Channel Training Design in Full-Duplex Wiretap Channels to Enhance Physical Layer Security

Shihao Yan[†], Xiangyun Zhou[†], Nan Yang[†], Thushara D. Abhayapala[†], and A. Lee Swindlehurst[‡]
[†]Research School of Engineering, The Australian National University, Canberra, ACT 0200, Australia
[‡]Center for Pervasive Communications and Computing, University of California, Irvine, CA 92697 USA
Emails: {shihao.yan, xiangyun.zhou, nan.yang, thushara.abhayapala}@anu.edu.au, swindle@uci.edu

***Abstract*—In this work, we propose a new channel training (CT) scheme to enhance physical layer security in a full-duplex wiretap channel, where the multi-antenna and full-duplex receiver simultaneously receives the information signal and transmits artificial noise (AN). In order to suppress the self-interference caused by AN, the receiver has to estimate the self-interference channel prior to the data communication phase. In the proposed CT scheme, the receiver transmits limited pilot symbols which are known only to itself, which prevents the eavesdropper from estimating the jamming channel from the receiver to the eavesdropper, hence effectively degrades the eavesdropping capability. Compared with the traditional CT scheme that uses publicly known pilots, the newly proposed secret CT scheme offers significantly better performance when the number of antennas at the eavesdropper is larger than one, e.g., $N_E > 1$. The optimal power allocation between CT and data/AN transmission at the legitimate transmitter/receiver is determined for the proposed secret CT scheme.**

I. Introduction

Physical layer security is emerging as a promising technique to realize and enhance the secrecy of wireless communications and is also compatible and complementary to the traditional cryptographic techniques [1]. In the pioneering studies of physical layer security (e.g., [2]), a wiretap channel was established as the fundamental model to characterize physical layer security, in which an eavesdropper (Eve) attempts to intercept the data transmission between a transmitter (Alice) and a legitimate receiver (Bob). In the context of multiple-input multiple-output (MIMO) wiretap channels, artificial noise (AN)-aided secure transmission is of growing interesting due to its robustness and desirable performance (e.g., [3–7]). As a result of the full-duplex techniques coming to reality [8], AN was proposed to be transmitted by a full-duplex receiver that can simultaneously receive an information signal and transmit AN to enhance physical layer security (e.g., [9–14]). We refer to the wiretap channel with a full-duplex Bob as the full-duplex wiretap channel.

One of the key challenges faced in designing practical full-duplex transceivers is self-interference and thus many techniques have been developed in the literature to suppress the self-interference [8]. Among the different types of self-interference cancellation techniques, the channel-aware technique has attracted increasing research interests since it is normally the last line of defense against self-interference in the digital domain [8]. In channel-aware self-interference cancellation, the channel state information (CSI) of the self-interference channel (i.e., the channel between the transmit and receive antennas of a full-duplex transceiver) is first estimated and then the self-interference is suppressed by beamforming or subtraction. However, how to perform the self-interference channel estimation and how to allocate transmit power between the channel training (CT) and data transmission have not been addressed in the context of physical layer security. The assumption that the CSI of the self-interference channel is perfectly known is widely adopted in the literature and thus the self-interference can be fully cancelled [9]. This assumption cannot be justified in many practical scenarios in which the self-interference channel consists of not only deterministic direct paths but also random reflected paths from nearby scatterers. This partially motivates this work, which, for the first time, examines CT in the full-duplex wiretap channel.

The assumption that Eve knows the CSI of the jamming channel (i.e., the channel between Bob's transmit antennas and Eve) in the full-duplex wiretap channel is adopted in the literature (e.g., [9, 14]). This assumption ignores one property of the full-duplex wiretap channel, which is that Bob knows exactly the signals he transmits. This means that the pilots used to estimate the self-interference channel are not required to be public. The ignorance of this property in the literature leads to the fact that the benefits of transmitting AN by a full-duplex Bob rather than an external jammer have not been fully exploited. Therefore, our work explores this property to redesign CT in order to enhance physical layer security. We develop, for the first time, a new secret CT scheme based on this property. Specifically, secret pilots are utilized to estimate the self-interference channel in limited symbol periods in order to avoid Eve obtaining the CSI of the jamming channel. In order to maximize the connection probability (CP) subject to a maximum allowable secrecy outage probability (SOP), we determine the optimal transmit power allocation between CT and data/AN transmission at Alice and Bob under average power constraints. Our study show that our proposed secret CT scheme significantly outperforms the traditional CT scheme (which utilizes publicly known pilots to estimate the self-interference channel) when $N_E > 1$, where N_E is the number of antennas at Eve. The performance advantage of our proposed secret CT scheme increases as N_E increases. We further find that the secret CT scheme obtains the same secrecy performance as the traditional CT scheme when $N_E = 1$.

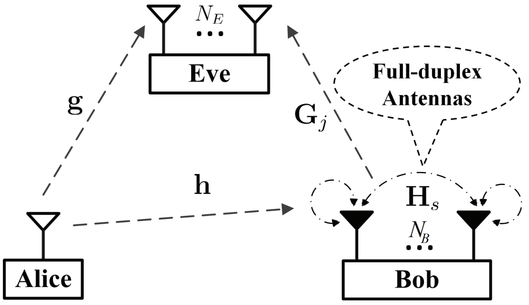

Fig. 1. The full-duplex wiretap channel of interest.

