note that these two schemes require the same amount of feedback overhead, which is $\lceil \log_2 4 \rceil = 2$ bits due to $N_{\rm S} = N = 4$. As such, this observation demonstrates the advantage of the proposed TAS-IHDAF scheme in terms of achieving a higher secrecy performance with the same feedback overhead. Besides this advantage, we note that the proposed TAS-IHDAF only require one active RF chain while CB-IHDAF scheme requests $N_{\rm S}$ (which is 4 in this figure). As expected, we observe that in the low regime of $\Omega_{\rm SE}$ (e.g., < 0 dB) the CB($N = 16$)-IHDAF scheme outperforms the proposed scheme at the cost of a higher feedback overhead (i.e., CB($N = 16$)-IHDAF costs 4 bits feedback overhead while TAS-IHDAF only requires 2 bits). However, we also observe that the

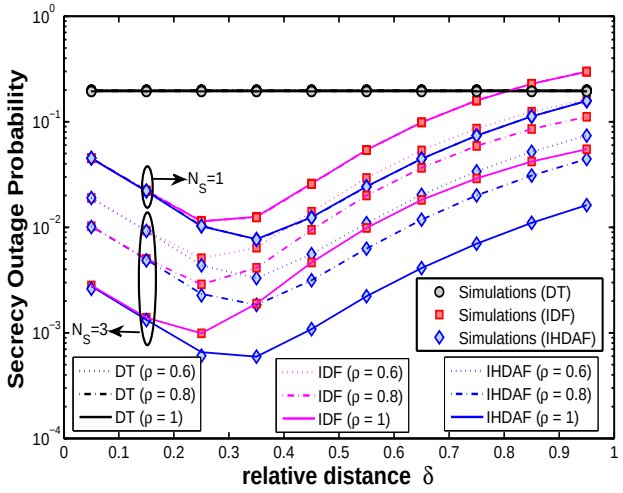


Fig. 9. Secrecy outage probability versus the normalized distance between S and R (i.e., δ) with $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$ dB, $\Omega_{\rm SD} = 20$ dB, $R_e = 2$ bpcu, $R_c = 3.6$ bpcu , $N_{\rm D} = 2$, $N_{\rm E} = 2$, and $\rho = 0.6, 0.8, 1$.

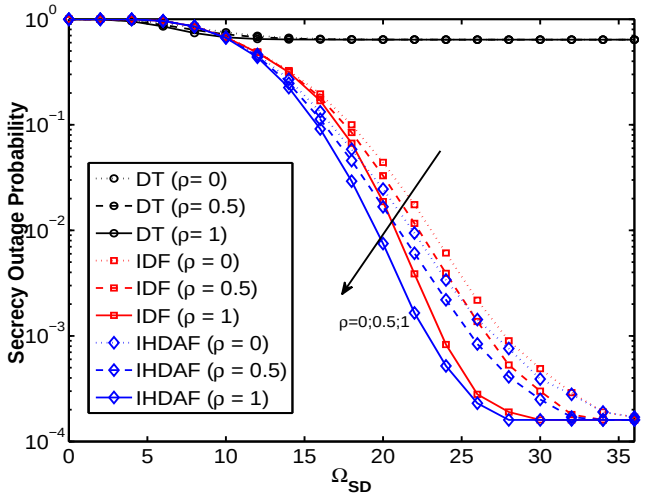


Fig. 10. Secrecy outage probability versus SNR at D with different values of ρ when $N_{\rm E} = 4$, $N_{\rm S} = N_{\rm D} = 2$, $R_e = 2$ bpcu, $R_c = 3.6$ bpcu, $\delta = 0.5$, and $\Omega_{\rm SE} = \Omega_{\rm RE} = 0$ dB.

