Anti-Eavesdropping Channel Estimation Using Multi-Antenna Half-Duplex Radios

Yingbo Hua
Department of ECE, University of California at Riverside, Riverside, California, 92521, USA

MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM) | 978-1-6654-3956-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/MILCOM52596.2021.9652986

***Abstract*—This paper reviews the basic principles of prior methods for the purpose of wireless anti-eavesdropping channel estimation (ANECE), and highlights their major shortcomings and limitations such as failure for carrier synchronization without a pilot and limited transmission range of a full-duplex radio. This paper also proposes and analyses a new scheme of ANECE using multi-antenna half-duplex radios. This new scheme consists of three phases of transmissions between two radio nodes (Alice and Bob). In phase 1, Bob sends out a pilot via one of his antennas so that Alice can carry out carrier synchronization and channel estimation. In phase 2, Alice sends out a pilot via one of her antennas so that Bob can carry out carrier synchronization and channel estimation. In phase 3, perfectly synchronized with phase 2, Alice applies transmit beamforming and sends out a stream of information via all her other antennas. This new scheme of ANECE for multi-antenna half-duplex radios is derived from an ANECE design for antenna-isolation based full-duplex radios.**

***Index Terms*—Wireless network security, physical layer security, channel estimation, anti-eavesdropping.**

I. Introduction

Information security for wireless communication networks has been a research problem of great interest. There are many situations where physical layer security is needed in addition to cryptography based security implemented at higher layers. One of the key strategies for physical layer security is to prevent eavesdroppers/adversaries from getting their receive channel state information with respect to a source node transmitting secret information.

There have been many works for the above stated purpose, which can be found under such terms as anti-eavesdropping channel estimation (ANECE) [1], [2], [3], discriminative channel estimation (DCE) [4], [5], [6], conjugate and return [8], and others [7], [9]. Unlike ANECE, the other prior works tried to achieve the purpose of ANECE by sending either no or very noisy pilot from a node which needs to send a secret information or a random sequence. As discussed later in section II, this approach cannot work due to failure of carrier synchronization without pilot.

The prior schemes of ANECE [1], [2], [3] exploit a unique property of full-duplex radios by letting two or more cooperative nodes transmit concurrently to each other specially designed pilots. These pilots prevent eavesdroppers from obtaining consistent estimates of their receive channel state information, but at the same time allow each cooperative node to obtain its consistent channel estimation. A basic principle of the prior ANECE, referred to as ANECE-1 here, is reviewed in section III where limitations of practical full-duplex radios are also discussed.

In section IV, we consider a modification of ANECE, referred to as ANECE-2, for antenna-isolation based full-duplex radios. Such full-duplex radios are easier to implement than those based on radio frequency (RF) circulator on each full-duplex antenna. More importantly, with a careful examination of ANECE-2, we show a surprising result referred to as ANECE-3 as detailed in section V.

ANECE-3 uses only half-duplex radios although one of the two cooperative nodes needs to have more than one antennas. ANECE-3 consists of three phases. In phase 1, one node (Bob) sends a pilot via one of his antennas, which allows the other node (Alice) to perform channel estimation. In phases 2 and 3, respectively, Alice sends a pilot and a stream of symbols with perfect synchronization between them. But in phase 2, Alice uses one of her antennas while in phase 3 she uses the other antennas. ANECE-3 appears to be the only known scheme that can achieve the purpose of ANECE while using only half-duplex radios without the issue of carrier synchronization.

II. Earlier History

Many earlier works such as [4], [5], [6], [7], [8], [9] proposed schemes for (discriminative) channel estimation between a pair of legitimate transceivers (Alice and Bob) and, at the same time, preventing eavesdropper (Eve) from estimating successfully its receive channel state information. There is a fundamental commonality in all those works, which is the (implicit) *assumption* that if a (radio) transmitter transmits a baseband random signal $r(k)$ without a pilot or with a however noisy pilot, any receiver can successfully conduct a carrier (frequency and phase) synchronization and the following standard baseband channel model applies:

$$y(k) = Qr(k) + n(k) \tag{1}$$

where $y(k)$ is the (demodulated) baseband representation of the signal received by the receiver, Q is supposed to be a time-invariant channel gain within each channel coherence period, and $n(k)$ is the channel noise. (In this paper, all symbols like $n(k)$, $\mathbf{n}(k)$ and $\mathbf{N}$ represent the noise terms.)

But the above assumption is incorrect. Without knowing any of the symbols transmitted within an independent transmission session, the receiver has no way to calibrate its radio carrier phase (to say the least) with respect to the transmitter. This means that without a pilot, Q would vary randomly from one transmission session to another even within the same (antenna-to-antenna) channel coherence period. In general, without a pilot, the signal received by a receiver (after demodulation) should have the following form

$$y(k) = \eta h e^{j\theta + j\Delta_f k} r(k) + n(k) \tag{2}$$

where h is invariant within a coherence period, Δ_f is proportional to the difference of the carrier frequencies at transmitter and receiver, and η and θ can be random from one transmission to another within the same (antenna-to-antenna) coherence period. The incorrect assumption behind many of the prior works makes their proposed schemes impossible to implement. An ideal phase-locked-loop could make $\Delta_f = 0$ but still leaves θ completely unknown.

