IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 6, 2018, accepted December 30, 2018, date of publication January 17, 2019, date of current version February 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893801

Security-Enhanced SC-FDMA Transmissions Using Temporal Artificial-Noise and Secret Key Aided Schemes

MOHAMED F. MARZBAN[1], (Student Member, IEEE),
AHMED EL SHAFIE[1], (Senior Member, IEEE), NAOFAL AL-DHAHIR[1], (Fellow, IEEE),
AND RIDHA HAMILA[2], (Senior Member, IEEE)
[1]Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080, USA
[2]Department of Electrical Engineering, Qatar University, Qatar

Corresponding author: Mohamed F. Marzban (mohamed.marzban@utdallas.edu)

This work was supported by the Qatar National Research Fund (a member of the Qatar Foundation) through NPRP under Grant 8-627-2-260. The statements made herein are solely the responsibility of the authors.

ABSTRACT We investigate the physical-layer security of uplink single-carrier frequency-division multiple-access (SC-FDMA) systems. Multiple users, Alices, send confidential messages to a common legitimate base-station, Bob, in the presence of an eavesdropper, Eve. To secure the legitimate transmissions, each user superimposes an artificial noise (AN) signal on the time-domain SC-FDMA data symbol. We reduce the computational and storage requirements at Bob's receiver by assuming simple per-sub-channel detectors. We assume that Eve has global channel knowledge of all links in addition to high computational capabilities, where she adopts high-complexity detectors such as single-user maximum likelihood (ML), multi-user minimum-mean-square-error, and multi-user ML. We analyze the correlation properties of the time-domain AN signal and illustrate how Eve can exploit them to reduce the AN effects. We prove that the number of useful AN streams that can degrade Eve's signal-to-noise ratio is dependent on the channel memories of Alices–Bob and Alices–Eve links. Furthermore, we enhance the system security for the case of partial Alices–Bob channel knowledge at Eve, where Eve only knows the precoding matrices of the data and AN signals instead of knowing the entire Alices–Bob channel matrices, and propose a hybrid security scheme that integrates temporal AN with channel-based secret key extraction.

INDEX TERMS Multi-user SC-FDMA, physical-layer (PHY) security, eavesdropping.

I. INTRODUCTION

Wireless channels are vulnerable to eavesdropping security attacks due to their broadcast nature where an illegitimate node can overhear confidential information about the communicating legitimate nodes. Information security is conventionally preserved using encryption schemes implemented at the upper layers of the protocol stack. However, such schemes require high storage and computational capabilities. In addition, they preserve security under the assumption of limited computation capabilities and limited network parameters knowledge at the eavesdroppers. To enhance and complement the upper-layers security approaches, physical-layer (PHY) security was introduced to provide security at the waveform level by exploiting the time-varying random nature of the wireless channel.

In his seminal work on secure communications, Wyner [2] showed that secure transmissions are feasible as long as the wiretap channel, i.e., the transmitter-eavesdropper channel, is more degraded than the legitimate channel, i.e., the transmitter-legitimate receiver channel. PHY security is quantified in terms of the secrecy capacity which is the maximum data rate with zero information leakage to the eavesdropper(s). Many research works investigated the impact of multiple transmit antennas at various nodes on the achievable secrecy rates by using data and artificial noise (AN) precoding schemes [3] where the transmissions are designed carefully to transmit the data signals in the direction of the legitimate channel vectors while the AN signals are transmitted along the directions orthogonal to the data vectors. The key idea of transmitting AN signals is to confuse the eavesdroppers and degrade their signal-plus-interference-to-noise ratios (SINRs) [3]–[5].

However, in Internet of Things (IoT) applications, where the communicating devices are equipped with limited processing and transmit power resources, only a single antenna is typically available at the wireless nodes. In addition, in uplink wireless transmissions, the limited transmit power and form factor constraints at portable devices typically prohibit equipping them with multiple transmit antennas/radio-frequency (RF) chains. In such practical scenarios, beamforming and spatial AN techniques cannot be implemented by the uplink transmitting nodes [3]–[5] which presents a major research challenge.

Another approach for PHY security is based on exploiting the randomness of the wireless channel for extracting identical secret keys at the legitimate communicating nodes. Wireless channels are characterized by a reciprocity property at a given time/frequency/space resource. That is, two communicating nodes observe identical (or at least highly correlated) multi-path characteristics at both ends of a wireless link at any instant of time. In a rich fading environment, channel variations over time maintain a source of randomness that can be exploited by the transmitter and the legitimate receiver to extract two identical sets of secret key samples. Secret key extraction and generation from wireless channel measurements have been realized using different properties of the received signal, e.g., received signal strength (RSS) [6], phase differences [7], time delay (in wideband transmission) [8], [9], and channel state information (CSI) [10]. Since RSS is easy to measure in practice, it is often used in many scenarios (see, e.g., [6]). Upon agreeing on secret key samples between the legitimate transmit-receiver pair, they can be used as one-time pad (OTP) cipher to encrypt several data samples. OTP encryption is perfectly secure and provably unbreakable as long as the number of secured data samples is equal to the number of secret key samples [11]. Unfortunately, the main restriction of OTP encryption is that the number of extracted secret key samples from a random source (i.e., channel) is too low to encrypt all the transmitted data samples [10], [12]–[14]. This is due to the fact that the channel reciprocity property can not be guaranteed unless the legitimate parties measure the channel simultaneously. Moreover, perfect independence between legitimate and eavesdropping links is not possible in some scenarios. Increasing the number of secret key samples has been investigated in many works, e.g., [10], [12]–[14], and the references therein.

PHY security has been recently investigated for many transmission scenarios including those based on the orthogonal-frequency division multiplexing (OFDM) modulation scheme and its multiple-access variant, namely, orthogonal-frequency division-multiple access (OFDMA), see e.g. [15]–[21]. The key advantage of OFDM is its ability to convert a frequency-selective channel into a group of orthogonal flat-fading frequency sub-channels. Zhang and Liu [15] constrained their problem formulation to meet the secrecy rate requirements of all users in an OFDMA network while optimizing the energy harvested by all users. In [16], a secret key generation scheme based on the precoding matrix indices was proposed for securing multiple-input multiple-output (MIMO)-OFDM systems. Qin *et al.* [18] investigated the PHY security of a single-input single-output single-antenna eavesdropper (SISOSE) OFDM system and proposed a temporal-AN injection scheme to increase the instantaneous secrecy rate (ISR). The problem formulation was then extended in [19] to investigate the PHY security of MIMOME-OFDM systems using a new hybrid spatial-temporal AN scheme. In [20] and [21], different AN precoding designs and power allocation schemes were investigated to enhance the ISR in OFDM systems.

Single-carrier frequency-division multiple access (SC-FDMA) has been adopted in the uplink of wireless cellular standards such as fourth generation long term evolution (LTE) [22] as well as the forthcoming fifth generation new radio (NR). In addition, it has been recently standardized as the multiple-access scheme for cellular-vehicle-to-everything (C-V2X) communication in LTE and NR side-links [23]. This paves the way for a wide range of IoT applications to use SC-FDMA. Furthermore, narrowband IoT (NB-IoT) was first introduced in 3GPP Release 13, and SC-FDMA technology is adopted for its uplink transmissions [24]. That is why many recent research studies investigated SC-FDMA for IoT [25]–[28]. SC-FDMA is based on single-carrier frequency-division equalization (SC-FDE) which evolved to realize the benefits of OFDM and single-carrier systems as discussed in, e.g., [29] and references therein. Unlike OFDMA systems, SC-FDMA has a relatively low peak-to-average power ratio (PAPR) which makes it suitable for low-power devices. Although securing uplink SC-FDMA transmissions is very critical, to the best of our knowledge, none of the previous research work has considered SC-FDMA PHY security (i.e., information-theoretic security).

Our main contributions in this paper are summarized as follows

- We design a security scheme for SC-FDMA systems by adding a temporal (time-domain) AN signal to the SC-FDMA symbol. The key idea is to exploit the available temporal degrees of freedom due to the insertion of a cyclic prefix (CP) sequence into each SC-FDMA data symbol. The AN precoding matrix is designed carefully to degrade the eavesdropper(s) channels only and to be canceled at the legitimate receiver.
- We allocate different power levels to the data and AN signals. To generalize the optimization setting, we assume a power fraction that determines the amount of power assigned to data signals relative to AN signals. Our AN design does not require the instantaneous channel state information (CSI) of Eve's link which makes our proposed scheme robust in mitigating eavesdropping attacks even when the eavesdroppers remain passive to conceal their presence.
- We investigate the average secrecy rate performance when Bob adopts the conventional linear block ZF and

MMSE detection strategies. We show that these detection strategies reduce to simple per-sub-channel filtering. That is, the detector design has low complexity at the legitimate receiver, which is a practical scenario for IoT devices.

- We consider the worst-case eavesdropping scenario where Eve is assumed to have very high computational capabilities and investigate three high-complexity detectors at Eve's receiver; namely, single-user ML, multi-user MMSE, and multi-user ML. We analyze the design complexity and the achieved data rate in each scenario. In addition, we consider the worst-case eavesdropping scenario where Eve has knowledge of the CSI of the Alices-Bob links and accounts for AN correlation in her detectors' designs. We compare the average secrecy rates under these detection strategies for different system design parameters.
- We show that the number of AN streams that Alice can inject without harming Bob is equal to the number of CP samples. We prove that, out of those streams, the number of useful AN streams that can actually degrade Eve's SINR is the maximum of the Alice-Bob's and Alice-Eve's channel memories. The remaining AN streams lie in the null space of the Alice-Eve's channel matrix. This prevents Alice from wasting her power on useless AN streams.
- We derive a new closed-form expression for the average secrecy rate and show that, at high input SNR, the average secrecy rate is a linear function of Alice's transmit power level (in dB scale). Hence, unlike the case of no AN injection where the ISR becomes independent of Alice's transmit power level and saturates with it, in our investigated AN-aided scheme, the transmit power can still increase the ISR. Moreover, for a large number of data samples per SC-FDMA symbol, the achievable average secrecy rate is a linear function of the number of useful AN streams.
- To enhance the system security for the case of partial Alices-Bob channel knowledge at Eve, we propose a hybrid scheme that integrates temporal AN with channel-based secret key extraction. In our proposed scheme, we exploit the channel variations to extract secret key samples which are used by the Alices to encrypt an equivalent number of data samples using an OTP. The encrypted data samples are then multiplexed with the remaining unencrypted data samples in the time domain. Finally, temporal-AN signals are added to the entire SC-FDMA symbol to secure the unencrypted data samples. The encrypted data samples are information-theoretically secured and their generation guarantees a positive total ISR. In addition, they provide an additional source of interference (in addition to temporal-AN samples) that degrades Eve's reception of the unencrypted data samples.

Notation: Lower- and upper-case bold letters denote vectors and matrices, respectively, while the subscripts, $(\cdot)_{\mathrm{f}}$ and $(\cdot)_{\mathrm{t}}$, refer to frequency-domain and time-domain quantities, respectively. $\mathbf{I}_N$ and $\mathbf{F}_N$ denote, respectively, the $N \times N$ identity matrix and the fast Fourier transform (FFT) matrix. $\mathbb{C}^{M\times N}$ and $\mathbb{R}^{M\times N}$ denote the set of all $M \times N$ complex and real matrices, respectively. $(\cdot)^{\top}$ and $(\cdot)^{*}$ denote the transpose and Hermitian (i.e., complex-conjugate transpose) operations, respectively, and $\mathbb{E}\{\cdot\}$, denotes statistical expectation. $\mathbf{A}^{(k)}$ denotes the matrix $\mathbf{A}$ associated with user k and $[\mathbf{A}]_{i,1:N}$ is the i-th row of the matrix $\mathbf{A} \in \mathbb{C}^{M\times N}$. $\mathbf{0}_{M\times N}$ denotes the all-zero matrix with size $M \times N$, and $|\cdot|$ denotes the absolute value. $\mathrm{diag}\{\cdot\}$ denotes a diagonal matrix whose diagonal elements are the enclosed entries, while $\mathrm{diag}\{\cdot\}_{i,i}$ represents the i-th diagonal element of the enclosed matrix. $[\cdot]^{+} = \max\{0, \cdot\}$ returns the maximum between the argument and zero, and $[\mathbf{A} \;\; \mathbf{B}]$ represents the horizontal concatenation of matrices $\mathbf{A}$ and $\mathbf{B}$. $\mathcal{CN}(0, \Sigma)$ denotes the complex Gaussian distribution with zero mean and covariance matrix denoted by Σ. Throughout this paper, the term, *sample*, is used to denote a single quadrature amplitude modulation (QAM) constellation symbol while the entire SC-FDMA symbol is denoted as, *symbol*. A list of the key variables used throughout the paper are summarized in Table 1.