proposed TAS-IHDAF scheme achieves a lower SOP than the CB($N = 16$)-IHDAF scheme in the medium and high regimes of $\Omega_{\rm SE}$ (e.g., ≥ 0 dB). This is due to the fact that in the CB-IHDAF scheme all antennas at S are active and E can obtain some diversity gain on average, while in the proposed TAS-IHDAF scheme only one antenna is active (which is the strongest one for D but random for E) and no such gain can be achieved at E. This gain increases as the S-E link becomes stronger (i.e., as $\Omega_{\rm SE}$ increases), and thus once $\Omega_{\rm SE}$ becomes larger than some specific value the CB-IHDAF scheme loses its benefits offered by the extra feedback overhead. This can be confirmed by the observation in this figure that the SOPs of the CB($N = 4$)-IHDAF and CB($N = 16$)-IHDAF schemes converge together in the high regime of $\Omega_{\rm SE}$.

Fig. 9 plots the SOP versus the normalized distance between S and R (i.e., the value of δ) with different values of $N_{\rm S}$ and ρ. As expected, we first observe that delayed feedback (i.e., outdated CSI) has detrimental effect on the secrecy performance of different schemes, and the SOPs of all the schemes decrease as ρ increases. Fig. 9 shows that, when $N_S = 1$, the SOPs of all schemes (i.e., DT, IDF, and IHDAF schemes) keep constant regardless of the value of ρ. This is due to the fact that the link of S-D is unique when $N_S = 1$ and no antenna selection is conducted. Fig. 9 also shows that the IDF and IHDAF schemes achieve better secrecy performance as N_S increases, and the advantage of the IHDAF scheme relative to the IDF scheme becomes more prominent as ρ increases.

In Fig. 10 , we further examine the impact of imperfect (i.e., outdated) CSI on the secrecy performance of the proposed scheme. As expected, in this figure we observe that the SOPs of all schemes increase as ρ decreases, since a smaller ρ indicates a severer imperfect impact (e.g., $\rho = 0$ represents a fully outdated CSI, while $\rho = 1$ represents perfect CSI). We also observe that with the imperfect CSI our proposed scheme still outperforms the other schemes, which demonstrates the robustness of the proposed scheme. This is mainly due to the fact that the benefits of the proposed scheme are not due to TAS but the IHDAF strategy.

VI. Conclusion

In this paper, for the first time, we propose the TAS-based IHDAF scheme to enhance physical layer security while maintaining low feedback overhead and hardware complexity in a cooperative relay network. In order to fully examine the secrecy performance of the proposed scheme, its SOP was first derived in a closed-form expression by considering no CSI at S. Then, asymptotic analysis on the SOP was conducted with the SDF and IDF schemes as benchmarks, disclosing a secrecy performance floor of the proposed TAS-based IHDAF scheme. Furthermore, we examine the impact of the number of antennas, relay locations, average SNRs, and secrecy rates on the SOP of the proposed scheme. It has been shown that the proposed TAS-based IHDAF scheme significantly outperforms the IDF, SDF, and DT schemes in view of the a lower SOP and a higher EST achieved, especially when R is close to D. Furthermore, the proposed TAS-based IHDAF scheme can outperform the CB scheme with less feedback overhead and fewer RF chains. For future work, we will examine the secrecy performance of IHDAF in multiple-antenna relaying networks, where antenna selection or artificial-noise-aided secure transmissions will be considered at the multiple-antenna relay.

Appendix A
Proof of Theorem 2

When the S-D transmission fails in the DT mode, but R can decode it correctly, R operates in the DF mode. According to

the Bayes' rule, the SOP given in (25) can be expressed as

$$P_{out}^{\text{DF}} = \Big[\Pr\left\{C_{\text{SRD}}^{\text{DF}} < R_c\right\} + \Pr\left\{C_{\text{SRE}}^{\text{DF}} \geq R_e\right\} \Pr\left\{C_{\text{SD}} < R_c\right\} - \Pr\left\{C_{\text{SRE}}^{\text{DF}} \geq R_e\right\} \Pr\left\{C_{\text{SRD}}^{\text{DF}} < R_c\right\}\Big] \Pr\left\{C_{\text{SR}} \geq R_c\right\}, \tag{56}$$

with

$$\Pr\{C_{\text{SR}} \geq R_c\} = 1 - \Pr\{C_{\text{SR}} < R_c\} = e^{-\frac{T}{\Omega_{\text{SR}}}}. \tag{57}$$