II. System Model

A. Channel Model

The full-duplex wiretap channel of interest is illustrated in Fig. 1, where Alice is equipped with a single antenna, Bob is equipped with N_B full-duplex antennas, and Eve is equipped with N_E antennas. We assume that Bob operates in the full-duplex mode (i.e., all N_B antennas are used for reception and transmission simultaneously). We denote $\mathbf{h} \in \mathbb{C}^{N_B \times 1}$ as the main channel vector, denote $\mathbf{g} \in \mathbb{C}^{N_E \times 1}$ as the channel vector between Alice and Eve (referred to as the eavesdropper's channel), denote $\mathbf{G}_j \in \mathbb{C}^{N_E \times N_B}$ as the jamming channel matrix, and denote $\mathbf{H}_s \in \mathbb{C}^{N_B \times N_B}$ as the self-interference channel matrix. We assume all the wireless channels within our system model are subject to independent quasi-static Rayleigh fading with equal block length[1]. We further assume that the entries of $\mathbf{h}$, $\mathbf{g}$, $\mathbf{G}_j$, and $\mathbf{H}_s$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero-mean. We adopt the assumption that the variance of each entry in $\mathbf{h}$, $\mathbf{g}$, and $\mathbf{G}_j$ is normalized to one, but the variance of each entry in $\mathbf{H}_s$ is σ_s^2. This assumption is to keep the generality of these channels, since the fading variances (including path loss) of $\mathbf{h}$, $\mathbf{g}$, and $\mathbf{G}_j$ can be effectively absorbed into the noise variance at Bob and the transmit powers of Alice and Bob, while the fading variance of $\mathbf{H}_s$ is quantified by σ_s^2.

We assume that the total duration of each block consists of T symbol periods, including pilot and data symbols. In the pilot symbol periods, Alice and Bob send pilots to enable the estimation of the main channel and the self-interference channel, respectively. The pilots used by Alice is publicly known. In the data symbol periods, Alice transmits confidential information to Bob while the full-duplex Bob sends AN to aid this secure transmission. We denote Alice's transmit powers for pilots and data by $\mathcal{P}_{Ap}$ and $\mathcal{P}_{Ad}$, respectively. We also denote Bob's transmit powers for pilots and AN by $\mathcal{P}_{Bp}$ and $\mathcal{P}_{Ba}$, respectively. We consider an average power constraint over a fading block [15], in which the total energy for a fading block at Alice and/or Bob is subject to a fixed upper bound. We also consider the passive eavesdropping scenario, in which Alice does not know the CSI of the eavesdropper's channel. In practice, it is difficult, if not impossible, to know the noise at Eve. As such, we adopt the worst-case scenario where the noise at Eve is zero, which is widely used in the literature (e.g., [4]).

B. Transmission Strategy and Performance Metrics

In the data symbol periods, Alice adopts a fixed-rate wiretap code that can be described using two rate parameters, namely, the codeword rate R_B and the redundancy rate R_E, which are predetermined and fixed [16]. The actual information rate is given by $R_B - R_E$. For such a transmission scheme, Bob cannot reliability decode the transmitted information when the capacity of the main channel is less than R_B, while perfect secrecy against Eve fails when the capacity of the eavesdropper's channel is larger than R_E [16]. We refer to the probability of achieving reliable decoding as CP and refer to the probability of failing to achieve perfect secrecy as SOP. The CP and SOP exist for the considered full-duplex wiretap channel due to channel estimation errors. The CP is the probability that Bob can decode the message for a given R_B with a negligible decoding error probability, which is given by

$$P_c = \Pr(\log_2(1+\gamma_B) \geq R_B). \tag{1}$$

Likewise, the SOP is the probability that the capacity of the eavesdropper's channel is less than R_E, which is given by

$$P_{so} = \Pr\left(\log(1+\gamma_E) > R_E\right). \tag{2}$$

As mentioned above, data transmission in the considered full-duplex wiretap channel may incur connection and secrecy outages. Considering block fading channels, we adopt the effective throughput subject to a given secrecy constraint as our key performance metric, which is given by [16]

$$\eta = \frac{T-N_B-1}{T}(R_B - R_E)P_c, \quad \text{s.t.} \quad P_{so} \leq \epsilon, \tag{3}$$

where ϵ is the maximum allowable SOP (i.e., the predetermined secrecy requirement of the system). We note that in this work T, R_B, and R_E are *a priori* determined. As such, the maximization of η subject to $P_{so} \leq \epsilon$ is equivalent to the following optimization

$$\max P_c, \quad \text{s.t.} \quad P_{so} \leq \epsilon. \tag{4}$$

III. Secret Channel Training Scheme

In the full-duplex wiretap channel, the pilots sent by Bob to estimate the self-interference channel can be kept secret to Eve (i.e., the pilots are secret and unknown to Eve). This is due to the fact that Bob knows exactly what he transmits and thus it is not necessary to *a priori* share his pilots with other devices to conduct the self-interference channel estimation. As such,

[1] The self-interference channel considered throughout this work is the effective self-interference channel after channel-unaware interference cancellation. Based on [8] we know that the deterministic components in the self-interference channel can be removed through channel-unaware interference cancellation and thus it is reasonable to assume the self-interference channel after the channel-unaware cancellation is subject to independent quasi-static Rayleigh fading.

in this section we develop a specific CT strategy dedicated to the full-duplex wiretap channel, which is named as the secret CT scheme.