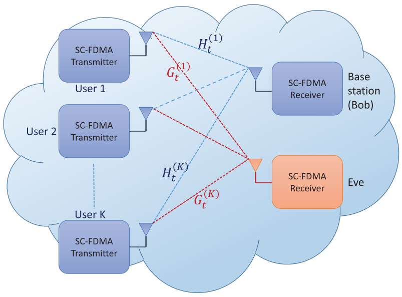

FIGURE 1. Eavesdropping multiple-access uplink system model.

II. SYSTEM MODEL

Consider an SC-FDMA uplink communication system consisting of K legitimate users, called Alices, and a single common base-station, called Bob. Each user sends confidential information messages to Bob in the presence of a passive eavesdropper, called Eve, who overhears the ongoing communications as depicted in Fig. 1. Let M denote the total number of sub-channels of the SC-FDMA symbol and $N \leq M$ is the number of sub-channels allocated to each user. We assume an equal sub-channel allocation to all users, i.e., $N = M/K$. All nodes are assumed to be equipped with a single antenna.[1] SC-FDMA transmissions can be considered as FFT-precoded OFDMA transmissions

[1] We consider a single antenna to meet the IoT application requirements where devices have limited processing capabilities. The single antenna assumption is considered not only at the eavesdropper, but at the intended receiver as well to guarantee fairness between both receivers. We add a further constraint to the legitimate system by assuming a single antenna at the transmitter to meet the limited processing requirements of the IoT applications. Most of the current PHY security schemes fail in this scenario. This is the main challenge that we address in this paper.

TABLE 1. List of key variables.

Symbol	Description	Symbol	Description
M	Total number of sub-channels in the SC-FDMA symbol	N	Number of sub-channels allocated to each user ($N \leq M$)
K	Number of legitimate users	M_{cp}	CP length
$\mathbf{x}_{\mathrm{t}}^{(k)} \in \mathbb{C}^{N\times 1}$	Time-domain data samples vector transmitted by k-th Alice	$\mathbf{x}_{\mathrm{f}}^{(k)} \in \mathbb{C}^{N\times 1}$	Frequency-domain data samples vector $\left(\mathbf{x}_{\mathrm{f}}^{(k)} = \mathbf{F}_N \mathbf{x}_{\mathrm{t}}^{(k)}\right)$
$\mathbf{F}_N \in \mathbb{C}^{N\times N}$	N-point FFT matrix	$\mathbf{S}^{(k)} \in \mathbb{R}^{M\times N}$	The k-th Alice binary sub-channel mapping matrix
$\mathbf{T}^{\mathrm{cp}} \in \mathbb{R}^{(M+M_{\mathrm{cp}})\times M}$	CP insertion matrix	$\mathbf{R}^{\mathrm{cp}} \in \mathbb{R}^{M\times(M+M_{\mathrm{cp}})}$	CP removal matrix
$L_{\mathrm{B}}^{(k)}$	Channel memory of the $\mathrm{A}_k - \mathrm{B}$ link	$L_{\mathrm{E}}^{(k)}$	Channel memory of the $\mathrm{A}_k - \mathrm{E}$ link
$\mathbf{n}_{\mathrm{B}}^{(k)} \in \mathbb{C}^{N\times 1}$	The zero-mean circularly-symmetric AWGN vector at Bob	$\mathbf{n}_{\mathrm{E}}^{(k)} \in \mathbb{C}^{N\times 1}$	The zero-mean circularly-symmetric AWGN vector at Eve
${\mathbf{y}_{\mathrm{B}}}_{\mathrm{f}}^{(k)} \in \mathbb{C}^{N\times 1}$	The k-th Alice frequency-domain received signal at Bob	${\mathbf{y}_{\mathrm{E}}}_{\mathrm{f}}^{(k)} \in \mathbb{C}^{N\times 1}$	The k-th Alice frequency-domain received signal at Eve
${\mathbf{H}_{\mathrm{t}}}^{(k)} \in \mathbb{C}^{(M+M_{cp})\times(M+M_{cp})}$	Toeplitz time-domain channel matrix of the of the $\mathrm{A}_k - \mathrm{B}$ link	${\mathbf{G}_{\mathrm{t}}}^{(k)} \in \mathbb{C}^{(M+M_{cp})\times(M+M_{cp})}$	Toeplitz time-domain channel matrix of the of the $\mathrm{A}_k - \mathrm{E}$ link
$\mathbf{H}_{\mathrm{f}}^{(k)} \in \mathbb{C}^{N\times N}$	Diagonal frequency-domain channel matrix of the $\mathrm{A}_k - \mathrm{B}$ link ($\mathbf{H}_{\mathrm{f}}^{(k)} = \mathbf{S}^{(k)^{\top}}\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{H}_{\mathrm{t}}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^{*}\mathbf{S}^{(k)}$)	$\mathbf{G}_{\mathrm{f}}^{(k)} \in \mathbb{C}^{N\times N}$	Diagonal frequency-domain channel matrix of the $\mathrm{A}_k - \mathrm{E}$ link ($\mathbf{G}_{\mathrm{f}}^{(k)} = \mathbf{S}^{(k)^{\top}}\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G}_{\mathrm{t}}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^{*}\mathbf{S}^{(k)}$)
$\mathbf{W}_{\mathrm{B}}^{(k)} \in \mathbb{C}^{N\times N}$	Linear equalization matrix filter for the k-th Alice data at Bob	$\mathbf{W}_{\mathrm{E}}^{(k)} \in \mathbb{C}^{N\times N}$	Linear equalization matrix filter for the k-th Alice data at Eve
$\mathbf{z}_{\mathrm{t}}^{(k)} \in \mathbb{C}^{M_{\mathrm{cp}}\times 1}$	Temporal AN vector transmitted by the k-th Alice to confuse Eve	$\alpha^{(k)}$	Data power fraction at k-th Alice
$\mathbf{Q}^{(k)} \in \mathbb{C}^{(M+M_{\mathrm{cp}})\times M_{\mathrm{cp}}}$	Temporal AN null space precoder at k-th Alice	p_{t}	Total transmit power at each user

where the samples are precoded using an N-point FFT before applying an OFDMA modulator at the transmitter side. Let $\mathbf{x}_{\mathrm{t}}^{(k)}$ denote the $N \times 1$ zero-mean unit-variance data samples vector transmitted by user $k \in \{1, 2, \ldots, K\}$. Following the 3GPP-LTE standard, we assume that each Alice allocates her transmission power equally across her data samples to maintain the low PAPR advantage of the SC-FDMA system. Let $p_{\mathrm{x}}^{(k)}$ denote the transmission power of the k-th user's samples. The data samples vector is first transformed into a frequency-domain samples vector, denoted by $\mathbf{x}_{\mathrm{f}}^{(k)}$, using an N-point FFT as $\mathbf{x}_{\mathrm{f}}^{(k)} = \mathbf{F}_N\mathbf{x}_{\mathrm{t}}^{(k)}$.

We follow the LTE uplink localized FDMA sub-channel mapping strategy [23] where each user is assigned an adjacent set of sub-channels. Let $\mathbf{S}^{(k)}$ denote the $M \times N$ binary sub-channel mapping matrix which assigns N out of the total M sub-channels to user k and is given by

$$\left[\mathbf{S}^{(k)}\right]_{i,j} = \begin{cases} 1, & \text{sub-channel } i \text{ is assigned to user } k \\ & \text{and mapped to element } j \\ 0, & \text{Otherwise} \end{cases} \tag{1}$$

Next, an M-point IFFT is used to transform the signal back to the time domain. Prior to transmission, a CP sequence of size M_{cp} is inserted at the beginning of each SC-FDMA data symbol using a CP insertion matrix, denoted by $\mathbf{T}^{\mathrm{cp}} = \left[\mathbf{E}_{M_{\mathrm{cp}}\times M}^{\top}\ \mathbf{I}_M\right]^{\top} \in \mathbb{R}^{(M+M_{\mathrm{cp}})\times M}$ with $\mathbf{E} = \left[\mathbf{0}_{M_{\mathrm{cp}}\times(M-M_{\mathrm{cp}})}\ \mathbf{I}_{M_{\mathrm{cp}}}\right]$.

Let A_k, B, and E, denote the k-th Alice, Bob, and Eve, respectively. Let $L_{\mathrm{B}}^{(k)}$ and $L_{\mathrm{E}}^{(k)}$ denote the channel memories (i.e. channel impulse response duration in samples) of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links, respectively. The CP is designed to be longer than the channel memories of all links to eliminate the inter-symbol interference. We assume a block-fading channel model where a codeword experiences many fading realizations and the coherence time of a single fading realization is sufficiently longer than the SC-FDMA symbol time. Let ${\mathbf{H}_{\mathrm{t}}}^{(k)} \in \mathbb{C}^{(M+M_{cp})\times(M+M_{cp})}$ and ${\mathbf{G}_{\mathrm{t}}}^{(k)} \in \mathbb{C}^{(M+M_{cp})\times(M+M_{cp})}$ denote the Toeplitz time-domain channel matrices of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links, respectively. For example, $\mathbf{H}_{\mathrm{t}}^{(k)}$ has the following form

$$\mathbf{H}_{\mathrm{t}}^{(k)} = \begin{bmatrix} h^{(k)}(0) & 0 & 0 & \ldots & 0 \\ h^{(k)}(1) & h^{(k)}(0) & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ldots & \vdots \\ h^{(k)}(L_{\mathrm{B}}^{(k)}) & \ddots & \ddots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ldots & 0 \\ 0 & \ldots & h^{(k)}(L_{\mathrm{B}}^{(k)}) & \ldots & h^{(k)}(0) \end{bmatrix} \tag{2}$$

where $h^{(k)}(i)$ denotes the i-th tap for the $\mathrm{A}_k - \mathrm{B}$ channel impulse response (CIR). Each CIR tap of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links has an average gain of $\sigma_{\mathrm{A-B}}^{2(k)}$ and $\sigma_{\mathrm{A-E}}^{2(k)}$, respectively.

At the receiver side, the CP is first removed using a CP removal matrix, denoted by $\mathbf{R}^{\mathrm{cp}} = \left[\mathbf{0}_{M\times M_{\mathrm{cp}}}\mathbf{I}_N\right] \in \mathbb{R}^{M\times(M+M_{\mathrm{cp}})}$. After that, an M-point FFT operation and a sub-channel de-mapping operation, denoted by $\mathbf{S}^{(k)^{\top}}$, are applied to extract the k-th user's data samples in the

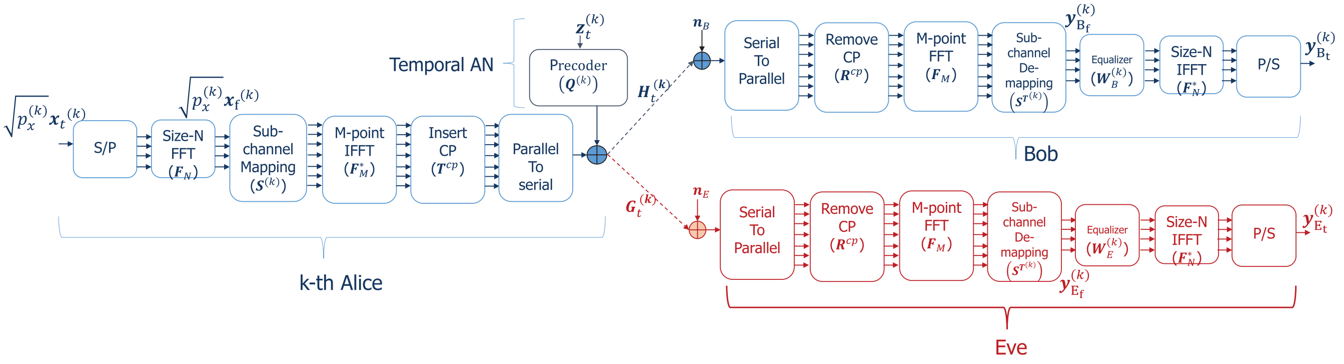

FIGURE 2. SC-FDMA system model with temporal AN.