This is due to the fact that the TAS scheme at S is based on the S-D link, and thus the CDF of ρ_{SR} as $F_{\rho_{\text{SR}}}(x) = (1 - e^{-\frac{x}{\Omega_{\text{SR}}}})$. Then, the key to obtaining the P_{out}^{DF} is to compute $\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\}$ and $\Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\}$. According to [11], $\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\}$ can be expressed as

$$\begin{aligned}\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\} &= \Pr\left\{\log_2(1 + \tilde{\rho}_{\text{SD}} + \rho_{\text{RD}}) < R_c\right\} \\ &= \Pr\left\{\tilde{\rho}_{\text{SD}} + \rho_{\text{RD}} < T\right\}.\end{aligned} \tag{58}$$

Defining $Y = \rho_{\text{RD}}$, we note that Y is a sum of the squares of N_{D} independent Gaussian random variables, therefore, the PDF of Y is obtained as [9]

$$f_Y(y) = \frac{e^{-\frac{y}{\Omega_{\text{RD}}}} y^{N_{\text{D}}-1}}{(\Omega_{\text{RD}})^{N_{\text{D}}}\, \Gamma(N_{\text{D}})}. \tag{59}$$

Using (21) and (59), we can further express (58) as

$$\begin{aligned}\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\} &= \Pr\left\{\tilde{\rho}_{\text{SD}} + \rho_{\text{RD}} < T\right\} \\ &= \int_0^T f_{\tilde{X}}(\tilde{x}) \big[\int_0^{T-\tilde{x}} f_Y(y) dy\big] d\tilde{x}.\end{aligned} \tag{60}$$

By applying the PDFs of X and Y into (60), we obtain (34). Following similar steps as in obtaining $\Pr\{C_{\text{SRD}}^{\text{DF}} < R_c\}$, $\Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\}$ can be further written as

$$\begin{aligned}\Pr\{C_{\text{SRE}}^{\text{DF}} \geq R_e\} &= 1 - \Pr\{C_{\text{SRE}}^{\text{DF}} < R_e\} \\ &= 1 - \Pr\{\rho_{\text{SE}} + \rho_{\text{RE}} < T_e\}.\end{aligned} \tag{61}$$

It is important to note that the selection of the strongest transmit antenna for D corresponds to selecting a random transmit antenna for E. As such for E with MRC, we can easily find that ρ_{SE}, ρ_{RE}, and ρ_{RD} have the same PDF and CDF. According to these characteristics and some mathematical manipulations, we can obtain (35), where we have calculated the resultant integral using [33, Eq. (3.381.1))] and [33, Eq. (3.382.1))]. Therefore, the SOP of P_{out}^{DF} is obtained by substituting (31), (34), (35), and (57) into (33). This completes the Proof.

APPENDIX B
PROOF OF THEOREM 3

If neither D nor R has received the message from S correctly, R operates in AF mode. Using equation (39), the SOP can be further expressed as (62), which is shown at the top of the next page.