To be more specific, let us consider a key example of prior ideas (e.g., see a discussion in [7]) as illustrated in Fig. 1. Here, Bob (with a single antenna) first sends a pilot $p(k)$ with $k = 1, \cdots, K_1$, and then Alice (with multiple antennas) receives

$$\mathbf{y}_A(k) = \mathbf{h}p(k) + \mathbf{n}_A(k) \tag{3}$$

with $k = 1, \cdots, K_1$. With a sufficient SNR in $\mathbf{y}_A(k)$, Alice is able to accurately estimate $\mathbf{h}$, which is the reciprocal channel vector between Alice and Bob. Then Alice sends out $\mathbf{x}_A(k) = \frac{1}{\|\mathbf{h}\|}\mathbf{h}^* s(k)$ with $k = 1, \cdots, K_2$ where $s(k)$ is a sequence of information symbols meant for Bob. If Bob's carrier is synchronized with Alice's, then the (demodulated baseband) signal received by Bob is

$$y_B(k) = \mathbf{h}^T \mathbf{x}_A(k) + n_B(k) = \|\mathbf{h}\| s(k) + n_B(k) \tag{4}$$

with $k = 1, \cdots, K_2$. Given this $y_B(k)$, Bob would be able to detect the information in $s(k)$ (assuming phase-shift-keying) without the knowledge of $\mathbf{h}$.

However, if Bob does not know any of $s(k)$ in $\mathbf{x}_A(k)$, then Bob is not able to synchronize with Alice at least in terms of carrier phase (if we assume that Alice and Bob have their radio frequency oscillators with perfectly matched frequencies). Note that $\mathbf{x}_A(k)$ is transmitted by Alice starting at a time unknown to Bob. A distributed synchronization is virtually impossible at a precision equal to a small fraction of the period of a radio frequency (MHz or higher).

If there is an embedded pilot in $s(k)$ to help Bob to perform synchronization, then that symbol also allows Eve to estimate her (effective) channel vector $\mathbf{g} = \mathbf{G}\frac{1}{\|\mathbf{h}\|}\mathbf{h}^*$ in her received signal:

$$\mathbf{y}_E(k) = \mathbf{G}\mathbf{x}_A(k) + \mathbf{n}_E(k) = \mathbf{g}s(k) + \mathbf{n}_E(k) \tag{5}$$

where $\mathbf{G}$ is the channel matrix from Alice to Eve. With the knowledge of $\mathbf{g}$, all other symbols in $s(k)$ are virtually exposed especially if Eve has a large number (N_E) of antennas. Here $\mathbf{g}$ has the dimension $N_E \times 1$.

III. ANECE-1: Using Ideal Full-Duplex Radios

We now review the principle of anti-eavesdropping channel estimation (ANECE) as proposed in [1] and further studied in [2] and [3]. For simplicity, we consider the case where Alice and Bob are each a single-antenna full-duplex radio. The objective of ANECE is the same as that of the prior works discussed previously. But an important feature of ANECE is that every session of transmission from each node has a pilot. This ensures that the corresponding receiver is always in synch with the transmitter at the carrier level and hence the standard baseband channel model applies. Note that since Alice and Bob are full-duplex, each of them can serve as a transmitter and a receiver at the same time on the same carrier frequency.

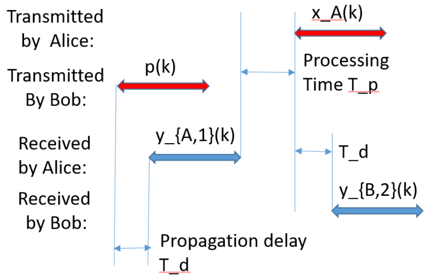

Fig. 1. A key example of prior ideas for discriminative channel estimation using half-duplex radios for (secret) information transmission from Alice to Bob. This idea does not work because the receiver (Bob) cannot perform carrier synchronization with the transmitter (Alice) due to lack of pilot.

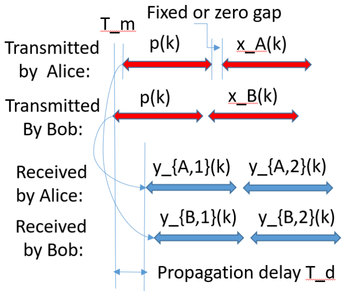

Fig. 2. ANECE-1 [1]: a prior ANECE using a pair of ideal full-duplex radios.

Specifically, as illustrated in Fig. 2, Alice and Bob transmit their packets at about the same time. Each packet has two parts that are in perfect synch with each other. Part 1 of each packet is a pilot sequence $p(k), k = 1, 2, \cdots, K_1$. The same pilot is applied by both Alice and Bob. Part 2 of the packet from Alice is $x_A(k), k = 1, 2, \cdots, K_2$, and part 2 of the packet from Bob is $x_B(k), k = 1, 2, \cdots, K_2$. The best choice of $p(k)$ (for the case of just two users) is a constant sequence, i.e., $p(k)$ is invariant to $k = 1, \cdots, K_1$. The constant pilot makes the concurrent transmissions from Alice and Bob feasible (if not too easy) to implement since the required precision T_m for the concurrence is any small fraction of $K_1 T_s$ with T_s being the symbol interval.