A. Secret Channel Training

In this secret CT scheme, we first set $T_B = N_B$, where T_B is the number of symbol periods used to estimate the self-interference channel $\mathbf{H}_s$. This assumption is to guarantee a reliable estimate of $\mathbf{H}_s$ at Bob according to the principle of the Linear Minimum Mean Square Error (LMMSE) estimation (i.e., if $T_B < N_B$ Bob cannot achieve a reliable estimate of $\mathbf{H}_s$) [17]. We note that $T_B = N_B$ is also a hard requirement for the secret CT scheme since when $T_B > N_B$ Eve can obtain partial information about the jamming channel $\mathbf{G}_j$ through blind channel estimation [18] even though she does not know the pilots sent by Bob. Setting $T_B = N_B$ guarantees that the estimation problem of $\mathbf{G}_j$ at Eve is ill-posed due to the unknown pilots (from the signal processing point of view), and thus Eve cannot achieve any information about $\mathbf{G}_j$ in the secret CT scheme.

To enable Bob to estimate the main channel, Alice transmits its publicly known pilots. We note that Alice and Bob have to transmit pilots in different symbol periods in order to achieve orthogonality between Alice's and Bob's pilots, due to the constraint $T_B = N_B$. In this work, we set the number of symbol periods used to estimate the main channel to be 1 since Alice is equipped with a single antenna. We note that prior studies on optimal training resource allocation have shown that the optimal number of pilot equals the number of transmit antennas (which is N_B for the self-interference channel and 1 for the main channel in this work), under the average power constraint [15].

When Alice transmits the pilot, the corresponding received signal at Bob is given by $\mathbf{z}_A = \sqrt{\mathcal{P}_{Ap}}\mathbf{h}s_A + \mathbf{w}_B$, where $\mathbf{z}_A \in \mathcal{C}^{N_B\times 1}$, $s_A \in \mathcal{C}^{1\times 1}$ is the pilot transmitted by Alice satisfying $s_A s_A^\dagger = 1$, and $\mathbf{w}_B \in \mathcal{C}^{N_B\times 1}$ is the noise at Bob with i.i.d entries, each of which follows the distribution $\mathcal{CN}(0, \sigma_B^2)$. Considering the LMMSE estimator, based on the known pilot Bob achieves the estimate of $\mathbf{h}$ as [17]

$$\hat{\mathbf{h}} = \frac{\sqrt{\mathcal{P}_{Ap}}}{\mathcal{P}_{Ap} + \sigma_B^2}\mathbf{z}_A s_A^\dagger. \tag{5}$$

Based on the properties of LMMSE [17], the entries of $\hat{\mathbf{h}}$ are i.i.d and each of them follows the distribution $\mathcal{CN}(0, \sigma_{\hat{h}}^2)$, where

$$\sigma_{\hat{h}}^2 = \frac{\mathcal{P}_{Ap}}{\mathcal{P}_{Ap} + \sigma_B^2}. \tag{6}$$

Again, due to the properties of LMMSE, the estimation error $\tilde{\mathbf{h}} = \mathbf{h} - \hat{\mathbf{h}}$ is independent of $\hat{\mathbf{h}}$ and the entries of $\tilde{\mathbf{h}}$ are i.i.d, each of which follows the distribution $\mathcal{CN}(0, \sigma_{\tilde{h}}^2)$, where

$$\sigma_{\tilde{h}}^2 = \frac{\sigma_B^2}{\mathcal{P}_{Ap} + \sigma_B^2}. \tag{7}$$

Since Alice's pilot is publicly known, Eve can obtain perfect CSI of the eavesdropper's channel $\mathbf{g}$ in the worst-case scenario (i.e., when the receive noise at Eve is zero).