frequency-domain as follows

$$\begin{aligned}\mathbf{y_B}_\mathrm{f}^{(k)} &= \mathbf{S}^{(k)}{}^\top\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{H}_\mathrm{t}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^*\mathbf{S}^{(k)}\mathbf{F}_N\sqrt{p_\mathrm{x}^{(k)}}\mathbf{x}_\mathrm{t}^{(k)}+\mathbf{n}_\mathrm{B}^{(k)}\\ &= \sqrt{p_\mathrm{x}^{(k)}}\mathbf{H}_\mathrm{f}^{(k)}\mathbf{x}_\mathrm{f}^{(\mathrm{k})}+\mathbf{n}_\mathrm{B}^{(k)} \qquad (3)\\ \mathbf{y_E}_\mathrm{f}^{(k)} &= \mathbf{S}^{(k)}{}^\top\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G}_\mathrm{t}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^*\mathbf{S}^{(k)}\mathbf{F}_N\sqrt{p_\mathrm{x}^{(k)}}\mathbf{x}_\mathrm{t}^{(k)}+\mathbf{n}_\mathrm{E}^{(k)}\\ &= \sqrt{p_\mathrm{x}^{(k)}}\mathbf{G}_\mathrm{f}^{(k)}\mathbf{x}_\mathrm{f}^{(\mathrm{k})}+\mathbf{n}_\mathrm{E}^{(k)} \qquad (4)\end{aligned}$$

where $\mathbf{n}_\mathrm{B}^{(k)} \sim \mathcal{CN}(0,\kappa_\mathrm{B})$ and $\mathbf{n}_\mathrm{E}^{(k)} \sim \mathcal{CN}(0,\kappa_\mathrm{E})$ denote the complex $N \times 1$ zero-mean circularly-symmetric additive white Gaussian noise (AWGN) vectors at Bob and Eve, respectively, $\kappa_\mathrm{B} = \Delta f\ \beta_\mathrm{B}$ and $\kappa_\mathrm{E} = \Delta f\ \beta_\mathrm{E}$ denote the noise power at Bob and Eve, respectively, Δf denotes the per-sub-channel bandwidth, β_B and β_E denote the AWGN variances at Bob and Eve, respectively. The matrices $\mathbf{H}_\mathrm{f}^{(k)} = \mathbf{S}^{(k)}{}^\top\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{H}_\mathrm{t}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^*\mathbf{S}^{(k)} \in \mathbb{C}^{N\times N}$ and $\mathbf{G}_\mathrm{f}^{(k)} = \mathbf{S}^{(k)}{}^\top\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G}_\mathrm{t}^{(k)}\mathbf{T}^{\mathrm{cp}}\mathbf{F}_M^*\mathbf{S}^{(k)} \in \mathbb{C}^{N\times N}$ denote the diagonal frequency-domain channel matrices of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links, respectively.

In the post-processing stage, channel equalization is carried out in the frequency domain. Then, an N-point IFFT operation is performed to recover the time-domain data samples. The k-th Alice's $N \times 1$ time-domain linearly equalized received vectors at Bob and Eve are given by

$$\mathbf{y_B}_\mathrm{t}^{(k)} = \mathbf{F}_N^*\mathbf{W}_\mathrm{B}^{(k)}\mathbf{H}_\mathrm{f}^{(k)}\mathbf{F}_N\sqrt{p_\mathrm{x}^{(k)}}\mathbf{x}_\mathrm{t}^{(k)}+\mathbf{F}_N^*\mathbf{W}_\mathrm{B}^{(k)}\mathbf{n}_\mathrm{B}^{(k)} \qquad (5)$$

$$\mathbf{y_E}_\mathrm{t}^{(k)} = \mathbf{F}_N^*\mathbf{W}_\mathrm{E}^{(k)}\mathbf{G}_\mathrm{f}^{(k)}\mathbf{F}_N\sqrt{p_\mathrm{x}^{(k)}}\mathbf{x}_\mathrm{t}^{(k)}+\mathbf{F}_N^*\mathbf{W}_\mathrm{E}^{(k)}\mathbf{n}_\mathrm{E}^{(k)} \qquad (6)$$

where $\mathbf{W}_\mathrm{B}^{(k)}$ and $\mathbf{W}_\mathrm{E}^{(k)} \in \mathbb{C}^{N\times N}$ are the linear equalization matrix filters for the k-th Alice data at Bob and Eve, respectively. We will investigate different design choices for $\mathbf{W}_\mathrm{B}^{(k)}$ and $\mathbf{W}_\mathrm{E}^{(k)}$ in addition to non-linear equalization at Eve in later sections. The SC-FDMA system symbol diagram is depicted in Fig. 2.

III. TEMPORAL AN DESIGN IN SC-FDMA

To confuse Eve, Alice sacrifices a portion of her transmit power to inject an AN signal in the time domain to exploit the temporal degrees of freedom provided by the CP. A precoding matrix, denoted by $\mathbf{Q}^{(k)} \in \mathbb{C}^{(M+M_\mathrm{cp})\times M_\mathrm{cp}}$, projects the AN vector to span the null space of the channel matrix between the k-th Alice and Bob by satisfying the following condition

$$\mathbf{R}^{\mathrm{cp}}\mathbf{H}_\mathrm{t}^{(k)}\mathbf{Q}^{(k)} = 0 \qquad (7)$$

Given that $\mathbf{Q}^{(k)}$ has M_cp orthonormal basis vectors, the k-th Alice can transmit a maximum of M_cp AN streams without harming Bob. Let $\mathbf{z}_\mathrm{t}^{(k)} \sim \mathcal{CN}(0,\Sigma_z^{(k)})$ denote the $M_\mathrm{cp} \times 1$ AN samples transmitted by the k-th Alice to confuse Eve. To cover all possible eavesdropping directions and maximize the AN randomness at Eve, each Alice sends uncorrelated AN samples. Hence, the AN covariance matrix, $\Sigma_z^{(k)}$, is diagonal with diagonal entries equal to the AN power for each AN stream. Let p_t denote the total transmit power available at each user. We assume that the k-th Alice divides her power such that a fraction $\alpha^{(k)} < 1$ of her total transmit power is allocated to data, i.e. $p_\mathrm{x}^{(k)} = \alpha^{(k)}\frac{p_\mathrm{t}}{N}$, and the remaining fraction, $\left(1-\alpha^{(k)}\right)$, is allocated to AN. Assuming that the k-th Alice knows her instantaneous CSI with Bob, she injects the AN signal in the null space of her channel matrix with Bob and, hence, the received signal at Bob in (5) will not change for all users. In contrast, the k-th Alice signal vector received at Eve in (6) is impaired with AN signals produced by all K Alices as follows

$$\begin{aligned}\mathbf{y_E}_\mathrm{t}^{(k)} = \mathbf{F}_N^*\mathbf{W}_\mathrm{E}^{(k)}\Bigg(&\mathbf{G}_\mathrm{f}^{(k)}\mathbf{F}_N\sqrt{p_\mathrm{x}^{(k)}}\mathbf{x}_\mathrm{t}^{(k)}+\mathbf{n}_\mathrm{E}^{(k)}\\ &+\mathbf{S}^{(k)}{}^\top\sum_{j=1}^{K}\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G}_\mathrm{t}^{(j)}\mathbf{Q}^{(j)}\mathbf{z}_\mathrm{t}^{(j)}\Bigg) \qquad (8)\end{aligned}$$

We emphasize here that this AN design does not assume knowledge of the Alices-Eve channels at the legitimate nodes. This is the best-case scenario for Eve where she remains passive and does not transmit to hide her CSI from the legitimate nodes. Furthermore, we assume that Eve has full knowledge of her own channel with all users as well as full knowledge of the Alices-Bob channels. For the considered block-fading channel environment, Bloch and Barros [30] showed that with main channel knowledge and no eavesdropper channel knowledge, wiretap codes that achieve the average secrecy rate exist. Therefore, in the next sections, we derive the ISR and then take the average over many coherence intervals to obtain the average secrecy rate.

IV. LINEAR SC-FDMA DATA DETECTION WITH TEMPORAL AN

In this section, we investigate two linear-detection strategies for SC-FDMA and derive the ISR for each strategy.

A. ZERO-FORCING (ZF) DETECTOR

A simple detection strategy at Bob and Eve is the zero-forcing (ZF) detector which completely eliminates the channel distortion by inverting the diagonal frequency domain channel matrices, i.e., $\mathbf{W}_{\mathrm{B}}^{(k)} = \mathbf{H}_{\mathrm{f}}^{(k)^{-1}}$ and $\mathbf{W}_{\mathrm{E}}^{(k)} = \mathbf{G}_{\mathrm{f}}^{(k)^{-1}}$ at Bob and Eve, respectively. Hence, the frequency-domain ZF-equalized received signals at Bob and Eve can be expressed, respectively, as

$$\mathbf{y}_{\mathrm{B_t}}^{(k)} = \sqrt{p_{\mathrm{x}}^{(k)}}\mathbf{x}_{\mathrm{t}}^{(k)} + \mathbf{F}_N^{*}\,\mathbf{H}_{\mathrm{f}}^{(k)^{-1}}\mathbf{n}_{\mathrm{B}}^{(k)} \tag{9}$$

$$\mathbf{y}_{\mathrm{E_t}}^{(k)} = \sqrt{p_{\mathrm{x}}^{(k)}}\mathbf{x}_{\mathrm{t}}^{(k)} + \mathbf{F}_N^{*}\,\mathbf{G}_{\mathrm{f}}^{(k)^{-1}}\left(\mathbf{n}_{\mathrm{E}}^{(k)} + \mathbf{S}^{(k)^{\top}}\sum_{j=1}^{K}\mathbf{O}^{(j)}\mathbf{z}_{\mathrm{t}}^{(j)}\right) \tag{10}$$

where the term $\mathbf{S}^{(k)^{\top}}\mathbf{O}^{(j)}\mathbf{z}_{\mathrm{t}}^{(j)}$ represents the interference signal affecting the k-th user data at Eve's receiver due to the AN transmission from User j, and the term $\mathbf{O}^{(j)}$ is given by $\mathbf{O}^{(j)} = \mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G_t}^{(j)}\mathbf{Q}^{(j)}$. At Bob, ZF equalization correlates the AWGN samples resulting in a noise covariance matrix of $\mathbb{E}\left(\mathbf{F}_N^{*}\mathbf{H}_{\mathrm{f}}^{(k)^{-1}}\mathbf{n}_{\mathrm{B}}^{(k)}\mathbf{n}_{\mathrm{B}}^{(k)*}\mathbf{H}_{\mathrm{f}}^{(k)^{-1*}}\mathbf{F}_N\right) = \kappa_{\mathrm{B}}\mathbf{F}_N^{*}|\mathbf{H}_{\mathrm{f}}^{(k)^{-1}}|^{2}\mathbf{F}_N$. At Eve, ZF equalization does not only correlate the AWGN, but it also ignores the AN which can severely impact ZF performance.

After ZF equalization, each data sample is decoded independently. Hence, the data rates of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links are, respectively, given by

$$R_{\mathrm{B}}^{(k)} = \sum_{i=1}^{N}\log_2\left(1 + \frac{p_{x_i}^{(k)}}{\gamma_{\mathrm{B},n_i}^{2(k)}}\right) \tag{11}$$

$$R_{\mathrm{E}}^{(k)} = \sum_{i=1}^{N}\log_2\left(1 + \frac{p_{x_i}^{(k)}}{\gamma_{\mathrm{E},n_i}^{2(k)} + \gamma_{\mathrm{E},z_i}^{2(k)}}\right) \tag{12}$$

where $\gamma_{\mathrm{B},n_i}^{2(k)}$ and $\gamma_{\mathrm{E},n_i}^{2(k)}$ represent the AWGN powers across the i-th sample at Bob and Eve, respectively, which are given by

$$\gamma_{\mathrm{B},n_i}^{2(k)} = \mathrm{diag}\left\{\mathbf{F}_N^{*}|\mathbf{H}_{\mathrm{f}}^{(k)^{-1}}|^{2}\,\mathbf{F}_N\right\}_{i,i}\kappa_{\mathrm{B}} \tag{13}$$

$$\gamma_{\mathrm{E},n_i}^{2(k)} = \mathrm{diag}\left\{\mathbf{F}_N^{*}|\mathbf{G}_{\mathrm{f}}^{(k)^{-1}}|^{2}\,\mathbf{F}_N\right\}_{i,i}\kappa_{\mathrm{E}} \tag{14}$$

where $\gamma_{\mathrm{E},z_i}^{2(k)}$ represents the AN power affecting the i-th data sample at Eve's receiver which is given by

$$\gamma_{\mathrm{E},z_i}^{(k)^2} = \mathrm{diag}\left\{\mathbf{F}_N^{*}\mathbf{G}_{\mathrm{f}}^{(k)^{-1}}\mathbf{S}^{(k)^{\top}}\left(\sum_{j=1}^{K}\mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)\right. \\ \left.\times\mathbf{S}^{(k)}\mathbf{G}_{\mathrm{f}}^{(k)^{-1*}}\mathbf{F}_N\right\}_{i,i} \tag{15}$$

Using the achievable rates of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ links, the ISR of user k (in bits/sec/Hz) is given by

$$R_s^{(k)} = \frac{1}{M + M_{\mathrm{cp}}}\left[R_{\mathrm{B}}^{(k)} - R_{\mathrm{E}}^{(k)}\right]^{+} \tag{16}$$