The (baseband) signals received by Alice and Bob, in parts 1 and 2, are respectively: $y_{A,1}(k) = hp(k) + n_{A,1}(k)$, $y_{A,2}(k) = hx_B(k) + n_{A,2}(k)$, $y_{B,1}(k) = hp(k) + n_{B,1}(k)$ and $y_{B,2}(k) = hx_A(k) + n_{B,2}(k)$, where h is the reciprocal channel gain between Alice and Bob. Note that since the pilot $p(k)$ is known to both Alice and Bob and the two parts of each transmission are in perfect synch, the carrier synchronization is not an issue for both Alice and Bob in both parts of each transmission.

Based on $y_{A,1}(k)$, Alice can estimate h. Then based on

$y_{A,2}(k)$, Alice can detect the information in $x_B(k)$. Similarly, Bob can estimate h and then detect the information in $x_A(k)$. If one of the two sequences $x_A(k)$ and $x_B(k)$ is zero, then there is just a one-way information transmission, but the two pilots must be transmitted still as explained below.

1) Effect of ANECE-1 on Eve: The signals received by Eve with N_E antennas, corresponding to the concurrent transmissions from Alice and Bob, are (in baseband):

$$\mathbf{y}_{E,1}(k) = (\mathbf{g}_A + \mathbf{g}_B)p(k) + \mathbf{n}_{E,1}(k) \tag{6}$$

$$\mathbf{y}_{E,2}(k) = \mathbf{g}_A x_A(k) + \mathbf{g}_B x_B(k) + \mathbf{n}_{E,2}(k) \tag{7}$$

where $\mathbf{g}_A$ and $\mathbf{g}_B$ are Eve's receive channel vectors with respect to Alice and Bob respectively. Based on the knowledge of $\{p(k), k = 1, \cdots, K_1\}$, $\{\mathbf{y}_{E,1}(k), k = 1, \cdots, K_1\}$ and $\{\mathbf{y}_{E,2}(k), k = 1, \cdots, K_2\}$, Eve is unable to obtain a consistent estimate of $\mathbf{g}_A$ and $\mathbf{g}_B$, and hence unable to detect all the information in $x_A(k)$ and $x_B(k)$ even if $\mathbf{n}_{E,1}(k) = \mathbf{n}_{E,2}(k) = 0$ and/or $N_E \to \infty$.

Note that if Eve is much closer to Alice than to Bob, then $\mathbf{g}_A + \mathbf{g}_B \approx \mathbf{g}_A$. In this case, Eve may obtain $\mathbf{g}_A$ and hence detect all information in $x_A(k)$. But this Eve is completely blind to $\mathbf{g}_B$ and unable to detect all information in $x_B(k)$.

In many situations, it is possible to keep Eve at comparable distances with respect to both Alice and Bob. This is equivalent to keep the distance between Alice and Bon relatively small compared to other potential receivers in the field.

The above principle of ANECE has been extended to cases where there are more than two legitimate users and each user may have multiple antennas [1]. But our interest in this paper is to re-examine the requirements for ANECE and present a simplified ANECE with lesser requirements.

A. Limitations of Full-Duplex Radios

The key requirement for ANECE is full-duplex radio. Although each antenna (connected to a RF circulator) can be made full-duplex in principle, e.g., see [14] and [15], the performance of such a full-duplex radio is limited. The performance can be measured by the ratio ρ_0 of the residual self-interference (RSI) power over the transmitted power. To understand the role of ρ_0 in ANECE, let us consider the SNR of $y_{A,1}(k)$ where $n_{A,1}(k)$ contains both RSI and the normal channel noise. It follows that

$$SNR_{A,1} = \frac{|h|^2 P_p}{\sigma_n^2 + \rho_0 P_p} \tag{8}$$

where P_p is the power of the pilot $p(k)$, $\rho_0 P_p$ is the residual self-interference power, and σ_n^2 is the normal channel noise variance. We can also write $h = \frac{\tilde{h}}{d^{\alpha/2}}$ where d is the distance between Alice and Bob, $\alpha > 2$ the power exponent of the large scale fading, and $\tilde{h}$ the small-scale fading. It is often to model $\tilde{h}$ as a complex circular Gaussian random variable $\mathcal{CN}(0,1)$ for fading environment or to choose $\tilde{h} = 1$ for non-fading environment. It follows that

$$SNR_{A,1} = \frac{|\tilde{h}|^2 \bar{P}_p}{\sigma_n^2 + \rho \bar{P}_p} \tag{9}$$

with $\bar{P}_p = P_p/d^\alpha$ being the normalized pilot power, and $\rho = d^\alpha \rho_0$ the normalized RSI power gain. We see that ρ can be larger than one although we know $\rho_0 < 1$.

For a near-ideal performance of full-duplex, we need $\rho \bar{P}_p \ll \sigma_n^2$ (see the denominator of (9)) or equivalently

$$d^\alpha \ll \frac{1}{\rho_0 SNR_p} \tag{10}$$

with $SNR_p = \frac{\bar{P}_p}{\sigma_n^2}$. In this case, the variance of the least square estimation of $\tilde{h}$ from $\{y_{A,1}(k), k = 1, \cdots, K_1\}$ can be shown to be $\sigma^2_{\Delta\tilde{h}} = \frac{1}{K_1 SNR_p}$. We see that for a given set of ρ_0, $\sigma^2_{\Delta\tilde{h}}$ and K_1, there is a corresponding upper bound on the distance d in order for Alice and Bob to have a near-ideal performance of full-duplex.