When Bob transmits pilots over N_B symbol periods with his N_B full-duplex antennas, the signal at his receive antennas is given by $\mathbf{Z}_B = \sqrt{\mathcal{P}_{Bp}}\mathbf{H}_s\mathbf{S}_B + \mathbf{W}_B$, where $\mathbf{Z}_B \in \mathcal{C}^{N_B\times N_B}$, $\mathbf{S}_B \in \mathcal{C}^{N_B\times N_B}$ are the pilots transmitted by Bob satisfying $\mathbf{S}_B\mathbf{S}_B^\dagger = \mathbf{I}_{N_B}$, and $\mathbf{W}_B \in \mathcal{C}^{N_B\times N_B}$ is the noise at Bob with i.i.d entries, each of which follows the distribution $\mathcal{CN}(0, \sigma_B^2)$. Again, adopting the LMMSE estimator (based on the known $\mathbf{S}_B$ and σ_s^2) Bob obtains the estimate of $\mathbf{H}_s$ as

$$\hat{\mathbf{H}}_s = \frac{\sqrt{\mathcal{P}_{Bp}}\sigma_s^2}{\mathcal{P}_{Bp}\sigma_s^2 + \sigma_B^2}\mathbf{Z}_B\mathbf{S}_B^\dagger. \tag{8}$$

Likewise, the estimation error $\tilde{\mathbf{H}}_s = \mathbf{H}_s - \hat{\mathbf{H}}_s$ is independent of $\hat{\mathbf{H}}_s$ and each of its entries follows the distribution $\mathcal{CN}(0, \sigma_{\tilde{H}}^2)$, where

$$\sigma_{\tilde{H}}^2 = \frac{\sigma_B^2\sigma_s^2}{\mathcal{P}_{Bp}\sigma_s^2 + \sigma_B^2}. \tag{9}$$

When Bob transmits the pilots $\mathbf{S}_B$, the received signal matrix at Eve in the worst-case scenario is given by

$$\mathbf{Z}_E = \sqrt{\mathcal{P}_{Bp}}\mathbf{G}_j\mathbf{S}_B. \tag{10}$$

We note $\mathbf{Z}_E \in \mathcal{C}^{N_E\times N_B}$ and in order to prevent Eve from achieving any information on $\mathbf{G}_j$ we have to guarantee $N_E \leq N_B$. Otherwise (i.e., if $N_E > N_B$), Eve can learn the null space of $\mathbf{G}_j$ through performing a singular value decomposition (SVD) on $\mathbf{Z}_E$ and this null space can be utilized to cancel the AN transmitted by Bob. As such, the secrecy CT scheme requires $N_E \leq N_B$. We would like to highlight that this requirement is solely due to the considered worst-case scenario where the noise at Eve is zero. This requirement has also to be met in the traditional CT scheme (e.g., [4]).

B. Data Transmission with AN following Secret CT

In the data symbol periods, Alice transmits a data stream while Bob transmits AN to confuse Eve. In addition to Eve, the AN also causes interference to Bob through the self-interference channel due to channel estimation errors. In general, Bob has two strategies to suppress such interference based on the estimated self-interference channel $\hat{\mathbf{H}}_s$. First, Bob can subtract the known part of AN based on $\hat{\mathbf{H}}_s$ at his receive antennas since Bob knows AN he transmits. Second, Bob can transmit AN in the null space of $\hat{\mathbf{H}}_s$, which leads to the fact that AN that lies in the null space of $\hat{\mathbf{H}}_s$ does not cause any interference to Bob. We note that the second approach requires that the number of Bob's transmit antennas is greater than that of his receive antennas, which is not satisfied in our system model. Therefore, in this work we assume that Bob adopts the first strategy to suppress the interference caused by the AN.

The received signal at Bob in each data symbol period is given by

$$\mathbf{y}_B = \sqrt{\mathcal{P}_{Ad}}\mathbf{h}x + \sqrt{\frac{\mathcal{P}_{Ba}}{N_B}}\mathbf{H}_s\mathbf{n} + \mathbf{v}_B, \tag{11}$$

$$= \sqrt{\mathcal{P}_{Ad}}(\hat{\mathbf{h}}+\tilde{\mathbf{h}})x + \sqrt{\frac{\mathcal{P}_{Ba}}{N_B}}(\hat{\mathbf{H}}_s+\tilde{\mathbf{H}}_s)\mathbf{n} + \mathbf{v}_B, \tag{12}$$

where $x \in \mathcal{C}^{1\times 1}$ denotes the transmitted signal satisfying $\mathbb{E}[|x|^2] = 1$, $\mathbf{n} \in \mathcal{C}^{N_B\times 1}$ is the AN vector, whose entries are i.i.d circularly-symmetric complex normal random variables with zero mean and unit variance, and $\mathbf{v}_B \in \mathcal{C}^{N_B\times 1}$ is the noise vector at Bob with i.i.d entries, each of which follows the distribution $\mathcal{CN}(0, \sigma_B^2)$. Knowing $\hat{\mathbf{H}}_s$ and $\mathbf{n}$, Bob can remove $\hat{\mathbf{H}}_s\mathbf{n}$ from $\mathbf{y}_B$ and obtain the effective received signal as

$$\mathbf{y}'_B = \sqrt{\mathcal{P}_{Ad}}\hat{\mathbf{h}}x + \sqrt{\mathcal{P}_{Ad}}\tilde{\mathbf{h}}x + \sqrt{\frac{\mathcal{P}_{Ba}}{N_B}}\tilde{\mathbf{H}}_s\mathbf{n} + \mathbf{v}_B. \quad (13)$$