The sum ISR of all users is thus given by

$$R_s = \sum_{k=1}^{K}R_s^{(k)} \tag{17}$$

Remark 1: From (10) *and* (12)*, we observe that all M data samples at Eve are perturbed by the AN interference from every Alice even though each Alice transmits only $M_{\mathrm{cp}} \ll M$ AN streams. This suggests that the AN interference is highly correlated across the M data samples within the same SC-FDMA data symbol. The ZF strategy detects each sample independently and does not account for this AN correlation. In the next subsections, we show that Eve can exploit the AN correlation to reduce its effects by adopting either an MMSE or an ML detection strategy. In particular, the MMSE detector jointly filters all samples within an SC-FDMA symbol simultaneously but detects each sample separately using a hard-decision device (slicer). The ML detector enables Eve to further exploit the AN correlation and minimize the interference by jointly filtering and detecting all samples within an SC-FDMA symbol in the time domain.*

B. LINEAR BLOCK MINIMUM MEAN-SQUARE ERROR (MMSE) DETECTOR

The MMSE detector [31] tackles the well-known noise enhancement problem of the ZF detector. The price paid is the need to estimate the noise covariance matrix. In this subsection, we investigate the achieved ISR when Bob and Eve use the block linear MMSE detection strategy which balances between minimizing inter-symbol interference (ISI) and noise enhancement. For the MMSE detector, the receive matrix filter, denoted by $\mathbf{W}$, can be expressed as follows

$$\mathbf{W} = \mathbf{R}_{\mathrm{xy}}\mathbf{R}_{\mathrm{yy}}^{-1} \tag{18}$$

where $\mathbf{R}_{\mathrm{xy}}$ is the cross-covariance matrix between the frequency-domain transmitted data vector, $\mathbf{x}_{\mathrm{f}}$, and the frequency-domain received signal vector, $\mathbf{y}_{\mathrm{f}}$, and $\mathbf{R}_{\mathrm{yy}}$ is the received signal covariance matrix in the frequency-domain. Hence, the error-covariance matrix is given by

$$\mathbf{R}_{\mathrm{ee}} = \mathbf{R}_{\mathrm{xx}} - \mathbf{R}_{\mathrm{xy}}\mathbf{R}_{\mathrm{yy}}^{-1}\mathbf{R}_{\mathrm{yx}} \tag{19}$$

where $\mathbf{R}_{\mathrm{xx}}$ is the covariance matrix of the frequency-domain transmitted data vector. Since Bob experiences AWGN noise along with the ISI, his linear MMSE detection filter for the k-th user's data samples is given by

$$\mathbf{W}_{\mathrm{B}}^{(k)} = p_x^{(k)} \mathbf{H}_{\mathrm{f}}^{(k)*} \left(p_x^{(k)} \mathbf{H}_{\mathrm{f}}^{(k)} \mathbf{H}_{\mathrm{f}}^{(k)*} + \kappa_{\mathrm{B}} \mathbf{I}_N \right)^{-1} \tag{20}$$

Since $\mathbf{H}_{\mathrm{f}}^{(k)}$ is a diagonal matrix, Bob can filter each sub-channel independently where the i-th sub-channel filter is then given by

$$w_{\mathrm{B_i}}^{(k)} = \frac{\left[\mathbf{H}_{\mathrm{f}}^{(k)}\right]_{i,i}^{*}}{|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2 + \frac{\kappa_{\mathrm{B}}}{p_x^{(k)}}} \tag{21}$$

Bob's estimation error covariance matrix is given by

$$\mathbf{R}_{\mathrm{ee,B}}^{(k)} = \left(\mathbf{I}_N + \frac{p_x^{(k)}}{\kappa_{\mathrm{B}}} \mathbf{H}_{\mathrm{f}}^{(k)*} \mathbf{H}_{\mathrm{f}}^{(k)} \right)^{-1} \tag{22}$$

where $\left[\mathbf{H}_{\mathrm{f}}^{(k)}\right]_{i,i}$ is the i-th diagonal entry of $\mathbf{H}_{\mathrm{f}}^{(k)}$. The inverse in (22) is easy to compute since the inverted matrix is diagonal. Therefore, the i-th sub-channel estimation error variance is given by

$$\left[\mathbf{R}_{\mathrm{ee,B}}^{(k)}\right]_{i,i} = \frac{1}{1 + \frac{p_x^{(k)}}{\kappa_{\mathrm{B}}} |\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2} \tag{23}$$

The unbiased decision point SINR for sample i can be expressed as

$$\mathrm{SINR}_{\mathrm{B_i}}^{(k)} = \frac{1}{\left[\mathbf{R}_{\mathrm{ee,B}}^{(k)}\right]_{i,i}} - 1 \tag{24}$$

Hence, the rate of the k-th Alice-Bob link is given by

$$\begin{aligned} R_{\mathrm{B}}^{(k)} &= \sum_{i=1}^{N} \log_2 \left(1 + \mathrm{SINR}_{\mathrm{B}_i}^{(k)} \right) \\ &= \sum_{i=1}^{N} \log_2 \left(1 + \frac{p_{\mathrm{x}}^{(k)} |\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}} \right) \end{aligned} \tag{25}$$

In addition to ISI and AWGN, Eve's received signal is perturbed by the temporal AN interference transmitted by all K users. Let $\tilde{\mathbf{n}}_{\mathrm{E}}^{(k)}$ denote the $N \times 1$ equivalent noise vector which includes both the AN and the AWGN, i.e.,

$$\tilde{\mathbf{n}}_{\mathrm{E}}^{(k)} = \mathbf{n}_{\mathrm{E}}^{(k)} + \mathbf{S}^{(k)\top} \sum_{j=1}^{K} \mathbf{O}^{(j)} \mathbf{z}_{\mathrm{t}}^{(j)} \tag{26}$$

We consider the worst-case security scenario where Eve has perfect knowledge of the CSI of the Alice-Bob link. Hence, she knows the null space precoder and can exploit the AN correlation across the data samples within the same SC-FDMA symbol in her MMSE filter design to mitigate the AN effect. The cross-covariance matrix between the frequency-domain received and the transmitted data vectors, denoted by $\mathbf{R}_{\mathrm{yx,E}}^{(\mathrm{k})}$, as well as the received signal covariance matrix at Eve's receiver, denoted by $\mathbf{R}_{\mathrm{yy,E}}^{(\mathrm{k})}$, are given, respectively, by

$$\mathbf{R}_{\mathrm{yx,E}}^{(\mathrm{k})} = \sqrt{p_{\mathrm{x}}^{(k)}} \mathbf{G}_{\mathrm{f}}^{(k)} \tag{27}$$

$$\mathbf{R}_{\mathrm{yy,E}}^{(\mathrm{k})} = p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} + \mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)} \tag{28}$$

where $\mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)}$ is the AN-plus-AWGN covariance matrix at Eve's receiver which is given by

$$\mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)} = \kappa_{\mathrm{E}} \mathbf{I}_N + \mathbf{S}^{(k)\top} \left(\sum_{j=1}^{K} \mathbf{O}^{(j)} \Sigma_{\mathrm{z}}^{(j)} \mathbf{O}^{(j)*} \right) \mathbf{S}^{(k)} \tag{29}$$

From (19) and (28), the MMSE filter matrix and the error-covariance matrix at Eve's receiver are given, respectively, by

$$\mathbf{W}_{\mathrm{E}}^{(k)} = \sqrt{p_{\mathrm{x}}^{(k)}} \mathbf{G}_{\mathrm{f}}^{(k)*} \left(p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} + \mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)} \right)^{-1} \tag{30}$$

$$\mathbf{R}_{\mathrm{ee,E}}^{(k)} = \mathbf{I}_N - p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \left(p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} + \mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)} \right)^{-1} \mathbf{G}_{\mathrm{f}}^{(k)} \tag{31}$$

The decision-point SINR at the i-th sub-channel can be obtained from (31) and (24) as follows

$$\mathrm{SINR}_{\mathrm{E}_i}^{(k)} = \frac{1}{\left[\mathbf{R}_{\mathrm{ee,E}}^{(k)}\right]_{i,i}} - 1 \tag{32}$$

Hence, the data rate of the k-th Alice-Eve link is given by

$$\mathbf{R}_{\mathrm{E}}^{(k)} = \sum_{i=1}^{N} \log_2 \left(1 + \mathrm{SINR}_{\mathrm{E}_i}^{(k)} \right) \tag{33}$$

The ISR and the sum ISR are computed, respectively, from (16) and (17). We emphasize that, from (21) and (23), Bob's block MMSE detector simplifies to per-sub-channel filtering. In contrast, from (30) and (31), Eve's block MMSE detector is much more complicated since it requires matrix inversion and joint filtering of all the received samples within the SC-FDMA symbol.

In the following two sections, we derive the achieved ISR when even more complicated detectors are implemented at Eve while Bob is still constrained to the simple per-sub-channel detectors of Section IV.

V. SINGLE-USER (SU) MAXIMUM LIKELIHOOD (ML) DETECTOR AT EVE

With equally-likely input symbols, the minimum error rate single-user (SU) detection strategy is the joint ML detection of all of the user's data symbols. This can be realized by performing exhaustive search over all of the k-th user's data symbols within the codeword which requires very high computational complexity and can not be implemented using a linear filter. Using ML detection, Eve can further exploit the AN correlation across the k-th user's data samples and reduce the AN effects. In this case, the data rate of the k-th Alice-Eve link is given by

$$R_{\mathrm{E}}^{(k)} = \log_2 \det\Bigg(\mathbf{I}_N + p_{\mathrm{x}}^{(k)}\mathbf{G}_{\mathrm{f}}^{(k)}\mathbf{G}_{\mathrm{f}}^{(k)*} \times \left\{\kappa_{\mathrm{E}}\mathbf{I}_N + \mathbf{S}^{(k)\top}\left(\sum_{j=1}^{\mathrm{K}}\mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)\mathbf{S}^{(k)}\right\}^{-1}\Bigg) \tag{34}$$

Similar to the linear detection methods, the ISR and the sum ISR under SU ML detection can be derived, respectively, using (16) and (17). Even though ML is the optimal detector in the sense that it minimizes the error rate for equally-likely data samples, its complexity increases exponentially with the number of users' samples per symbol.

Proposition 1: Let $L_{\mathrm{u}}^{(k)}$ denote the maximum of the channel memories of the k-th Alice-Bob and k-th Alice-Eve links (i.e., $L_{\mathrm{u}}^{(k)} = \max(L_{\mathrm{B}}^{(k)}, L_{\mathrm{E}}^{(k)})$. There are $(M_{\mathrm{cp}} - L_{\mathrm{u}}^{(k)})$ useless AN directions that project the AN signals in the null space of the equivalent channel matrix of the k-th Alice-Eve link, and $L_{\mathrm{u}}^{(k)}$ useful AN directions that can degrade Eve's instantaneous rate. The useful AN streams can be extracted by designing the null space precoder as in (56).

Proof: See Appendix A. □

This proposition suggests that although the k-th Alice can transmit a maximum of M_{cp} AN streams in Bob's null space, only $L_{\mathrm{u}}^{(k)} \leq M_{\mathrm{cp}}$ of them are useful in the sense that they hurt Eve. Hence, increasing M_{cp} without changing the channel memories of the Alices-Bob and Alices-Eve links will not increase the ISR.

Proposition 2: Assuming SU ML detection at Eve, at very high input SNR levels, the average secrecy rate (in bits/sec/Hz) is approximated as follows

$$\frac{1}{M + M_{\mathrm{cp}}}\mathbb{E}\left\{\left[R_{\mathrm{B}}^{(k)} - R_{\mathrm{E}}^{(k)}\right]^{+}\right\} \gtrapprox \frac{\max_k\{L_{\mathrm{u}}^{(k)}\}}{M + M_{\mathrm{cp}}}\log_2\left(\frac{p_{\mathrm{t}}}{N\kappa_{\mathrm{B}}}\right) \tag{35}$$

Proof: See Appendix B. □

This is a very promising result since it shows that using our proposed temporal AN design, increasing the input power level, denoted by p_{t}, can increase the average secrecy rate unlike the no-AN case. Moreover, the average secrecy rate is always positive and increases linearly with the number of useful AN streams, $L_{\mathrm{u}}^{(k)}$. In Fig. 3, we compare the simulated average secrecy rate with the derived theoretical approximation. Fig. 3 verifies the tightness of the approximation especially at high input SNR levels. The Alices design the rates of the wiretap codes based on the average secrecy rate. However the average secrecy rate depends on the detection strategies at both Bob and Eve. Since the Alices do not know which detection strategy Eve is using, the Alices design the wiretap codes assuming the worst-case scenario where Eve employs an ML detector. Wiretap codes are also designed assuming a conventional per-sub-channel detector at Bob to reduce his detector's complexity. In Appendix C, we discuss the Wiretap codes design based on the average secrecy rate without the knowledge of the A$_k$−E channels at the legitimate nodes.