Using (13), $\Pr\{(C_{\text{SRD}}^{\text{AF}} < R_c) | (C_{\text{SD}} < R_c, C_{\text{SR}} < R_c)\}$ can be expressed as

$$\begin{aligned}&\Pr\{(C_{\text{SRD}}^{\text{AF}} < R_c) | (C_{\text{SD}} < R_c, C_{\text{SR}} < R_c)\} \\ &= \Pr\{\log_2(1 + \tilde{\rho}_{\text{SD}} + \frac{\rho_{\text{SR}}\rho_{\text{RD}}}{\rho_{\text{SR}} + \rho_{\text{RD}} + 1}) < R_c | (\Phi_1, \Phi_2)\}.\end{aligned} \tag{63}$$

For notational convenience, here we introduce the shorthand $\Phi_1 = (C_{\text{SR}} < R_c)$ and $\Phi_2 = (C_{\text{SD}} < R_c)$. We have

$$\begin{aligned}&\Pr\{\log_2(1 + \tilde{\rho}_{\text{SD}} + \frac{\rho_{\text{SR}}\rho_{\text{RD}}}{\rho_{\text{SR}} + \rho_{\text{RD}} + 1}) < R_c | \Phi_1, \Phi_2\} && (64)\\ &\gtrapprox \Pr\{\log_2(1 + \tilde{\rho}_{\text{SD}} + \min(\rho_{\text{SR}}, \rho_{\text{RD}})) < R_c \,|\Phi_1, \Phi_2\} && (65)\\ &= \Pr\{\tilde{\rho}_{\text{SD}} + \rho_{\min}^d < T \,|\Phi_1, \Phi_2\}, && (66)\end{aligned}$$

with $\rho_{\min}^d = \min(\rho_{\text{SR}}, \rho_{\text{RD}})$, where (65) is obtained using the approximation of $\frac{S_1 S_2}{S_1+S_2+1} < \frac{S_1 S_2}{S_1+S_2} < \min[S_1, S_2]$ [29], and the effect of the approximation error can be neglected in high SNR regions. In addition, this effect can also be ignored when considering a secrecy transmission as in this paper. As shown in Section V, our simulation results corroborate the theoretical analysis, and the approximation is actually very accurate for the whole SNR region.

To proceed, according to [21], the expressions of $\Pr\{\rho_{\min}^d < x \,|\Phi_1\}$, and $\Pr(\tilde{\rho}_{\text{SD}} \leq y \,|\Phi_2\}$ and their corresponding PDFs can be obtained as in (67) and (68), which are shown at the top of the next page. Then, we compute

$$\begin{aligned}&\Pr\left\{\tilde{\rho}_{\text{SD}} + \rho_{\min}^d < T \,|\Phi_1, \Phi_2\right\} \\ &= \int_0^T \int_0^{T-x} f_{\rho_{\min}^d}(x|\Phi_1) f_{\tilde{\rho}_{\text{SD}}}(y|\Phi_2) dy dx.\end{aligned} \tag{69}$$

By substituting (67) and (68) into (69), and performing some mathematical manipulations, we can obtain (41), where we have introduced the shorthand $P_{out}^{\text{AF1}} = \Pr\{(C_{\text{SRD}}^{\text{AF}} < R_c) | (C_{\text{SD}} < R_c, C_{\text{SR}} < R_c)\}$ for notational convenience.

Similarly, we can obtain $\Pr\{(C_{\text{SRE}}^{\text{AF}} > R_e) | (C_{\text{SR}} < R_c\}$ as

$$\begin{aligned}&\Pr\{(C_{\text{SRE}}^{\text{AF}} \geq R_e) | C_{\text{SR}} < R_c)\} \\ &= \Pr\{\log_2\big(1 + \rho_{\text{SE}} + \frac{\rho_{\text{SR}}\rho_{\text{RE}}}{\rho_{\text{SE}} + \rho_{\text{RE}} + 1}\big) \geq R_e | \log_2(1 + \rho_{\text{SR}}) < R_c\} \\ &\gtrapprox \Pr\{\log_2(1 + \rho_{\text{SE}} + \min(\rho_{\text{SE}}, \rho_{\text{RE}})) \geq R_e \,|\Phi_1\} \\ &= 1 - \Pr\{\rho_{\text{SE}} + \rho_{\min}^e < T_e \,|\Phi_1\},\end{aligned} \tag{70}$$