Although Bob knows that his received signal is subject to the interference caused by the channel estimation errors in $\mathbf{h}$ and $\mathbf{H}_s$, he cannot suppress such interference since he does not know $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{H}}_s$. As such, the optimal combining technique that maximizes the signal-to-interference-plus-noise ratio (SINR) at Bob is maximum ratio combining (MRC) based on $\hat{\mathbf{h}}$ (since the entries of $\hat{\mathbf{h}}$, $\tilde{\mathbf{h}}$, $\hat{\mathbf{H}}_s$, $\tilde{\mathbf{H}}_s$ are independent), which leads to the instantaneous SINR at Bob as

$$\gamma_B = \frac{\mu_B\|\hat{\mathbf{h}}\|^2}{\frac{\mu_B|\hat{\mathbf{h}}^\dagger\tilde{\mathbf{h}}|^2}{\|\hat{\mathbf{h}}\|^2} + \frac{\mu_S\|\hat{\mathbf{h}}^\dagger\tilde{\mathbf{H}}_s\|^2}{N_B\|\hat{\mathbf{h}}\|^2} + 1}, \quad (14)$$

where $\mu_B = \mathcal{P}_{Ad}/\sigma_B^2$ and $\mu_S = \mathcal{P}_{Ba}/\sigma_B^2$.

Likewise, the received signal at Eve in one data symbol period is given by

$$\mathbf{y}_E = \sqrt{\mathcal{P}_{Ad}}\mathbf{g}x + \sqrt{\frac{\mathcal{P}_{Ba}}{N_B}}\mathbf{G}_j\mathbf{n}. \quad (15)$$

Although Eve knows that her received signal is subject to the interference caused by the AN, she cannot suppress such interference since she does not know $\mathbf{G}_j$ as discussed in Section II-B. As such, the optimal combining technique that maximizes the signal-to-interference ratio (SIR) at Eve is MRC based on the CSI of the eavesdropper's channel $\mathbf{g}$. Following (15) and applying MRC, the SIR at Eve for the secret CT scheme is given by

$$\gamma_E = \frac{\mathcal{P}_{Ad}N_B}{\mathcal{P}_{Ba}}\frac{\|\mathbf{g}\|^2}{\left\|\frac{\mathbf{g}^\dagger\mathbf{G}_j}{\|\mathbf{g}\|}\right\|^2}. \quad (16)$$

C. Traditional Channel Training Scheme as a Benchmark

In order to better illustrate the benefits of the secret CT scheme, we now consider the traditional CT scheme as a benchmark. Unlike the secret CT scheme, in the traditional CT scheme the pilot transmitted by Bob (i.e., $\mathbf{S}_B$) is publicly known, which can be jointly designed with the pilot transmitted by Alice (i.e., s_A). As such, in the traditional CT scheme we do not need the constraint $T_B = N_B$ because Bob's pilots are known by Eve anyway. Hence, Alice and Bob can simultaneously transmit pilots over $1 + N_B$ symbol periods while still ensuring the orthogonality of their pilots. This setting also guarantees a fair comparison between the secret CT scheme and the traditional CT scheme, since the total number of symbol periods allocated to CT is $1 + N_B$ in both schemes. Therefore, $\sigma_{\hat{h}}^2$, $\sigma_{\tilde{h}}^2$, and $\sigma_{\tilde{H}}^2$ (which are given by (6), (7), and (9), respectively, in the secret CT scheme) for the traditional CT scheme should be updated accordingly.

In the traditional CT scheme, the pilot $\mathbf{S}_B$ is public and thus Eve can obtain perfect CSI for the jamming channel $\mathbf{G}_j$ in the worst-case scenario (where the noise at Eve is zero). Since Eve knows that her received signal is subject to the interference caused by the AN transmitted by Bob, the optimal combining technique that maximizes the SIR at Eve is MMSE based on $\mathbf{g}$ and $\mathbf{G}_j$. Following (15) and applying the MMSE combiner, for the traditional CT scheme the instantaneous SIR at Eve is given by

$$\gamma_E = \frac{\mathcal{P}_{Ad}N_B}{\mathcal{P}_{Ba}}\mathbf{g}^\dagger\left(\mathbf{G}_j\mathbf{G}_j^\dagger\right)^{-1}\mathbf{g}. \quad (17)$$

We note that (17) is only valid when $\mathbf{G}_j\mathbf{G}_j^\dagger$ is invertible. Otherwise, Eve can perfectly cancel the interference caused by AN and thus the SIR given in (17) approaches infinity. As such, the traditional CT scheme does also require $N_E \le N_B$ in order to guarantee interference at Eve (e.g., [4]).

IV. Optimal Power Allocation within the Secret Channel Training Scheme

In this section, we determine the optimal transmit power allocation between CT and data/AN transmission at Alice and Bob under average power constraints in order to maximize the CP for a maximum allowable SOP.