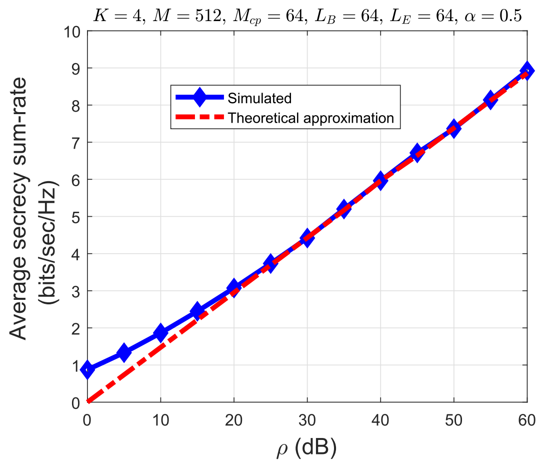

FIGURE 3. Simulated average secrecy sum-rate and the derived theoretical approximation versus SNR.

VI. MULTI-USER (MU) DETECTION AT EVE

In the previous sections, the SU detectors at Bob and Eve separated each user's data using the sub-channel de-mapping matrix, $\mathbf{S}^{(k)\top}$, prior to data detection. However, in MU detection, multiple users' data samples are detected simultaneously. From a performance perspective, MU detection is equivalent to SU detection when the data streams of the different users do not interfere with each other. This is the case at Bob's receiver since there is no AN. However, at Eve's receiver, each temporal AN sample interferes with all users' data samples within the size-M SC-FDMA symbol. This suggests that the AN is correlated across all users' samples within the SC-FDMA symbol as discussed in Remark 1. Hence, MU detection can enhance the detection performance at Eve at the expense of increased complexity. In the following subsections, we will assume that Eve can perform MU detection and we will evaluate the achieved sum ISR.

A. MULTI-USER (MU) MMSE DETECTOR

To perform MU detection, Eve re-arranges all users' frequency-domain data samples into a single $M \times 1$ vector denoted by, $\mathbf{y}_{\mathrm{Ef}} = \left[\mathbf{y}_{\mathrm{E\ f}}^{(1)}, \mathbf{y}_{\mathrm{E\ f}}^{(2)}, \ldots\ \mathbf{y}_{\mathrm{E\ f}}^{(K)}\right]^{\top}$, which is expressed as follows

$$\mathbf{y}_{\mathrm{Ef}} = \mathbf{G}_{\mathrm{f}}\mathbf{P}_{\mathrm{x}}^{\frac{1}{2}}\mathbf{x}_{\mathrm{f}} + \tilde{\mathbf{n}}_{\mathrm{E}} \tag{36}$$

The $M \times M$ diagonal matrix $\mathbf{G}_{\mathrm{f}}$ represents the equivalent channel matrix at Eve for all users in which the k-th data symbol matrix is $\mathbf{G}_{\mathrm{f}}^{(k)}$, $\mathbf{x}_{\mathrm{f}}$ denotes the $M \times 1$ frequency-domain transmitted data vector of all users which is given by $\left[\mathbf{x}_{\mathrm{f}}^{(1)}, \mathbf{x}_{\mathrm{f}}^{(2)}, \ldots, \mathbf{x}_{\mathrm{f}}^{(K)}\right]^{\top}$. In addition, $\tilde{\mathbf{n}}_{\mathrm{E}}$ denotes the equivalent AWGN-plus-AN vector at Eve, which is given by $\left[\tilde{\mathbf{n}}_{\mathrm{E}}^{(1)}, \tilde{\mathbf{n}}_{\mathrm{E}}^{(2)}, \ldots, \tilde{\mathbf{n}}_{\mathrm{E}}^{(K)}\right]^{\top}$, and the diagonal matrix $\mathbf{P}_{\mathrm{x}} \in \mathbb{R}^{M\times M}$

represents the data transmit power matrix which contains the transmit power levels for all users' data samples and is given by

$$\mathbf{P}_{\mathrm{x}} = \mathrm{diag}\Bigg(\underbrace{p_{\mathrm{x}}^{(1)}, p_{\mathrm{x}}^{(1)}, \dots\, p_{\mathrm{x}}^{(1)}}_{N \text{ terms}}, \underbrace{p_{\mathrm{x}}^{(2)}, \dots\, p_{\mathrm{x}}^{(2)}}_{N \text{ terms}}, \dots, \underbrace{p_{\mathrm{x}}^{(K)}, \dots\, p_{\mathrm{x}}^{(K)}}_{N \text{ terms}}\Bigg) \quad (37)$$

Similar to (29), (30) and (31), the $M \times M$ noise covariance matrix, the size-M MMSE filter matrix, and the estimation error covariance matrix can be expressed, respectively, as

$$\mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}} = \kappa_{\mathrm{E}}\mathbf{I}_{\mathrm{M}} + \mathbf{G}_{\mathrm{f}}^{-1}\left(\sum_{j=1}^{K}\mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)\mathbf{G}_{\mathrm{f}}^{-1*}$$

$$\mathbf{W}_{\mathrm{E}} = \mathbf{P}_{\mathrm{x}}^{\frac{1}{2}}\mathbf{G}_{\mathrm{f}}^{*}\left(\mathbf{G}_{\mathrm{f}}\mathbf{P}_{\mathrm{x}}\mathbf{G}_{\mathrm{f}}^{*} + \mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)}\right)^{-1}$$

$$\mathbf{R}_{\mathrm{ee},\mathrm{E}} = \mathbf{I}_{M} - \mathbf{P}_{\mathrm{x}}^{\frac{1}{2}}\mathbf{G}_{\mathrm{f}}^{*}\left(\mathbf{G}_{\mathrm{f}}\mathbf{P}_{\mathrm{x}}\mathbf{G}_{\mathrm{f}}^{*} + \mathbf{R}_{\tilde{\mathrm{n}}\tilde{\mathrm{n}},\mathrm{E}}^{(k)}\right)^{-1}\mathbf{G}_{\mathrm{f}}\mathbf{P}_{\mathrm{x}}^{\frac{1}{2}} \quad (38)$$

We emphasize here that, in contrast to SU MMSE detection, the MU MMSE detector at Eve exploits the temporal AN correlation across all M-sub-channels of all users to mitigate the AN effects. However, this requires a much higher computational complexity at Eve since the $N \times N$ matrix inversion in the SU detection is now an $M \times M$ matrix inversion as shown in (38). The decision-point SINR for the i-th sample is given by

$$\mathrm{SINR}_{\mathrm{E}_i} = \frac{1}{\left[\mathbf{R}_{\mathrm{ee},\mathrm{E}}\right]_{i,i}} - 1 \quad (39)$$

Hence, the rate of the k-th Alice-Eve link is given by

$$\mathbf{R}_{\mathrm{E}}^{(k)} = \sum_{i \in \nu^{(k)}} \log_2\left(1 + \mathrm{SINR}_{\mathrm{E}_i}\right) \quad (40)$$

where $\nu^{(k)}$ is the set of samples assigned to user k. Similarly, the ISR and the sum ISR can be computed as in (16) and (17), respectively.

B. MULTI-USER (MU) ML DETECTOR

Similar to the MMSE case, Eve can jointly decode all users data simultaneously using an ML detector. This is the optimal detection strategy for Eve in terms of minimizing the error rate assuming equally-likely data symbols. However, it requires very high computation complexity. At Eve's receiver, the data samples are first re-arranged as in (36). Then, Eve performs exhaustive search across the M data samples of all users within the SC-FDMA symbol. In this case, Eve's sum-rate is given by

$$\sum_{k} R_{\mathrm{E}}^{(k)} = \log_2 \det\Bigg(\mathbf{I}_M + \mathbf{G}_{\mathrm{f}}\mathbf{P}_{\mathrm{x}}\mathbf{G}_{\mathrm{f}}^{*} \times\left(\kappa_{\mathrm{E}}\mathbf{I}_M + \sum_{j=1}^{K}\mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)^{-1}\Bigg) \quad (41)$$

Therefore, the sum ISR is given by

$$R_{\mathrm{s}} = \frac{1}{M + M_{\mathrm{cp}}}\left[\sum_{k} R_{\mathrm{B}}^{(k)} - \sum_{k} R_{\mathrm{E}}^{(k)}\right]^{+} \quad (42)$$

VII. HYBRID TEMPORAL AN SECRET KEY SCHEME

In the propsed temporal AN scheme, the k-th Alice and Bob exchange control and training sequences to estimate their links' channels. Bob designs the AN precoding matrices using Eqn. (7) based on the channel estimates and only feedbacks the designed AN precoder to the k-th Alice. In this section, for more practical considerations, we relax the global channel knowledge assumption at Eve. We assume that Eve exploits the shared training sequences to estimate her own channel with all Alices and Bob ($\mathrm{A}_k - \mathrm{E}$ and $\mathrm{B} - \mathrm{E}$ channels) perfectly. In addition, she overhears the shared AN precoding matrices but does not know the exact channel matrices between the Alices and Bob ($\mathrm{A}_k - \mathrm{B}$ channels). In this case, we propose enhancing the system security using a hybrid temporal-AN/secret-key (TAN-SK) scheme.

Next, we describe our proposed hybrid scheme. The k-th Alice (A_k) selects her data samples from a set of constellation points, denoted by $\mathcal{S}$, that is approximated to follow a Gaussian probability distribution [32]. Then, A_k and Bob start exchanging training and control signals to estimate the CSI of their links. Based on the channel reciprocity property, A_k and Bob exploit their channel estimates to generate identical secret key samples using any of the approaches in, e.g., [10], [14], and the references therein.[2] Let $\mathbf{r}^{(k)}$ denote the generated common secret key of size $N_{\mathrm{en}}^{(k)}$ where $\mathbf{r}^{(k)} = [r_1^{(k)}, r_2^{(k)}, \cdots, r_{N_{\mathrm{en}}^{(k)}}^{(k)}]$ with $r_i^{(k)} \in \mathcal{S}$. Eve is assumed to be sufficiently distant from all Alices and Bob such that the channel responses of her links $\mathrm{A}_k - \mathrm{E}$ and $\mathrm{B} - \mathrm{E}$ are independent from those of $\mathrm{A}_k - \mathrm{B}$ links and, hence, she can not generate the same secret key samples. Upon agreeing on secret key samples, A_k uses the generated secret key samples to encrypt an equivalent number of the data samples through an OTP encryption scheme. The OTP encryption scheme provides a one-to-one mapping between the time-domain unencrypted data sample, $x_{\mathrm{t}_i}^{(k)}$, and its encrypted version, $x_{\mathrm{t,en_i}}^{(k)}$, given knowledge of the secret key, $r_i^{(k)}$. The security is unbreakable since each secret key sample, $r_i^{(k)}$, is uniformly distributed over $\mathcal{S}$. Hence, no information is leaked to any eavesdropping node that intercepts the encrypted data samples [32].

[2] The channel-based secret key extraction process is beyond the scope of this paper. Secret key extraction algorithms for fading channels are given in [10] and [14], where Alice and Bob 1) exchange known control and training sequences and estimate their channels. Then, they perform error correction algorithms to reconcile errors between the measurements/generated secret keys at both Alice and Bob. 3) use one-way hash functions for privacy amplification [33] to ensure that Eve does not know the final secret key. We emphasize that due to the nature of the block-fading channel, the coherence time is much longer than the SC-FDMA symbol duration. Bi-directional channel estimation, reconciliation and privacy amplification typically take few SC-FDMA symbols which is negligible compared to the channel coherence time. Hence, their effect on the average secrecy rate can be neglected.

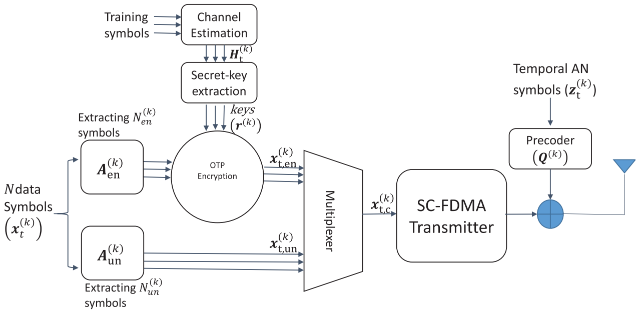

FIGURE 4. ***k*-th Alice's transmitter architecture to employ the hybrid TAN-SK scheme.**

In general, the key generation rates are lower than the achievable data rates. Only a fraction of the data samples (i.e., SC-FDMA sub-channels) can be encrypted using the extracted secret keys. Let $\mathbf{x}_{\mathrm{t,un}}^{(k)}$ denote the remaining unencrypted data samples of size $N_{\mathrm{un}}^{(k)}$ with $N_{\mathrm{un}}^{(k)} + N_{\mathrm{en}}^{(k)} = N$. The k-th Alice then multiplexes the encrypted data samples, $\mathbf{x}_{\mathrm{t,en}}^{(k)}$, with $\mathbf{x}_{\mathrm{t,un}}^{(k)}$, in the time domain to form the composite data signal, $\mathbf{x}_{\mathrm{t,c}}^{(k)}$. Temporal AN samples, $\mathbf{z}_{\mathrm{t}}^{(k)}$, are then added to the entire time-domain SC-FDMA data symbol to secure the unencrypted data samples. The proposed modified SC-FDMA transmitter employing the TAN-SK scheme is illustrated in Figure 4.