In practice, the value of ρ_0 depends on how the full-duplex radio is designed. The best (smallest) value of ρ_0 is typically achieved by using antenna isolation, e.g., see [10], [11], [12] and [13]. Specifically, if a node has two antennas, we can let one of the two antennas transmit and the other antenna receive. With a proper isolation between the two antennas, the cross-antenna interference can be substantially reduced even before any steps of self-interference cancellation (SIC) take place.

IV. ANECE-2: Using Antenna-Isolation Based Full-Duplex Radios

We now present a modification of ANECE, which uses antenna-isolation based full-duplex radios. We consider a channel between Alice with N_A antennas and Bob with N_B antennas. Let one of the antennas at Alice be A1 and all other antennas at Alice be A2, and one of the antennas at Bob be B1 and all other antennas at Bob be B2. Assume that when A1 transmits, the cross-antenna interference from A1 to A2 (or self-interference at Alice) is minimum due to antenna isolation followed by self-interference cancellation. The same is assumed for B1 and B2. Due to the requirement of antenna isolation, we need $N_A \geq 2$ and $N_B \geq 2$.

Like ANECE-1, ANECE-2 has two steps as illustrated in Fig. 3.

Step 1: Alice and Bob use their A1 and B1 respectively to transmit concurrently (at the symbol precision) the identical pilot sequences $p(k), k = 1, \cdots, K_1$. Consequently, Alice and Bob use their A2 and B2 respectively to receive the following signals:

$$\mathbf{y}_{A2,1}(k) = \mathbf{h}_{A2,B1} p(k) + \mathbf{n}_{A2,1}(k) \tag{11}$$

$$\mathbf{y}_{B2,1}(k) = \mathbf{h}_{B2,A1} p(k) + \mathbf{n}_{B2,1}(k) \tag{12}$$

where $k = 1, \cdots, K_1$. Here $\mathbf{h}_{A2,B1}$ is the channel vector from B1 to A2, which is typically independent from the channel vector $\mathbf{h}_{B2,A1}$ from A1 to B2. With a sufficient energy in the pilot sequence, Alice and Bob can accurately estimate, respectively, $\mathbf{h}_{A2,B1}$ and $\mathbf{h}_{B2,A1}$.

Step 2: After a fixed gap T_0 (at the carrier precision) from its transmitted pilot, Alice uses A2 to transmit $\mathbf{x}_A(k) = \frac{1}{\|\mathbf{h}_{A2,B1}\|}\mathbf{h}^*_{A2,B1} s_A(k)$ for $k = 1, \cdots, K_2$. Similarly, Bob uses B2 to transmit $\mathbf{x}_B(k) = \frac{1}{\|\mathbf{h}_{B2,A1}\|}\mathbf{h}^*_{B2,A1} s_B(k)$ for

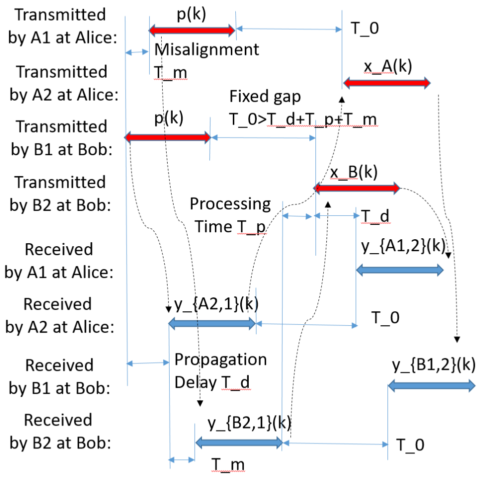

Fig. 3. ANECE-2: A modification of ANECE using antenna-isolation based full-duplex radios. The curved arrows indicate the causality.

$k = 1, \cdots, K_2$. Here, $s_A(k)$ and $s_B(k)$ are two sequences of information symbols, which are independent of each other. Consequently, Alice and Bob use their A1 and B1, respectively, to receive the following signals:

$$\begin{aligned} y_{A1,2}(k) &= \mathbf{h}_{A1,B2}^T \mathbf{x}_B(k) + n_{A1,2}(k) \\ &= \|\mathbf{h}_{B2,A1}\| s_B(k) + n_{A1,2}(k) \end{aligned} \tag{13}$$

$$\begin{aligned} y_{B1,2}(k) &= \mathbf{h}_{B1,A2}^T \mathbf{x}_A(k) + n_{B1,2}(k) \\ &= \|\mathbf{h}_{A2,B1}\| s_A(k) + n_{B1,2}(k) \end{aligned} \tag{14}$$

where $k = 1, \cdots, K_2$. Here we have applied the reciprocal properties $\mathbf{h}_{A1,B2} = \mathbf{h}_{B2,A1}$ and $\mathbf{h}_{B1,A2} = \mathbf{h}_{A2,B1}$.