with $\rho_{\min}^e = \min(\rho_{\text{SR}}, \rho_{\text{RE}})$. Furthermore, we have

$$\begin{aligned}&f_{\rho_{\min}^e}(x|\Phi_1) \\ &= \frac{\partial}{\partial x}\left[\frac{\Pr(\rho_{\min}^e \leq x, \Phi_1)}{\Pr(\Phi_1)}\right] \\ &= \frac{\Omega_{\text{RE}} e^{\frac{-x}{\Omega_{\text{SR}}}} \Gamma(N_{\text{E}}, \frac{x}{\Omega_{\text{RE}}}) + \Omega_{\text{SR}} e^{\frac{-x}{\Omega_{\text{RE}}}} (\frac{x}{\Omega_{\text{RE}}})^{N_{\text{E}}-1} [e^{-\frac{x}{\Omega_{\text{SR}}}} - e^{-\frac{T}{\Omega_{\text{SR}}}}]}{\Omega_{\text{SR}}\Omega_{\text{RE}}\Gamma(N_{\text{E}})(1 - e^{-\frac{T}{\Omega_{\text{SR}}}})}.\end{aligned} \tag{71}$$

According to $f_{\rho_{\text{SE}}}(y)$ in Theorem 2 and $f_{\rho_{\min}^e}(\,x \,|\,\Phi_1\,)$ in (71), $\Pr\{\rho_{\text{SE}} + \rho_{\min}^e < 2^{R_e} - 1 \,|\Phi_1\}$ in (70) can be rewritten as

$$\begin{aligned}&\Pr\{\rho_{\text{SE}} + \rho_{\min}^e < T_e \,|\Phi_1\} \\ &= \int_0^{T_e} \int_0^{T_e - y} f_{\rho_{\min}^e}(x|\Phi_1) f_{\rho_{\text{SE}}}(y) dx dy.\end{aligned} \tag{72}$$

With some mathematical manipulations, and the shorthand $P_{out}^{\text{AF2}} = \Pr\{(C_{\text{SRE}}^{\text{AF}} \geq R_e) | (C_{\text{SR}} < R_c)\}$, we can finally obtain (42). Hence, we complete the proof of Theorem 3 .

$$P_{out}^{\mathrm{AF}} = \Big[\Pr\{(C_{\mathrm{SRD}}^{\mathrm{AF}} < R_c) | (C_{\mathrm{SD}} < R_c, C_{\mathrm{SR}} < R_c)\} + \Pr\{(C_{\mathrm{SRE}}^{\mathrm{AF}} \geq R_e) | (C_{\mathrm{SR}} < R_c)\} - \Pr\{(C_{\mathrm{SRD}}^{\mathrm{AF}} < R_c) | (C_{\mathrm{SD}} < R_c, C_{\mathrm{SR}} < R_c)\} \Pr\{(C_{\mathrm{SRE}}^{\mathrm{AF}} \geq R_e) | (C_{\mathrm{SR}} < R_c)\} \Big] \Pr\{C_{\mathrm{SD}} < R_c, C_{\mathrm{SR}} < R_c\}. \quad (62)$$

$$f_{\rho_{\min}^d}(x|\Phi_1) = \frac{\partial}{\partial x}\left[\frac{\Pr(\rho_{\min}^d \leq x, \Phi_1)}{\Pr(\Phi_1)}\right] = \frac{\Omega_{\mathrm{RD}} e^{\frac{-x}{\Omega_{\mathrm{SR}}}} \Gamma(N_{\mathrm{D}}, \frac{x}{\Omega_{\mathrm{RD}}}) + \Omega_{\mathrm{SR}} e^{\frac{-x}{\Omega_{\mathrm{RD}}}} (\frac{x}{\Omega_{\mathrm{RD}}})^{N_{\mathrm{D}}-1} [e^{-\frac{x}{\Omega_{\mathrm{SR}}}} - e^{-\frac{T}{\Omega_{\mathrm{SR}}}}]}{\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}\Gamma(N_{\mathrm{D}})(1 - e^{-\frac{T}{\Omega_{\mathrm{SR}}}})}, \quad (67)$$