A. SINGLE-USER (SU) ML DETECTION WITH SECRET KEYS

Using linear detectors to detect the data samples at Eve can significantly degrade her performance since her received signal is perturbed by temporal AN interference and encryption from secret keys. Therefore, we focus in this section on the worst-case eavesdropping scenario where Eve applies the SU-ML and multi-user (MU) ML detectors. We assume that both Bob and Eve know the indices of the encrypted and the unencrypted samples in every SC-FDMA symbol. Since the encrypted samples are perfectly secure due to the OTP encryption with secret keys, Eve can only select the sub-channels containing the unencrypted data samples and jointly decode them. The time-domain received signal at Eve is given by

$$\mathbf{y}_{\mathrm{Et}}^{(k)} = \sqrt{p_{\mathrm{x}}^{(k)}}\,\mathbf{G}^{\mathrm{c}(k)}\mathbf{x}_{\mathrm{t,c}}^{(k)} + \mathbf{S}^{(k)\top}\mathbf{F}_N{}^{*}\sum_{j=1}^{K}\mathbf{O}^{(j)}\mathbf{z}_{\mathrm{t}}^{(j)} + \mathbf{n}_{\mathrm{E}}^{(k)} \tag{43}$$

where $\mathbf{G}^{\mathrm{c}(k)} = \mathbf{F}_N{}^{*}\mathbf{G}_{\mathrm{f}}^{(k)}\mathbf{F}_N$ is the equivalent circulant channel matrix of the $\mathrm{A}_k - \mathrm{E}$ link, $\mathbf{x}_{\mathrm{t,c}}^{(k)} \in \mathbb{C}^{N\times 1}$ is the data samples vector which is comprised of unencrypted data samples $\mathbf{x}_{\mathrm{t,un}}^{(k)}$ of length $N_{\mathrm{un}}^{(k)}$, in addition to the encrypted data samples $\mathbf{x}_{\mathrm{t,en}}^{(k)}$ of length $N_{\mathrm{en}}^{(k)}$, which is given by

$$\mathbf{x}_{\mathrm{t,c}}^{(k)} = \mathbf{A}_{\mathrm{un}}^{(k)}\mathbf{x}_{\mathrm{t,un}}^{(k)} + \mathbf{A}_{\mathrm{en}}^{(k)}\mathbf{x}_{\mathrm{t,en}}^{(k)} \tag{44}$$

where the $N \times N_{\mathrm{en}}^{(k)}$ matrix $\mathbf{A}_{\mathrm{en}}^{(k)}$ and the $N \times N_{\mathrm{un}}^{(k)}$ matrix, $\mathbf{A}_{\mathrm{un}}^{(k)}$ denote the binary matrices that map the encrypted and unencrypted data samples, respectively, to the composite data samples vector. For example, $\mathbf{A}_{\mathrm{un}}^{(k)}$ is given by

$$\left[\mathbf{A}_{\mathrm{un}}^{(k)}\right]_{i,j} = \begin{cases} 1, & \text{unencrypted symbol } j \text{ is mapped to} \\ & \text{data symbol } i \\ 0, & \text{Otherwise} \end{cases} \tag{45}$$

While extracting the unencrypted samples, Eve's received signal is perturbed by interference from temporal AN in addition to noise due to coupling with the encrypted samples. Therefore, the achievable rate of the Alice-Eve link using the SU ML detection strategy is given by

$$\begin{aligned} R_{\mathrm{E}}^{(k)} = \log_2 \det \Bigg(&\mathbf{I}_N + p_{\mathrm{x}}^{(k)}\mathbf{G}^{\mathrm{c}(k)}\mathbf{A}_{\mathrm{un}}^{(k)}\mathbf{A}_{\mathrm{un}}^{(k)*}\mathbf{G}^{\mathrm{c}(k)*} \\ &\times \Bigg\{ \kappa_{\mathrm{E}}\mathbf{I}_N + p_{\mathrm{x}}^{(k)}\mathbf{G}^{\mathrm{c}(k)}\mathbf{A}_{\mathrm{en}}^{(k)}\mathbf{A}_{\mathrm{en}}^{(k)*}\mathbf{G}^{\mathrm{c}(k)*} \\ &+ \mathbf{F}_N{}^{*}\mathbf{S}^{(k)\top}\left(\sum_{j=1}^{\mathrm{K}}\mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)\mathbf{S}^{(k)}\mathbf{F}_N \Bigg\}^{-1} \Bigg) \end{aligned} \tag{46}$$

From (25), the achievable rate of the k-th Alice-Bob link using the MMSE detection strategy can be divided into two terms for unencrypted and encrypted samples as follows

$$\begin{aligned} R_{\mathrm{B}}^{(k)} = &\sum_{i\in\mathcal{E}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right) \\ &+ \sum_{i\in\mathcal{U}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right) \end{aligned} \tag{47}$$

where $\mathcal{E}$ ($\mathcal{U}$) denotes the set of encrypted (unencrypted) sub-channels. The expression in (47) consists of two terms. The first term is perfectly secured due to encryption using the secret keys while the second term is unsecured and its security should be measured using the secrecy rate. Hence, the ISR of the legitimate system is given by

$$\begin{aligned} R_{\mathrm{s}}^{(k)} = \frac{1}{M + M_{\mathrm{cp}}} \Bigg\{ &\sum_{i\in\mathcal{E}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right) \\ &+ \left[\sum_{i\in\mathcal{U}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right) - R_{\mathrm{E}}^{(k)}\right]^{+} \Bigg\} \end{aligned} \tag{48}$$

We emphasize here that in our proposed hybrid TAN-SK scheme, the term $\sum_{i\in\mathcal{E}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right)$ in Eqn. (48) guarantees a positive ISR in contrast to the conventional PHY security schemes. Then, the sum ISR can be obtained as in Eqn. (17).

B. MULTI-USER (MU) ML DETECTION WITH SECRET KEYS

To perform MU ML detection over the unencrypted data samples, Eve re-arranges the received signals as discussed in

Section VI. In this case, the instantaneous sum-rate at Eve is given by

$$\begin{aligned}\sum_k R_{\mathrm{E}}^{(k)} &= \log_2 \det \Big(\mathbf{I}_M + \mathbf{G}_{\mathrm{un}}\mathbf{P}_{\mathrm{xun}}\mathbf{G}_{\mathrm{un}}^* \\ &\quad \times \left\{\kappa_{\mathrm{E}}\mathbf{I}_M + \mathbf{G}_{\mathrm{en}}\mathbf{P}_{\mathrm{xen}}\mathbf{G}_{\mathrm{en}}^* + \left(\sum_{j=1}^{\mathrm{K}} \mathbf{O}^{(j)}\Sigma_{\mathrm{z}}^{(j)}\mathbf{O}^{(j)*}\right)\right\}^{-1}\Big)\end{aligned} \tag{49}$$

where $\mathbf{G}_{\mathrm{un}} \in \mathbb{C}^{M\times\left(\sum_k N_{\mathrm{un}}^{(k)}\right)}$ and $\mathbf{G}_{\mathrm{en}} \in \mathbb{C}^{M\times\left(\sum_k N_{\mathrm{en}}^{(k)}\right)}$ denote the equivalent channel matrices of all-users' unencrypted and encrypted data samples, respectively, with block diagonal matrices $\mathbf{G}_{\mathrm{f}}^{(k)}\mathbf{A}_{\mathrm{un}}^{(k)}$ and $\mathbf{G}_{\mathrm{f}}^{(k)}\mathbf{A}_{\mathrm{en}}^{(k)}$, respectively. The matrices $\mathbf{P}_{\mathrm{xun}} \in \mathbb{R}^{\left(\sum_k N_{\mathrm{un}}^{(k)}\right)\times\left(\sum_k N_{\mathrm{un}}^{(k)}\right)}$ and $\mathbf{P}_{\mathrm{xen}} \in \mathbb{R}^{\left(\sum_k N_{\mathrm{en}}^{(k)}\right)\times\left(\sum_k N_{\mathrm{en}}^{(k)}\right)}$ denote the diagonal transmit power matrices whose diagonal entries are the data power of all-users' unencrypted and encrypted data samples, respectively, and are given by

$$\begin{aligned}\mathbf{P}_{\mathrm{xun}} = \mathrm{diag}\Bigg(&\underbrace{p_{\mathrm{x}}^{(1)}, p_{\mathrm{x}}^{(1)}, \dots p_{\mathrm{x}}^{(1)}}_{N_{\mathrm{un}}^{(1)} \text{ terms}}, \underbrace{p_{\mathrm{x}}^{(2)}, \dots p_{\mathrm{x}}^{(2)}}_{N_{\mathrm{un}}^{(2)} \text{ terms}}, \dots, \\ &\underbrace{p_{\mathrm{x}}^{(K)}, \dots p_{\mathrm{x}}^{(K)}}_{N_{\mathrm{un}}^{(K)} \text{ terms}}\Bigg)\end{aligned} \tag{50}$$

$$\begin{aligned}\mathbf{P}_{\mathrm{xen}} = \mathrm{diag}\Bigg(&\underbrace{p_{\mathrm{x}}^{(1)}, p_{\mathrm{x}}^{(1)}, \dots p_{\mathrm{x}}^{(1)}}_{N_{\mathrm{en}}^{(1)} \text{ terms}}, \underbrace{p_{\mathrm{x}}^{(2)}, \dots p_{\mathrm{x}}^{(2)}}_{N_{\mathrm{en}}^{(2)} \text{ terms}}, \dots, \\ &\underbrace{p_{\mathrm{x}}^{(K)}, \dots p_{\mathrm{x}}^{(K)}}_{N_{\mathrm{en}}^{(K)} \text{ terms}}\Bigg)\end{aligned} \tag{51}$$

The sum ISR is given by

$$\begin{aligned}R_{\mathrm{s}} = \frac{1}{M+M_{\mathrm{cp}}} &\left\{\sum_k \sum_{i\in\mathcal{E}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right)\right. \\ &\left. + \left[\sum_k \sum_{i\in\mathcal{U}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)}|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}\right) - \sum_k R_{\mathrm{E}}^{(k)}\right]^+\right\}\end{aligned} \tag{52}$$

Remark 2: The Alices-Eve's rate expressions in (46) *and* (49) *are based on the assumption that Eve knows the AN precoding matrices* $\mathbf{Q}^{(k)}$ $\forall k$*. Given that the null space of a matrix can be obtained from the singular value decomposition (SVD) of that matrix (i.e., by selecting the right singular vectors corresponding to zero singular values), knowledge of the AN precoding matrix,* $\mathbf{Q}^{(k)}$*, may imply that Eve knows some information about the Alices-Bob channel matrices. This, in turn, might sacrifice the key's security which is based on the CIR of the Alices-Bob links. However, as shown in [32, Lemma 1], the right singular vectors of a random matrix do not reveal any information about the matrix itself. Hence, even when Eve knows the AN precoding matrix, she does not know the matrix itself and this information does not reveal additional correlated information about the CSI of the Alices-Bob links. Therefore, we can assume that Eve has full knowledge of the null space matrices without compromising the information-theoretic security.*