Even though $\mathbf{h}_{B2,A1}$ is only known to Bob (and Alice does not know $\|\mathbf{h}_{B2,A1}\|$), Alice can detect all information in $s_B(k)$ from $y_{A1,2}$ (assuming PSK symbols and sufficient SNR in $y_{A1,2}$) since the signal component in $y_{A1,2}$ is a positive scale of $s_B(k)$. The same applies to $y_{B1,2}(k)$ from which Bob can detect all information in $s_A(k)$.

It is important to note (see Fig. 3) that T_0 must be larger than the sum of T_d, T_p and T_m, i.e., $T_0 > T_d + T_p + T_m$. Here, T_d is the propagation delay between Alice and Bob, T_p is a processing time needed from the reception of $\mathbf{y}_{A2,1}(k)$ to the construction of $\mathbf{x}_A(k)$, and T_m is a time of misalignment between Alice and Bob. In principle, as long as there are known upper bounds on T_d, T_p and T_m for given applications, T_0 can be predetermined.

Furthermore, T_0 must be precisely controlled so that the receive carrier of each node remains synchronized with the transmit carrier of the other node throughout the two-step process. Specifically, we can think that each node has two virtual carriers: one for transmit and one for receive. For example, Bob uses his transmit carrier when he transmits the pilot $p(k)$ via B1 in step 1, pauses for T_0 microseconds and then transmits the information sequence $\mathbf{x}_B(k)$ via B2 in step 2. Correspondingly, Alice synchronizes her receive carrier with Bob's transmit carrier when she receives the pilot via A2 (from Bob) in step 1 and then applies her receive carrier to receive the information sequence via A1 (from Bob) in step 2. The same applies to the (concurrent) other way around between Alice and Bob.

1) Effect of ANECE-2 on Eve: When Alice and Bob transmit $p(k)$ via A1 and B1 respectively, the eavesdropper (Eve) with N_E antennas receives

$$\mathbf{y}_{E,1}(k) = (\mathbf{g}_{E,A1} + \mathbf{g}_{E,B1}) p(k) + \mathbf{n}_{E,1}(k) \tag{15}$$

where $\mathbf{g}_{E,A1}$ and $\mathbf{g}_{E,B1}$ are the channel vectors from A1 of Alice and B1 of Bob, respectively, to Eve. It is clear that Eve is unable to estimate $\mathbf{g}_{E,A1}$ and $\mathbf{g}_{E,B1}$ consistently from $\mathbf{y}_{E,1}(k)$.

When Alice and Bob transmit $\mathbf{x}_A(k)$ and $\mathbf{x}_B(k)$ via A2 and B2 respectively, Eve receives

$$\begin{aligned} \mathbf{y}_{E,2}(k) &= \mathbf{G}_{E,A2} \mathbf{x}_A(k) + \mathbf{G}_{E,B2} \mathbf{x}_B(k) + \mathbf{n}_{E,2}(k) \\ &= \mathbf{g}_{E,A2} s_A(k) + \mathbf{g}_{E,B2} s_B(k) + \mathbf{n}_{E,2}(k) \end{aligned} \tag{16}$$

with

$$\mathbf{g}_{E,A2} = \mathbf{G}_{E,A2} \frac{1}{\|\mathbf{h}_{A2,B1}\|} \mathbf{h}_{A2,B1}^* \tag{17}$$

$$\mathbf{g}_{E,B2} = \mathbf{G}_{E,B2} \frac{1}{\|\mathbf{h}_{B2,A1}\|} \mathbf{h}_{B2,A1}^* \tag{18}$$

where $\mathbf{G}_{E,A2}$ and $\mathbf{G}_{E,B2}$ are the channel matrices from A2 of Alice and B2 of Bob, respectively, to Eve.

It is important to note that in scattering-rich environment, $\mathbf{h}_{A2,B1}$, $\mathbf{h}_{B2,A1}$, $\mathbf{g}_{E,A1}$, $\mathbf{g}_{E,B1}$, $\mathbf{G}_{E,A2}$ and $\mathbf{G}_{E,B2}$ are all independent of each other. This means that even if Eve could find the exact $\mathbf{g}_{E,A1}$ and $\mathbf{g}_{E,B1}$, this would be useless for Eve to detect the information in $s_A(k)$ and $s_B(k)$ from $\mathbf{y}_{E,2}(k)$ (which is independent of $\mathbf{g}_{E,A1}$ and $\mathbf{g}_{E,B1}$).

The above observation means that a good alignment between the two pilots from Alice and Bob are not needed at all. Indeed, the two pilots could be significantly misaligned to even allow Eve to have a good estimate of both $\mathbf{g}_{E,A1}$ and $\mathbf{g}_{E,B1}$.

2) One-Way Information Transmission: If only one-way information transmission is conducted, one of the information sequences $s_A(k)$ and $s_B(k)$ (or equivalently $\mathbf{x}_A(k)$ and $\mathbf{x}_B(k)$) can be simply dropped (i.e., set to zero). In this case, can we also simply drop one of the two pilots? The answer is no. Both pilots are needed for the receive carrier of each node to be synchronized with the transmit carrier of the other node.

If only Alice needs to send secret information to Bob, the scheme shown in Fig. 3 reduces to Fig. 4. Here we see that there is no more constraint on the fixed gap T_0. To minimize the negative effect of drifting of carrier frequency and/or phase, we should minimize T_0, which leads to a surprising result shown in the next section.