In this work, we consider the average power constraint at both Alice and Bob. Following (4) the power allocation optimization for the secret CT scheme can be presented as

$$\max_{\mathcal{P}_{Ap},\mathcal{P}_{Ad},\mathcal{P}_{Bp},\mathcal{P}_{Ba}} \; P_c, \quad (18)$$

$$\text{s.t.} \quad P_{so} \le \epsilon, \quad (19)$$

$$\mathcal{P}_{Ap} + \mathcal{P}_{Ad}(T - N_B - 1) \le \mathcal{E}_A, \quad (20)$$

$$\mathcal{P}_{Bp}N_B + \mathcal{P}_{Ba}(T - N_B - 1) \le \mathcal{E}_B, \quad (21)$$

where $\mathcal{E}_A$ and $\mathcal{E}_B$ are the total powers available at Alice and Bob for each block of T symbol periods (hence, the average power constraints per symbol for Alice and Bob are $\mathcal{E}_A/T$ and $\mathcal{E}_B/T$), respectively. We next detail how to determine the solution to (18) (i.e., the optimal values of $\mathcal{P}_{Ad}$, $\mathcal{P}_{Ap}$, $\mathcal{P}_{Ba}$, and $\mathcal{P}_{Bp}$) in the following theorem.

Theorem 1: The optimal value of $\mathcal{P}_{Ad}$ that maximizes P_c subject to the constraints given in (19), (20), and (21) can be obtained through

$$\mathcal{P}_{Ad}^* = \underset{0<\mathcal{P}_{Ad}<\mathcal{P}_{Ad}^m}{\operatorname{argmax}} \; P_c(\mathcal{P}_{Ap}^\dagger, \mathcal{P}_{Ad}, \mathcal{P}_{Bp}^\dagger, \mathcal{P}_{Ba}^\dagger), \quad (22)$$

where

$$\mathcal{P}_{Ad}^m = \min\left\{\frac{\mathcal{E}_A}{T - N_B - 1}, \frac{\mathcal{E}_B}{\tau^*(T - N_B - 1)}\right\}, \quad (23)$$

$$\mathcal{P}_{Ap}^\dagger = \mathcal{E}_A - \mathcal{P}_{Ad}(T - N_B - 1), \quad (24)$$

$$\mathcal{P}_{Ba}^\dagger = \tau^*\mathcal{P}_{Ad}, \quad (25)$$

$$\mathcal{P}_{Bp}^\dagger = \frac{\mathcal{E}_B - \tau^*\mathcal{P}_{Ad}(T - N_B - 1)}{N_B}, \quad (26)$$

and τ^* can be obtained by solving the following equation

$$P_{so}(\tau^*) = \epsilon. \quad (27)$$

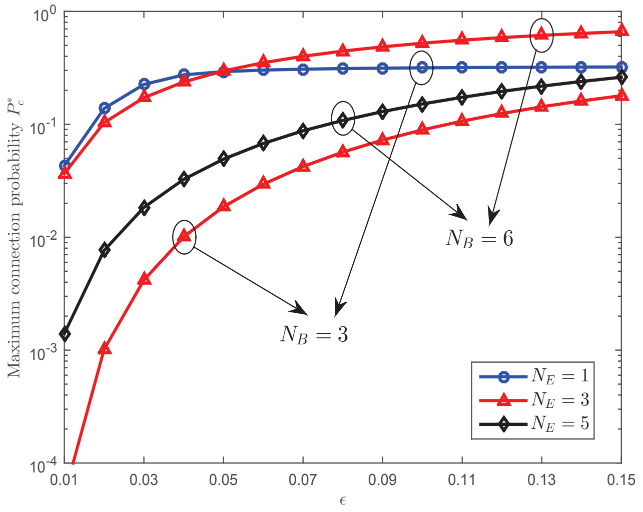

Fig. 2. The maximum connection probability of the secret CT scheme versus the secrecy constraint ϵ for different values of N_B and N_E, where $R_B = 5$, $R_E = 3$, $T = 300$, $\mathcal{E}_A/T = \mathcal{E}_B/T = 10$dB, $\sigma_s^2 = 1$, and $\sigma_B^2 = 1$.

Then, the optimal values of $\mathcal{P}_{Ap}$, $\mathcal{P}_{Ba}$, and $\mathcal{P}_{Bp}$ are functions of $\mathcal{P}_{Ad}^*$ given as follows

$$\mathcal{P}_{Ap}^* = \mathcal{E}_A - \mathcal{P}_{Ad}^*(T - N_B - 1), \tag{28}$$

$$\mathcal{P}_{Ba}^* = \tau^*\mathcal{P}_{Ad}^*, \tag{29}$$

$$\mathcal{P}_{Bp}^* = \frac{\mathcal{E}_B - \tau^*\mathcal{P}_{Ad}^*(T - N_B - 1)}{N_B}. \tag{30}$$