$$f_{\tilde{\rho}_{\mathrm{SD}}}(y|\Phi_2) = \frac{\partial}{\partial y}\left[\frac{\Pr(\tilde{\rho}_{\mathrm{SD}} \leq y, \Phi_2)}{\Pr(\Phi_2)}\right] = \frac{\sum_{i=0}^{N_{\mathrm{S}}-1} \sum_{j=0}^{i(N_{\mathrm{D}}-1)} \sum_{k=0}^{j} \Xi(i,j,k,\Omega_{\mathrm{SD}})\, e^{-\frac{(i+1)y}{(i(1-\rho)+1)\Omega_{\mathrm{SD}}}} y^{k+N_{\mathrm{D}}-1}}{\sum_{i=0}^{N_{\mathrm{S}}-1} \sum_{j=0}^{i(N_{\mathrm{D}}-1)} \sum_{k=0}^{j} \Xi(i,j,k,\Omega_{\mathrm{SD}}) \frac{\Gamma_1\left(k+N_D, \frac{(i+1)T}{(i(1-\rho)+1)\Omega_{\mathrm{SD}}}\right)}{\left(\frac{(i+1)}{(i(1-\rho)+1)\Omega_{\mathrm{SD}}}\right)^{k+N_D}}}. \quad (68)$$

REFERENCES

[1] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part I: The MISOME wire-tap channel," *IEEE Trans. Inf. Theory,* vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.,* vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.,* vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[4] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.,* vol. 30, no. 5, pp. 29–40, Sep. 2013.

[5] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.,* vol. 59, no. 1, pp. 351–361, Jan. 2011.

[6] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.,* vol. 61, no. 1, pp. 144–154, Jan. 2013.

[7] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.,* vol. 19, no. 6, pp. 372–375, Jun. 2012.

[8] F. Oggier and B. Hassibi,"The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory,* vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[9] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.,* vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[10] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.,* vol. 63, no.1, pp. 215–218, Jan. 2015.

[11] G. Brante, H. Alves, R. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Trans. Commun.,* vol. 63, no. 4, pp. 1330–1342, Apr. 2015.

[12] Y. Feng, Z. Yang, W.-P. Zhu, Q. Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.,* vol. 66, no. 3, pp. 2354–2366 Mar. 2017

[13] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secrecy analysis of unauthenticated amplify-and-forward relaying with antenna selection," *in Proc. IEEE ICASSP,* Mar. 2012.

[14] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.,* vol. 13, no. 4, pp. 2189–2203, Mar. 2014.

[15] C. Kundu, S. Ghose, and R. Bose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Trans. Commun.,* vol. 14, no. 8, pp. 4614–4625, Aug. 2015.

[16] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.,* vol. 63, no. 5, pp. 1756–1770, May 2015.

[17] Y. Huang, C. Zhong, J. Wang, T. Duong, Q. Wu, and G. Karagiannidis, "Improving the security of cooperative relaying networks with multiple antennas," in *Proc. IEEE VTC Spring*, May 2016, pp. 1–6.

[18] J. N. Laneman, D. N. C. Tse, and G.W.Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory,* vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[19] T. Q. Duong and H. J. Zepernick, "On the performance gain of hybrid decode-amplify-forward cooperative communications," *EURASIP J. Wireless Commun. Netw.*, pp. 1-10, May 2009.

[20] T. Duong and H.-J. Zepernick, "Hybrid decode-amplify-forward cooperative communications with multiple relays," in *Proc. IEEE Wireless Communications and Networking Conference*, Apr. 2009, pp.1-6.