V. ANECE-3: Using Multi-Antenna Half-Duplex Radios

Inspired by the analysis of ANECE-2 shown previously, we can increase T_m to avoid the need of full-duplex radios, and also reduce T_0 to zero to optimize carrier synchronization.

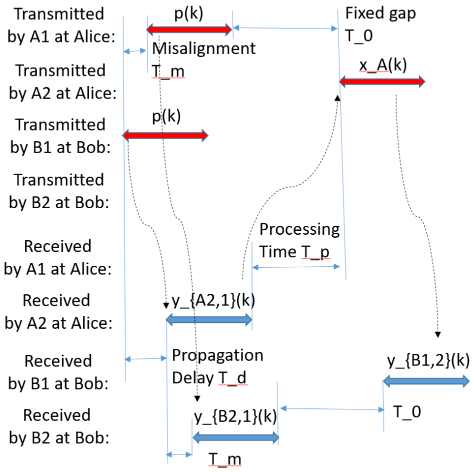

Fig. 4. This figure results from Fig. 3 if only Alice transmits info to Bob. Here T_0 and T_m are no longer constrained by each other.

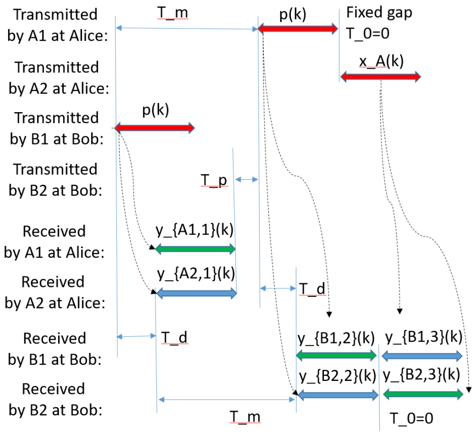

Fig. 5. ANECE-3: A 3-phase ANECE using half-duplex radios for information transmission from Alice to Bob. Here $\mathbf{y}_{B2,2}(k)$ and $y_{B1,3}(k)$ correspond to $\mathbf{y}_{B2,1}(k)$ and $y_{B1,2}(k)$ in ANECE-2.

As illustrated in Fig. 5, the new scheme of ANECE for information transmission from Alice to Bob has three (orthogonal) phases of transmissions as discussed below.

In phase 1, Bob transmits a pilot $p(k)$ via B1, and Alice receives the signal $\mathbf{y}_{A2,1}(k) = \mathbf{h}_{A2,B1}p(k)+\mathbf{n}_{A2,1}(k)$ via A2. Alice then estimates $\mathbf{h}_{A2,B1}$ from $\mathbf{y}_{A2,1}(k)$ and prepares the construction of $\mathbf{x}_A(k) = \frac{1}{\|\mathbf{h}_{A2,B1}\|}\mathbf{h}^*_{A2,B1}s_A(k)$ with $s_A(k)$ being the sequence of information symbols. Unlike ANECE-2, Alice also receives $y_{A1,1}(k) = h_{A1,B1}p(k) + n_{A1,1}(k)$ via A1 from which $h_{A1,B1}$ could be estimated. But Alice does not need the knowledge of $h_{A1,B1}$ in this scheme.

Both phases 2 and 3 are for transmissions from Alice, which however must be perfectly in synch using the same transmit carrier at Alice. Also, in phase 2, Alice transmits a pilot $p(k)$ with $k = 1, \cdots, K_2$ via A1, and in phase 3, Alice transmits $\mathbf{x}_A(k)$ with $k = 1, \cdots, K_3$ via A2. The transmission in phase 2 allows Bob to synchronize his receive carrier based on $y_{B1,2}(k)$ and $\mathbf{y}_{B2,2}(k)$ received via B1 and B2. This in turn allows Bob to reliably receive $y_{B1,3}(k)$ and $\mathbf{y}_{B2,3}(k)$ via B1 and B2 in phase 3. Since $y_{B1,3}(k)$ is equivalent to $y_{B1,2}(k)$ in (14), Bob is able to detect the information in $s_A(k)$ (assuming PSK).

1) Effect of ANECE-3 on Eve: The signals received by Eve in phases 2 and 3 from Alice are

$$\mathbf{y}_{E,2}(k) = \mathbf{g}_{E,A1}p(k) + \mathbf{n}_{E,2}(k), \tag{19}$$

$$\mathbf{y}_{E,3}(k) = \mathbf{G}_{E,A2}\mathbf{x}_A(k) + \mathbf{n}_{E,3}(k). \tag{20}$$

Since $\mathbf{g}_{E,A1}$ is independent of $\mathbf{G}_{E,A2}$, Eve is completely blind to $\mathbf{G}_{E,A2}$ in $\mathbf{y}_{E,3}(k)$. Equivalently, Eve is completely blind to $\mathbf{g}_{E,A2}$ in the following:

$$\mathbf{y}_{E,3}(k) = \mathbf{g}_{E,A2}s_A(k) + \mathbf{n}_{E,3}(k) \tag{21}$$

where $\mathbf{g}_{E,A2} = \mathbf{G}_{E,A2}\frac{1}{\|\mathbf{h}_{A2,B1}\|}\mathbf{h}^*_{A2,B1}$.