Proof: We first note that both P_{so} and P_c are both monotonically decreasing functions of $\mathcal{P}_{Ba}$ (since as shown in (14) and (16) both γ_B and γ_E decrease as $\mathcal{P}_{Ba}$ increases). As such, $P_{so} = \epsilon$ is always achieved in order to maximize P_c subject to the secrecy constraint (19). Otherwise (i.e., if $P_{so} < \epsilon$), we can decrease $\mathcal{P}_{Ba}$ to increase P_c. Following (16), we note that P_{so} only depends on the ratio of $\mathcal{P}_{Ba}$ to $\mathcal{P}_{Ad}$ (i.e., τ) but not the specific values of $\mathcal{P}_{Ba}$ or $\mathcal{P}_{Ad}$. As such, we can obtain τ^* through solving (27). As per $\tau = \mathcal{P}_{Ba}/\mathcal{P}_{Ad}$, we obtain (25). We also note that P_{so} is not a function of $\mathcal{P}_{Ap}$ or $\mathcal{P}_{Bp}$ as per (16), while P_c monotonically increases as $\mathcal{P}_{Ap}$ or $\mathcal{P}_{Bp}$ increases as per (14). Then, we can conclude that the equality in both (20) and (21) is always guaranteed, which leads to (24) and (26), respectively. Finally, (23) is achieved due to $\mathcal{P}_{Ap} > 0$ and $\mathcal{P}_{Bp} > 0$. ■

By substituting $\mathcal{P}_{Ad}^*$, $\mathcal{P}_{Ap}^*$, $\mathcal{P}_{Ba}^*$, and $\mathcal{P}_{Bp}^*$ into (1), we can obtain the maximum CP of the secret CT scheme.

V. Numerical Results

In this section, we present numerical results to examine the secrecy performance of the proposed secret CT scheme with the traditional CT scheme as the benchmark.

In Fig. 2 we plot the maximum CP of the secret CT scheme versus the secrecy constraint indicator ϵ for different values of N_B and N_E. We first observe that as ϵ increases the maximum CP increases, which demonstrates the tradeoff between the effective throughput and the secrecy constraint. For example, by comparing the values of the maximum CP for $\epsilon = 0.01$ and $\epsilon = 0.15$ we can see that the cost in terms of the reduction in the maximum CP to achieve secrecy is significant. We also observe that the maximum CP decreases as N_E increases or N_B decreases, which is mainly due to the fact that the SOP increases as N_E increases or N_B decreases.

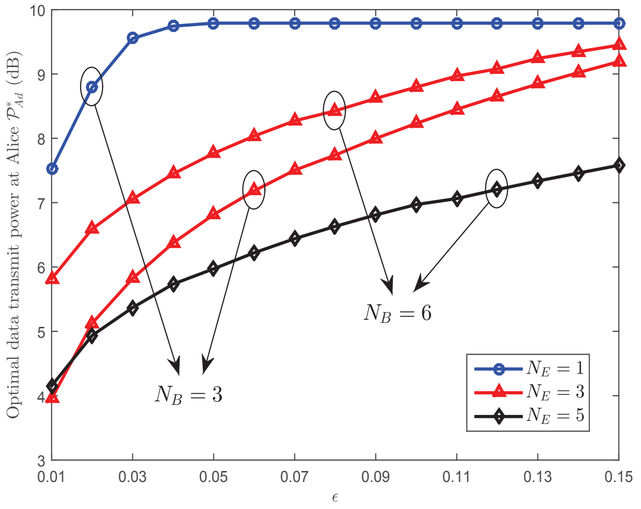

Fig. 3. Alice's optimal data transmit power $\mathcal{P}_{Ad}^*$ versus the secrecy constraint ϵ for different values of N_B and N_E, where $R_B = 5$, $R_E = 3$, $T = 300$, $\sigma_s^2 = 1$, $\mathcal{E}_A/T = \mathcal{E}_B/T = 10$dB, and $\sigma_B^2 = 1$.

Under the same settings of Fig. 2, we plot Alice's optimal transmit power for data (i.e., $\mathcal{P}_{Ad}^*$) and Bob's optimal transmit power for AN (i.e., $\mathcal{P}_{Ba}^*$) versus ϵ in Fig. 3 and Fig. 4, respectively. We first observe that $\mathcal{P}_{Ad}^*$ increases as ϵ increases in Fig. 3, which demonstrates that more transmit power is allocated to data transmission as the secrecy constraint is relaxed. We also observe that $\mathcal{P}_{Ba}^*$ decreases as ϵ increases in Fig. 4, which demonstrates that as the secrecy constraint is relaxed less transmit power is allocated to AN at Bob. These two observations confirm that as ϵ increases the optimal power ratio τ^* decreases since the SOP is a monotonically increasing function of τ. In Fig. 3, we also observe that more transmit power is allocated to data transmission at Alice as N_E decreases or N_B increases. In Fig. 4, we also observe that less transmit power is allocated to AN at Bob as N_E decreases or N_B increases. Overall, we can conclude that more transmit power is allocated to data transmission at Alice and less transmit power is allocated to AN at Bob as Eve becomes weaker or Bob becomes more powerful.