Remark 3: For the temporal AN only scheme in a multiple non-colluding eavesdroppers scenario, under a generalized detection setting, we assume a total of J eavesdroppers using different detection strategies. In this case, k-th Alice's ISR is given by

$$R_{\mathrm{s}}^{(\mathrm{k})} = \frac{1}{M+M_{\mathrm{cp}}}\left[R_{\mathrm{B}}^{(k)} - \max_{\mathrm{j}=1,2,\dots,\mathrm{J}} R_{\mathrm{E}_j}{}^{(k)}\right]^+ \tag{53}$$

where $R_{\mathrm{B}}^{(k)}$ *is calculated using Eqn.* (25) *for linear MMSE detector at Bob while the* k^{th} *Alice*$-j^{\mathrm{th}}$ *Eve's instantaneous link rate,* $R_{\mathrm{E}_j}{}^{(k)}$*, is calculated from Eqn.* (12), (33) *or* (34) *depending on the l-th Eve's detection strategy. For the TAN-SK scheme, the ISR in a multiple non-colluding eavesdroppers scenario is given by*

$$R_{\mathrm{s}}^{(\mathrm{k})} = \frac{1}{M+M_{\mathrm{cp}}}\left(R_{\mathrm{B}}^{(k)}{}_{\mathrm{un}} + \left[R_{\mathrm{B}}^{(k)}{}_{\mathrm{en}} - \max_{\mathrm{j}=1,2,\dots,\mathrm{J}} R_{\mathrm{E}_j}{}^{(k)}\right]^+\right) \tag{54}$$

where $R_{\mathrm{B}}^{(k)}{}_{\mathrm{un}}$ *and* $R_{\mathrm{B}}^{(k)}{}_{\mathrm{en}}$ *are the* $\mathrm{A}_k-\mathrm{B}$ *instantaneous rate over the unencrypted and encrypted sub-channels, respectively which are calculated from the two terms of Eqn.* (47) *for the linear MMSE detector at Bob. The* k^{th} *Alice*$-j^{\mathrm{th}}$ *Eve's instantaneous link rate,* $R_{\mathrm{E}_j}{}^{(k)}$*, can be calculated from Eqn.* (46) *for the SU ML detector at Eve.*

VIII. SIMULATION RESULTS

In this section, we evaluate the average secrecy rate performance of the temporal-AN scheme in SC-FDMA systems under the investigated detection strategies. Due to the space limitations, we plot the average secrecy sum-rate using the same parameters for all users. The per-user average secrecy rate can therefore be obtained by dividing the average secrecy sum-rate over the number of users due to the symmetry in parameters. Unless stated explicitly, we consider an SC-FDMA system with $K = 8$ users, $M = 512$, $N = 64$, $M_{\mathrm{cp}} = 64$, $L_{\mathrm{B}} = L_{\mathrm{B}}^{(k)} = 64\ \forall\ k$, $L_{\mathrm{E}} = L_{\mathrm{E}}^{(k)} = 64\ \forall\ k$, and $\rho = \frac{p_t}{N\kappa_{\mathrm{B}}} = \frac{p_t}{N\kappa_{\mathrm{E}}} = 30$ dB. Each CIR tap has an average power of $\sigma_{\mathrm{A-B}}^{2(k)} = 1/(L_{\mathrm{B}}^{(k)}+1)$ and $\sigma_{\mathrm{A-E}}^{2(k)} = 1/(L_{\mathrm{E}}^{(k)}+1)\ \forall k$, (i.e., uniform power delay profile). We assume $\alpha = \alpha^{(k)} = 0.7\ \forall\ k$, which means that 70% of the total transmit power is assigned to data signals and the remaining 30% is assigned to AN signals. The data power is divided equally across the data samples and the AN power is divided equally across the AN samples.

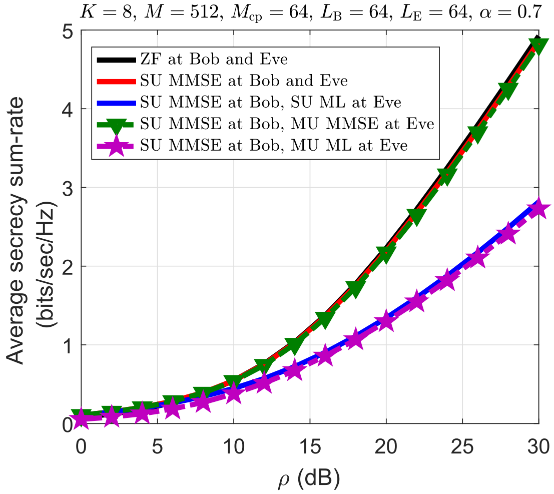

FIGURE 5. Average secrecy sum-rate versus SNR for different detection strategies.

Fig. 5 depicts the achieved average secrecy sum-rate using the temporal-AN scheme versus the input SNR when Eve uses different detection strategies (SU ZF, SU MMSE, MU MMSE, SU ML, and MU ML) while Bob is constrained to simple linear detection strategies (SU ZF and SU MMSE). As Bob and Eve increase their detector complexity from ZF to MMSE, both of them achieve gains in their link rates. That is why the SU ZF and the SU MMSE detectors achieve close secrecy rate performance. As Eve adopts the ML detection strategy, she exploits the correlation properties of the temporal AN to minimize its effect as explained in Remark 1. As a result, Eve achieves gains in her link rate and the average secrecy rate decreases. Fig. 5 also reveals that the average secrecy rate gains that Eve achieves by adopting MU detection strategies (MMSE or ML) result in a slight degradation in the achieved secrecy rate. This demonstrates the robustness of the proposed temporal AN scheme to high-complexity detectors at Eve. Even when Eve has very high computational capabilities while Bob maintains simple per-sub-channel detection schemes (SU ZF and SU MMSE), a high average secrecy rate is achieved.

In Fig. 6, we show the achieved average secrecy rate versus the transmit power fraction parameter, α, for different detection strategies at Bob and Eve. The case of $\alpha = 1$ corresponds to the benchmark case of no-AN injection. Therefore, Fig. 6 quantifies the average secrecy rate gain of our proposed temporal-AN scheme compared to the no-AN injection scenario.

Figs 7 and 8 depict the achieved average secrecy rates for different detection strategies as L_{B} and L_{E} increase, respectively. As discussed in Proposition 1, the number of useful AN streams depends on the channel memories of the Alices-Bob and Alices-Eve links. Dispersive channels can accommodate more useful AN streams. Increasing the number of useful AN streams introduces diversity in interference and reduces the AN correlation at Eve. Therefore, the Alices-Eve link rates experience more degradation and the secrecy rate is boosted.

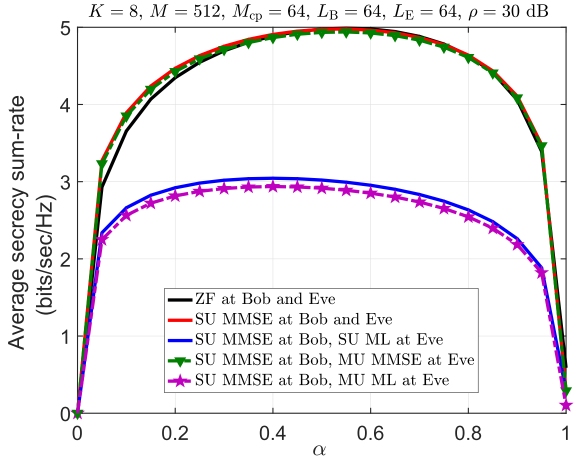

FIGURE 6. Average secrecy sum-rate versus the power fraction allocation parameter, α.

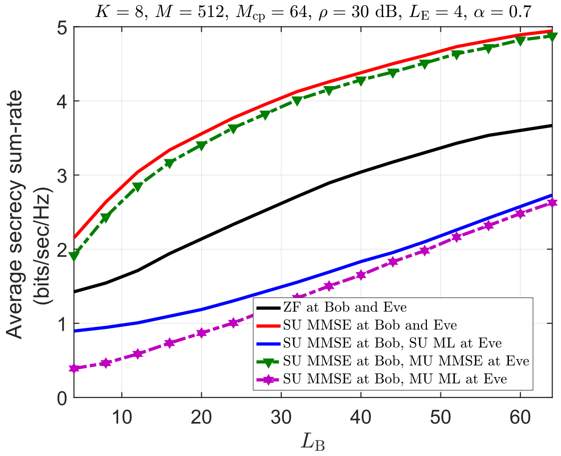

FIGURE 7. Average secrecy sum-rate versus Alices-Bob's channel memory, L_{B}.

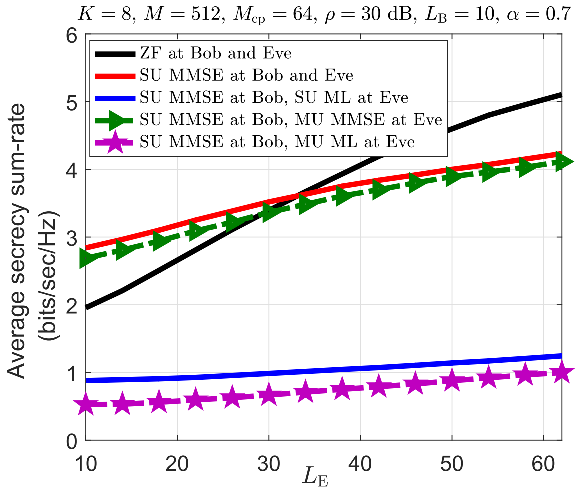

FIGURE 8. Average secrecy sum-rate versus Alices-Eve's channel memory, L_{E}.

Fig 9 depicts the average secrecy rate performance for different detection strategies versus the number of users, K. We fix M and M_{cp} while $N = M/K$ varies as we vary K.

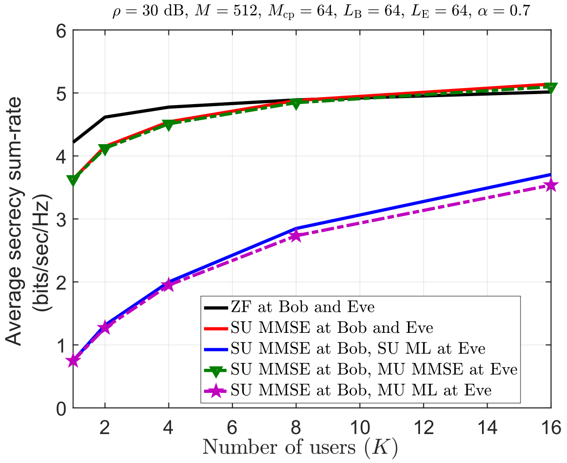

FIGURE 9. Average secrecy sum-rate versus the number of users, K.

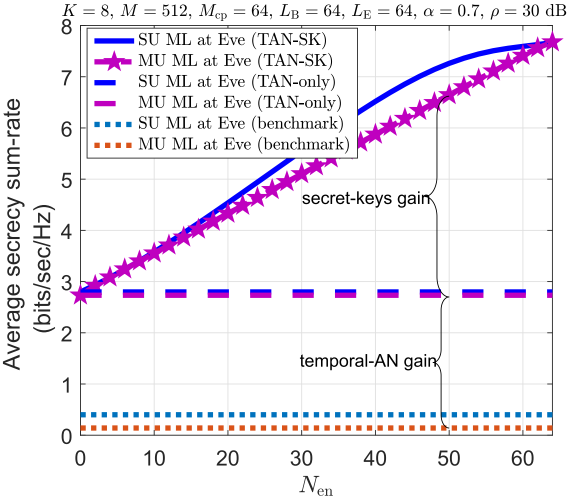

FIGURE 10. Average secrecy sum-rate of the hybrid TAN-SK scheme versus the number of encrypted samples, $N_{\rm en}$.

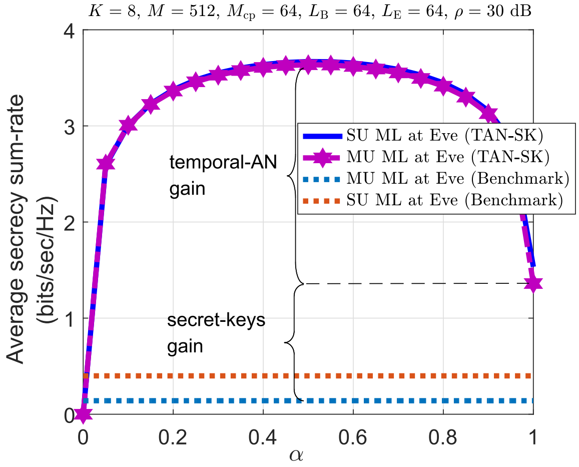

FIGURE 11. Average secrecy sum-rate of the hybrid TAN-SK scheme versus the power fraction allocation parameter, α.

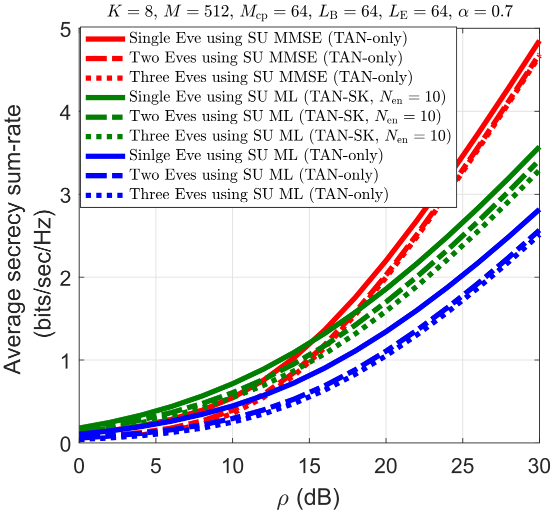

FIGURE 12. Average secrecy sum-rate under multiple eavesdroppers scenario.