2) Remarks: We see that in ANECE-3 (for information transmission from Alice to Bob), Alice does not need to receive any signal via A1, i.e., A1 only serves as a transmit antenna to help Bob to perform carrier synchronization. Also the two pilots from Alice and Bob can be totally different from each other.

Compared to the (infeasible) scheme in Fig. 1, the critical difference here is the transmission of a pilot from Alice via A1 (one of her antennas) which is immediately followed by transmission of beamformed information via A2 (her other antennas). This design change seems small but is also significant. (In theory, A1 could be more than one antennas as well.)

A. Further Analysis

Unlike ANECE-2, ANECE-3 allows Bob to receive signals via both B1 and B2 in each of phases 2 and 3. We will discuss next the roles of the additional received signals (shown in green color in Fig. 5). Define

$$\mathbf{X}_A = \left[\begin{array}{c|c} p(1), \cdots, p(K_2) & 0 \\ \hline 0 & \mathbf{x}_A(1), \cdots, \mathbf{x}_A(K_3) \end{array}\right] = \begin{bmatrix} \mathbf{p}^T & 0 \\ 0 & \mathbf{X} \end{bmatrix}, \tag{22}$$

$$\mathbf{H}_{B,A} = \begin{bmatrix} h_{B1,A1} & \mathbf{h}^T_{B1,A2} \\ \mathbf{h}_{B2,A1} & \mathbf{H}_{B2,A2} \end{bmatrix}, \tag{23}$$

and

$$\mathbf{Y}_B = [\mathbf{Y}_{B,2}, \mathbf{Y}_{B,3}] = \begin{bmatrix} y_{B1}(1), \cdots, y_{B1}(K_2+K_3) \\ \mathbf{y}_{B2}(1), \cdots, \mathbf{y}_{B2}(K_2+K_3) \end{bmatrix} \tag{24}$$

where $\mathbf{X}_A$ is the $N_A \times (K_2 + K_3)$ matrix of the signals transmitted by Alice in phases 2 and 3, $\mathbf{H}_{B,A}$ is the $N_B \times N_A$ channel matrix from Alice to Bob, and $\mathbf{Y}_B$ is the $N_B \times (K_2 + K_3)$ matrix of the signals received by Bob in phases 2 and 3. Also $\mathbf{Y}_{B,2}$ is the block of the first K_2 columns of $\mathbf{Y}_B$, and $\mathbf{Y}_{B,3}$ the block of the last K_3 columns of $\mathbf{Y}_B$. It follows from $\mathbf{Y}_B = \mathbf{H}_{B,A}\mathbf{X}_A + \mathbf{N}_B$ that

$$\mathbf{Y}_{B,2} = \begin{bmatrix} h_{B1,A1}\mathbf{p}^T \\ \mathbf{h}_{B2,A1}\mathbf{p}^T \end{bmatrix} + \mathbf{N}_{B,2}, \tag{25}$$

and

$$\mathbf{Y}_{B,3} = \left[\begin{array}{c} \mathbf{h}_{B1,A2}^T \mathbf{X} \\ \mathbf{H}_{B2,A2} \mathbf{X} \end{array} \right] + \mathbf{N}_{B,3}. \tag{26}$$

It is clear that Bob can use all the RF waveforms associated with $\mathbf{Y}_{B,2}$ (not just the signal $\mathbf{y}_{B2,1}(k)$ shown in Fig. 4) for carrier synchronization. Bob can also estimate $h_{B1,A1}$ and $\mathbf{h}_{B2,A1}$ from $\mathbf{Y}_{B,2}$. However, the channel from Alice via A1 is not secure since Eve can also estimate her channel vector with respect to A1 of Alice. In ANECE-3, Alice sends no information via A1.

In $\mathbf{Y}_{B,3}$ shown in (26), both $\mathbf{h}_{B1,A2}^T$ and $\mathbf{H}_{B2,A2}$ are unknown to Bob. But one can write that

$$\mathbf{h}_{B1,A2}^T \mathbf{X} = \gamma \mathbf{s}_A^T \tag{27}$$

with $\gamma = \|\mathbf{h}_{B1,A2}\| = \|\mathbf{h}_{A2,B1}\| > 0$ and $\mathbf{s}_A^T = [s_A(1), \cdots, s_A(K_3)]$. And also

$$\mathbf{H}_{B2,A2} \mathbf{X} = \mathbf{v} \mathbf{s}_A^T \tag{28}$$

with $\mathbf{v} = \mathbf{H}_{B2,A2} \frac{1}{\|\mathbf{h}_{A2,B1}\|} \mathbf{h}_{A2,B1}^*$ being a complex vector unknown to Bob. Equivalently, one can write

$$\mathbf{Y}_{B,3} = \left[\begin{array}{c} \gamma \\ \mathbf{v} \end{array} \right] \mathbf{s}_A^T + \mathbf{N}_{B,3} \tag{29}$$