We now consider the scenario where Bob and Eve have the same number of antennas, i.e., $N_B = N_E = N$, to compare the secrecy performance of the secret and traditional CT schemes. In Fig. 5 we plot the maximum reliable probabilities of the secret and traditional CT schemes versus N. In this figure, we first observe that for $N = 1$ our proposed secrecy CT achieves the same maximum CP as the traditional CT scheme. This can be explained by the fact that the SOP for the secret CT scheme is the same as that for the traditional CT

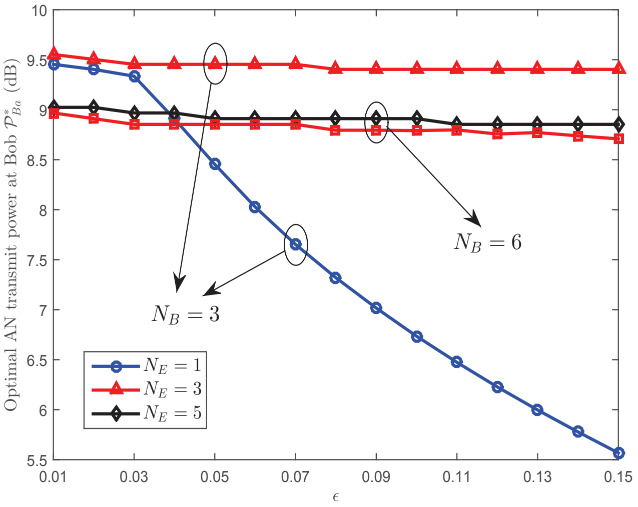

Fig. 4. Bob's optimal AN transmit power $\mathcal{P}^*_{Ba}$ versus the secrecy constraint ϵ for different values of N_B and N_E, where $R_B = 5$, $R_E = 3$, $T = 300$, $\sigma_s^2 = 1$, $\mathcal{E}_A/T = \mathcal{E}_B/T = 10$dB, and $\sigma_B^2 = 1$.

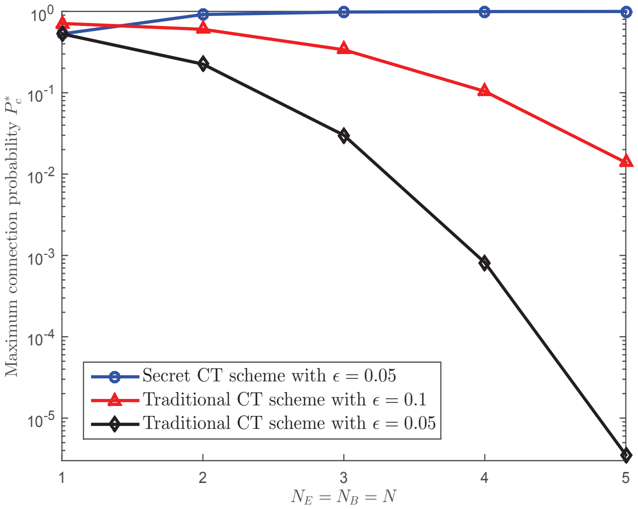

Fig. 5. Maximum connection probability versus N, where $N_B = N_E = N$, $R_B = 2$, $R_E = 1$, $T = 300$, $\sigma_s^2 = 1$, $\mathcal{E}_A/T = 10$dB, $\mathcal{E}_B/T = 20$dB, and $\sigma_B^2 = 1$.

scheme for $N = 1$ and the number of symbol periods allocated to CT in both the secret CT scheme and the traditional CT scheme is optimal under average power constraints. We also observe that for $N > 1$ our proposed secret CT scheme significantly outperforms the traditional CT scheme in terms achieving a much higher maximum CP. Specifically, the secret CT scheme with $\epsilon = 0.05$ even achieves a much higher maximum CP than the traditional CT scheme with $\epsilon = 0.1$ when $N > 1$. This is due to the fact that the secret CT scheme prevents Eve from obtaining the CSI of the jamming channel.

VI. Conclusion

This work devised a new secret CT scheme based on the property of the full-duplex wiretap channel in which Bob knows exactly what he transmits. Our studies show that when $N_E > 1$ the secret CT scheme significantly outperforms the traditional CT scheme in terms of achieving a much higher CP subject to the same secrecy constraint, and when $N_E = 1$ they achieve the same secrecy performance. The secrecy performance improvement of the secret CT scheme relative to the traditional CT scheme increases as N_E increases.

Acknowledgments

This work was supported by the Australian Research Council's Discovery Projects (DP150103905).

References

[1] 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.

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

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[4] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[5] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[6] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[7] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, accepted to appear, DOI: 10.1109/ACCESS.2017.2653182, Jan. 2017.

[8] A. Sabharwal, P. Schniter, D. Guo, D. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

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

[10] L. Li, Z. Chen, and J. Fang, "A full-duplex Bob in the MIMO Gaussian wiretap channel: Scheme and performance," *IEEE Signal Process. Lett.*, vol. 21, no. 1, pp. 107–111, Jan. 2016.

[11] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, pp. 1628–1631, Oct. 2012.

[12] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[13] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Full-duplex wiretap channels: security enhancement via antenna switching," in *Proc. IEEE GlobeCOM TCPLS Workshop*, Dec. 2014, pp. 1412–1417.

[14] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[15] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[16] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[17] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1993.

[18] L. Tong and S. Perreau, "Multichannel blind identification: From subspace to maximum likelihood methods," *Proc. IEEE*, vol. 86, no. 10, pp. 1951–1968, Oct. 1998.