[21] Z. Bai, J. Jia, C.-X. Wang, and D. Yuan, "Performance analysis of SNR-based incremental hybrid decode-amplify-forward cooperative relaying protocol," *IEEE Trans. Commun.,* vol. 63, no. 6, pp. 2094–2106, Jun. 2015.

[22] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, " Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.,* vol. 15, no. 12, pp. 8009–8024, Nov. 2016.

[23] Y. Huang, F. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. Alnuweiri, "Performance analysis of multiuser multiple antenna relaying networks with co-channel interference and feedback delay," *IEEE Trans. Commun.,* vol. 62, no. 1, pp. 59–73, Jan. 2014.

[24] S. Yadav, P. K. Upadhyay, and S. Prakriya, "Performance evaluation and optimization for two-way relaying with multi-antenna sources," *IEEE Trans. Veh. Technol.,* vol. 63, no. 6, pp. 2982–2989, Jul. 2014.

[25] Y. Wu, B. Zhang, X. Yi, and Y. Tang, "Communication-motion planning for wireless telay-assisted multi-robot system," *IEEE Wireless Commun. Lett.,* vol. 5, no. 6, pp. 568–571, Dec. 2016.

[26] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.,* vol. PP, no. 99, pp. 1–1, 2017.

[27] A. Goldsmith, *Wireless Communications*, 1st ed. Cambridge, U.K: Cambridge Univ. Press, 2005.

[28] M. N. Khormuji and E. G. Larsson, "Cooperative transmission based on decode-and-forward relaying with partial repetition coding," *IEEE Trans. Wireless Commun.,* vol. 8, no. 4, pp. 1716–1725, Apr. 2009.

[29] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.,* vol. 62, no. 9, pp. 3299-3310, Sep. 2014.

[30] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.,* vol. 14, no. 11, pp. 6377–6388, May 2015.

[31] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K. K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Theory,* vol. 10, no. 8, pp. 1617-1629, Aug. 2015.

[32] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.,* vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products,* 7th edition. Academic, 2007.

[34] J. Tang and X. Zhang, "Transmit selection diversity with maximalratio combining for multicarrier DS-CDMA wireless networks over Nakagamim fading channels," *IEEE J. Sel. Areas Commun.,* vol. 24, no. 1, pp. 104–112, Jan. 2006.
[35] M. K. Simon and M.-S. Alouini, Digital Communications Over Fading Channels: A Unified Approach to Performance Analysis, 1st ed. New York, NY, USA: Wiley, 2000.
[36] H. Gamal, G. Caire, and M. Damen, "The MIMO ARQ channel: diversity-multiplexing-delay tradeoff," *IEEE Trans. Inf. Theory,* vol. 52, no. 8, pp. 3601–3621, Aug. 2006.
[37] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.,* vol. 10, no. 4, pp. 1212–1223, Apr. 2011.
[38] S. Zhou and B. Li, "BER criterion and codebook construction for finiterate precoded spatial multiplexing with linear receivers," *IEEE Trans. Signal Process.,* vol. 54, no. 5, pp. 1653–1665, May 2006.
[39] Available: http://engineering.purdue.edu/ djlove/grass.html

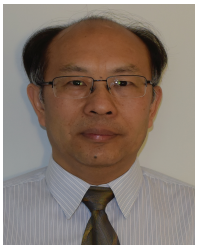
Youhong Feng (S'16) received the B.S. degree and the M.S. degree in information engineering from Chang'an University, Xi'an, China, in 2003 and 2006, respectively. He is currently working toward the Ph.D. degree with Nanjing University of Posts and Telecommunications. He is currently an Associate Professor with the College of Physics and Electronic information Engineering, Anhui Normal University. His research interests include cooperative communications, energy-efficient communications and physical layer security.

Shihao Yan (S'11-M'15) received the Ph.D degree in Electrical Engineering from The University of New South Wales, Sydney, Australia, in 2015. He received the B.S. in Communication Engineering and the M.S. in Communication and Information Systems from Shandong University, Jinan, China, in 2009 and 2012, respectively. He is currently a Postdoctoral Research Fellow in the Research School of Engineering, The Australian National University, Canberra, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, covert wireless communications, and location verification.