We can show that if $K_3 \geq 2$ and $\mathbf{s}_A^T \doteq [s_A(1), \cdots, s_A(K_3)]$ consists of PSK symbols, then all $s_A(k)$, γ and $\mathbf{v}$ are uniquely identifiable from $\mathbf{Y}_{B,3}$ asymptotically. Specifically, in the absence of noise and up to a positive scaling, $[\gamma, \mathbf{v}^T]^T$ is the left principal singular vector of $\mathbf{Y}_{B,3}$, and $\mathbf{s}_A$ is the corresponding right singular vector of $\mathbf{Y}_{B,3}$. Clearly, the optimal detection of $\mathbf{s}_A$ should be based on all signals received by Bob. If the noise is white Gaussian, the optimal detection is the minimum distance detector, i.e.,

$$\min_{\gamma > 0, \mathbf{v}, \|\mathbf{s}_A\|^2 = K_3} \left\| \mathbf{Y}_{B,3} - \left[\begin{array}{c} \gamma \\ \mathbf{v} \end{array} \right] \mathbf{s}_A^T \right\|^2 . \tag{30}$$

The principal singular vectors of $\mathbf{Y}_{B,3}$ mentioned earlier can be used as the initial joint estimation of γ, $\mathbf{v}$ and $\mathbf{s}_A$. For optimal performance, an iterative search of the above optimization problem can be conducted where $s_A(k) \forall k$ are subject to PSK (or any QAM if γ is known).

If SNR of the signal (i.e., $y_{B1,3}(k) = \gamma s_A(k) + n_{B1,3}(k)$) received by Bob via B1 in phase 3, is sufficiently high, then Bob can reliably detect all information in $s_A(k)$ by using $y_{B1,3}(k)$ alone. However, using multiple antennas, Bob could perform blind beamforming on $\mathbf{Y}_{B,3}$ to detect all information from Alice. In other words, ANECE-3 can yield a positive secrecy using just half-duplex radios against full-duplex adversaries who, with any number of antennas located virtually anywhere, perform both jamming and eavesdropping.

VI. Conclusion

This paper reviewed the key principles of many prior methods for the purpose of ANECE and highlighted their shortcomings and limitations. It also proposed and analyzed a new scheme of ANECE using multi-antenna half-duplex radios. To the author's knowledge, if only half-duplex radios are available, this new scheme could be the first feasible scheme that allows the legitimate users to conduct RF carrier synchronization, necessary channel estimation and detection of transmitted information, and at the same time completely prevents any eavesdropper at virtually any location from finding its channel state information relative to any transmit antenna where secret information is transmitted. This new scheme also appears easy to implement since there is no strict requirement of synchronization between two distributed radios. In application, all public information in a packet should be "lumped" with its pilot.

Acknowledgement

This work was supported in part by ARO under Grant Number W911NF-17-1-0581 and DoD under W911NF2020267.

References

[1] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," IEEE Transactions on Signal Processing, vol. 67, no. 1, pp. 120-135, 2019.

[2] R. Sohrabi, Q. Zhu, and Y. Hua, "Secrecy analyses of a full-duplex MIMOME network," IEEE Transactions on Signal Processing, vol. 67, no. 23, pp. 5968-5982, 2019.

[3] Q. Zhu, S. Wu, and Y. Hua, "Optimal pilots for anti-eavesdropping channel estimation IEEE Transactions on Signal Processing, vol. 68, pp. 2629-2644, 2020.

[4] T.-H. Chang, W.-C. Chiang, Y.-W. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," IEEE Trans. Signal Processing, Vol. 58, No. 12, pp. 6223-6237, Dec. 2010.

[5] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," IEEE Trans. Signal Process., vol. 61, no. 10, pp. 27242738, may 2013.

[6] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang, "A semiblind two-way training method for discriminatory channel estimation in MIMO systems," IEEE Trans. Commun., vol. 62, no. 7, pp. 2400-2410, 2014.

[7] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading," IEEE Trans. Wireless Communications, Vol. 14, No. 1, pp. 94-106, Jan. 2015.

[8] D. E. Simmons, N. Bhargav, J. P. Coon, S. L. Cotton, "Physical layer security over OFDM-based links: conjugate-and-return," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 10.1109/VTCSpring.2015.7146015.

[9] T. Y. Liu, S. C. Lin, and Y. W. Hong, "On the role of artificial noise in training and data transmission for secret communications," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 3, pp. 516-531, 2017.

[10] J. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in Proc of MobiCom2010, New York, Sep. 2010.

[11] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in Proc. Asilomar 2010.

[12] Y. Hua, Y. Ma, A. Gholian, Y. Li, A. C. Cirik, and P. Liang, "Radio self-interference cancellation by transmit beamforming, all-analog cancellation and blind digital tuning," Signal Process., vol. 108, pp. 322-340, 2015.

[13] E. Ahmed, A. M. Eltawil, Z. Li, and B. A. Cetiner, "Full-duplex systems using multi-reconfigurable antennas," IEEE Trans. Wireless Commun., vol. 14, no. 11, pp. 5971-5983, Nov. 2015.

[14] Y. Hua, P. Liang, Y. Ma, A. Cirik and Q. Gao, "A method for broadband full-duplex MIMO radio," IEEE Signal Processing Letters, Vol. 19, No. 12, pp. 793-796, Dec 2012.

[15] S. Khaledian, F. Farzami, B. Smida and D. Erricolo, "Inherent self-interference cancellation for in-band full-duplex single-antenna systems," in IEEE Transactions on Microwave Theory and Techniques, vol. 66, no. 6, pp. 2842-2850, June 2018, doi: 10.1109/TMTT.2018.2818124.