Zhen Yang received his B.Eng. and M.Eng. degrees from Nanjing University of Posts and Telecommunications, China in 1983 and 1988, respectively, and his Ph.D. degree from Shanghai Jiao Tong University,China in 1999, all in electrical engineering. He was initially employed as a Lecturer in 1983 by Nanjing University of Posts and Telecommunications, where he was promoted to Associate Professor in 1995 and then a Full Professor in 2000. He was a visiting scholar at Bremen University, Germany during 1992-1993, and an exchange scholar at Maryland University, USA in 2003. His research interests include various aspects of signal processing and communication, such as communication systems and networks, cognitive radio, spectrum sensing, speech and audio processing, compressive sensing and wireless communication. He has published more than 200 papers in academic journals and conferences.

Prof. Yang serves as Vice Chairman and Fellow of Chinese Institute of Communications, Chairman of Jiangsu Institute of Internets, Vice Director of Editorial Board of The Journal on Communications. He is also a Member of Editorial Board for several other journals such as Chinese Journal of Electronics, China Communications, Data Collection and Processing et al, the Chair of APCC(Asian Pacific Communication Conference) Steering Committee during 2013-2014.

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He has been with the Research School of Engineering at the Australian National University since July 2014, where he currently works as a Future Engineering Research Leadership Fellow and a Senior Lecturer. Prior to this, he was a Postdoctoral Research Fellow at the University of New South Wales from 2012 to 2014 and a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012. He received the Exemplary Reviewer Award of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015 and 2016, the Top Reviewer Award from the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, and the Exemplary Reviewer Award of the IEEE COMMUNICATIONS LETTERS in 2013 and 2012. He is also a co-recipient of the Best Paper Awards from the IEEE GlobeCOM 2016 and the IEEE VTC 2013-Spring. He is currently serving in the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. His general research interests lie in the areas of communications theory and signal processing, with specific interests in massive multi-antenna systems, millimeter wave communications, ultra-reliable low latency communications, cyber-physical security, and molecular communications.



Wei-Ping Zhu (SM97) received the B.E. and M.E. degrees from Nanjing University of Posts and Telecommunications, and the Ph.D. degree from Southeast University, Nanjing, China, in 1982, 1985, and 1991, respectively, all in electrical engineering. He was a Postdoctoral Fellow from 1991 to 1992 and a Research Associate from 1996 to 1998 with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. During 1993-1996, he was an Associate Professor with the Department of Information Engineering, Nanjing University of Posts and Telecommunications. From 1998 to 2001, he worked with hi-tech companies in Ottawa, Canada, including Nortel Networks and SR Telecom Inc. Since July 2001, he has been with Concordias Electrical and Computer Engineering Department as a full-time faculty member, where he is presently a Full Professor. Since 2008, he has been an Adjunct Professor at Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include digital signal processing fundamentals, speech and statistical signal processing, and signal processing for wireless communication with a particular focus on MIMO systems and cooperative communication.

Dr. Zhu served as an Associate Editor for the IEEE Transactions on Circuits and Systems Part I: Fundamental Theory and Applications during 2001-2003, an Associate Editor for Circuits, Systems and Signal Processing during 2006-2009, and an Associate Editor for the IEEE Transactions on Circuits and Systems Part II: Transactions Briefs during 2011-2015. He was also a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issues of: Broadband Wireless Communications for High Speed Vehicles, and Virtual MIMO during 2011-2013. Currently, he is an Associate Editor of Journal of The Franklin Institute. Dr. Zhu was the Chair-Elect of Digital Signal Processing Technical Committee (DSPTC) of the IEEE Circuits and System Society during June 2012-May 2014, and the Chair of the DSPTC during June 2014-May 2016.