Each user transmits a temporal AN signal that not only interferes with Eve's reception of the user's own data signal, but it interferes with Eve's reception of the other users' signals as well. This, in turn, increases the achieved average secrecy rate even when Eve adopts the MU ML detection strategy. This confirms the robustness of our proposed temporal-AN scheme in highly-dense user deployments.

Fig 10 depicts the average secrecy sum-rate performance of the hybrid TAN-SK scheme versus the number of encrypted samples, $N_{\rm en} = N_{\rm en}^{(k)}\ \forall k$, for the cases of SU and MU ML detectors at Eve. As the number of encrypted samples increases, the gain of the perfectly secured term in (48) and (52) increases and the secrecy rate is boosted. To highlight the secrecy rate gains, the performance is compared with the temporal-AN-only scheme and the benchmark case with no secret keys generation or temporal AN. In Fig. 11, we show the average secrecy sum-rate of the hybrid TAN-SK scheme versus α. The figure quantifies the performance gains of the hybrid TAN-SK scheme and illustrates the gains introduced by the temporal-AN only and secret keys only schemes for $N_{\rm en} = 10$ encrypted data samples. The performance is compared with the benchmark case of no injected temporal-AN or secret keys generation.

Finally, Fig. 12 depicts the average secrecy sum-rate performance under multiple non-colluding eavesdroppers scenario. The figure quantifies the average secrecy rate performance when Eve applies SU ML or linear MMSE detectors while Bob is constrained to the per-sub-channel linear MMSE detector. We observe only a slight degradation in the average secrecy sum-rate for both the TAN-only scheme and the TAN-SK scheme as the number of Eves increases which verifies the robustness of the proposed schemes.

IX. CONCLUSIONS

We proposed a temporal-AN-aided scheme to secure SC-FDMA communications from eavesdropping. We analyzed the achieved data rates of the Alices-Bob links (legitimate links) and the Alices-Eve links (eavesdropping links) under low-complexity detectors at Bob and high-complexity detectors with global channel knowledge at Eve. In addition, we showed that, as Eve increases her SU detector complexity (from ZF to MMSE and to ML) to exploit the correlation properties of the temporal AN signal, she can reduce the AN effect on her data rate. As Eve adopts the high-complexity multi-user detection strategies, she can only introduce slight degradation in the achieved secrecy rate which validates the robustness of our proposed scheme. In addition, we investigated the performance of the temporal-AN scheme under different transmit power allocation fractions for the data and AN signals. Furthermore, we proved that the number of useful AN streams that can be injected to degrade Eve's SNR is equal to the maximum of the k-th Alice-Bob and the k-th Alice-Eve channel memories. We derived a closed-form expression for an approximation of the average secrecy rate at high input SNR levels. The derived expression showed that, in the worst-case secrecy scenario for the legitimate system when Eve uses the ML detector, the average secrecy rate is always positive and increases linearly with the number of useful AN streams. We showed that increasing the number of users increases the achievable secrecy rate due to the ability of those users to transmit AN signals that degrade Eve's receiver only. Moreover, for the case of partial Alices-Bob channel knowledge at Eve, we proposed a hybrid TAN-SK scheme to exploit Eve's unawareness of the Alices-Bob channel in enhancing the secrecy rate. Our proposed TAN-SK scheme guarantees a positive instantaneous secrecy rate even when Eve adopts the high-complexity (SU or MU) ML detector. Simulations results demonstrated that for the case of global channel knowledge at Eve, adopting the proposed temporal-AN injection scheme is critical to achieve higher secrecy rates compared to the benchmark case with no-AN injection. For the case of partial Alices-Bob channels knowledge at Eve, additional secrecy rate gains are achievable through our proposed TAN-SK scheme.

APPENDIX A
PROOF OF PROPOSITION 1

The k-th Alice superimposes the temporal-AN signal on the data signal after CP insertion. The composite (data + AN) signal is received at Bob after it passes through the time-domain $\mathrm{A}_k - \mathrm{B}$ channel matrix given by

$$\mathbf{R}^{\mathrm{cp}}\mathbf{H}_{\mathrm{t}}^{(k)} = \left[\mathbf{0}_{M\times(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)})}\ \mathbf{H'}^{(k)}_{M\times(M+L_{\mathrm{B}}^{(k)})}\right] \tag{55}$$

where $\mathbf{H'}^{(k)} \in \mathbb{C}^{M\times(M+L_{\mathrm{B}}^{(k)})}$ is the Toeplitz upper-triangular $\mathrm{A}_k - \mathrm{B}$ channel matrix after CP removal with $\left[h'^{(k)}(0), h'^{(k)}(1), \ldots, h'^{(k)}(L_{\mathrm{B}}^{(k)}), 0, \ldots, 0\right]$ as its first row.

The AN signal is precoded using a precoding matrix $\mathbf{Q}^{(k)}$ which is designed to ensure that the temporal AN is eliminated at Bob by spanning the null-space of $\mathbf{R}^{\mathrm{cp}}\mathbf{H}_{\mathrm{t}}^{(k)}$ as follows

$$\begin{aligned}\mathbf{Q}^{(k)} &= \mathrm{Null}\left(\mathbf{R}^{\mathrm{cp}}\mathbf{H}^{\mathrm{time}(k)}\right)\\ &= \mathrm{Null}\left(\left[\mathbf{0}_{M\times\left(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)}\right)}\ \mathbf{H'}^{(k)}_{M\times\left(M+L_{\mathrm{B}}^{(k)}\right)}\right]\right)\end{aligned} \tag{56}$$

We notice that $\mathbf{R}^{\mathrm{cp}}\mathbf{H}^{\mathrm{time}(k)}$ has $\left(M_{\mathrm{cp}} - L_{\mathrm{B}}^{(k)}\right)$ all-zero columns. Let $\mathbf{W} = \left[\mathbf{I}_{\left(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)}\right)}\ \mathbf{0}_{\left(M+L_{\mathrm{B}}^{(k)}\right)\times\left(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)}\right)}\right]^{\top}$ denote the orthonormal basis matrix that extracts the all-zero columns out of $\mathbf{R}^{\mathrm{cp}}\mathbf{H}^{\mathrm{time}(k)}$ as follows

$$\mathbf{R}^{\mathrm{cp}}\mathbf{H}^{\mathrm{time}(k)}\mathbf{W} = \mathbf{0}_{M\times\left(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)}\right)} \tag{57}$$

The null space precoder, $\mathbf{Q}^{(k)}$, can therefore be expressed as

$$\mathbf{Q}^{(k)} = \left[\mathbf{W}_{(M+M_{\mathrm{cp}})\times(M_{\mathrm{cp}}-L_{\mathrm{B}})}\ \mathbf{Q'}^{(k)}_{(M+M_{\mathrm{cp}})\times L_{\mathrm{B}}^{(k)}}\right] \tag{58}$$

where $\mathbf{Q'}^{(k)} = \mathrm{Null}\left(\mathbf{H'}^{(k)}\right)$ denotes the orthonormal basis matrix that spans the null space of $\mathbf{H'}^{(k)}$. At Eve, the k-th Alice AN signal vector interfering with the l-th Alice N data sub-channels is given by

$$\mathbf{i}_{N\times 1}^{(k)} = \mathbf{S}^{(l)^{\top}}\mathbf{F}_M\mathbf{R}^{\mathrm{cp}}\mathbf{G}_{\mathrm{t}}^{(j)}\mathbf{Q}^{(j)}\mathbf{z}_{\mathrm{t}}^{(k)} \tag{59}$$

The equivalent $\mathrm{A}_k - \mathrm{E}$ time-domain channel matrix after CP removal is similarly given by

$$\mathbf{R}^{\mathrm{cp}}\mathbf{G}^{\mathrm{time}(k)} = \left[\mathbf{0}_{M\times(M_{\mathrm{cp}}-L_{\mathrm{E}}^{(k)})}\ \mathbf{G'}^{(k)}_{M\times(M+L_{\mathrm{E}}^{(k)})}\right] \tag{60}$$

where $\mathbf{G'}^{(k)} \in \mathbb{C}^{M\times(M+L_{\mathrm{E}}^{(k)})}$ is the Toeplitz upper-triangular $\mathrm{A}_k - \mathrm{E}$ channel matrix. The AN vector across the data SC-FDMA sub-channels of Eve can therefore be expressed as

$$\begin{aligned}\mathbf{i}_{N\times 1}^{(k)} &= \mathbf{S}^{(l)^{\top}}\mathbf{F}_M\left[\mathbf{0}_{M\times(M_{\mathrm{cp}}-L_{\mathrm{E}}^{(k)})}\ \mathbf{G'}^{(k)}_{M\times(M+L_{\mathrm{E}}^{(k)})}\right]\\ &\quad\times\left[\mathbf{W}_{(M+M_{\mathrm{cp}})\times(M_{\mathrm{cp}}-L_{\mathrm{B}}^{(k)})}\ \mathbf{Q'}^{(k)}_{(M+M_{\mathrm{cp}})\times L_{\mathrm{B}}^{(k)}}\right]\times\mathbf{z}_{\mathrm{t}}^{(k)}{}_{M_{\mathrm{cp}}\times 1}\\ &= \left[\mathbf{0}_{N\times\left(M_{\mathrm{cp}}-L_{\mathrm{u}}^{(k)}\right)}\ \mathbf{U'}^{(k)}_{\mathrm{useful}\ \left(\mathrm{N}\times\mathrm{L}_{\mathrm{u}}^{(k)}\right)}\right]\times\mathbf{z}_{\mathrm{t}}^{(k)}{}_{M_{\mathrm{cp}}\times 1}\end{aligned} \tag{61}$$

where $L_{\mathrm{u}}^{(k)} = \max\left(L_{\mathrm{B}}^{(k)}, L_{\mathrm{E}}^{(k)}\right)$ and $\mathbf{U'}^{(k)}_{\mathrm{useful}}$ is given by $\mathbf{U'}^{(k)}_{\mathrm{useful}} = \mathbf{S}^{(l)^{\top}}\mathbf{F}_M\left[\mathbf{0}_{\left(\mathrm{M}\times(\mathrm{M}_{\mathrm{cp}}-\mathrm{L}_{\mathrm{E}}^{(k)})\right)}\ \mathbf{G'}^{(k)}_{M\times(M+L_{\mathrm{E}}^{(k)})}\right]\times\left[\mathbf{W}_{(M+M_{\mathrm{cp}})\times\left(L_{\mathrm{u}}^{(k)}-L_{\mathrm{B}}^{(k)}\right)}\ \mathbf{Q'}^{(k)}_{(M+M_{\mathrm{cp}})\times L_{\mathrm{B}}^{(k)}}\right]$. From Eqn. (61), we notice that the first $\left(M_{\mathrm{cp}} - L_{\mathrm{u}}^{(k)}\right)$ AN streams of $\mathbf{z}_{\mathrm{t}}^{(k)}{}_{M_{\mathrm{cp}}\times 1}$ are projected into all-zero columns. In other words, those AN streams lie in the null space of the $\mathrm{A}_k - \mathrm{E}$ channel and cause no harm to Eve. The matrix $\left(\mathbf{R}^{\mathrm{cp}}\mathbf{G}_{\mathrm{t}}^{(k)}\mathbf{Q}^{(k)}\right)$ has a rank of $L_{\mathrm{u}}^{(k)}$. Therefore, there are only $L_{\mathrm{u}}^{(k)}$ *useful* AN directions in the sense that they can degrade Eve's SINR.

We conclude that the number of useful AN streams depends on the maximum of the $\mathrm{A}_k - \mathrm{B}$ and $\mathrm{A}_k - \mathrm{E}$ channels memories. As $L_{\mathrm{B}}^{(k)}$ increases, the number of orthonormal basis vectors of the $\mathrm{A}_k - \mathrm{B}$ channel matrix null space increases which, in turn, increases the number of AN streams. As $L_{\mathrm{E}}^{(k)}$ increases, the $\mathrm{A}_k - \mathrm{E}$ channel spreads each AN stream across more of its data sub-channels.

APPENDIX B
PROOF OF PROPOSITION 2

Assuming ML detection, the instantaneous rate expression of the $\mathrm{A}_k - \mathrm{E}$ link is given by

$$R_{\mathrm{E}}^{(k)} = \log_2 \det \left(\mathbf{I}_N + p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \times \left(\kappa_{\mathrm{E}} \mathbf{I}_N + \left(\sum_{j=1}^{K} \mathbf{S}^{(k)\top} \mathbf{O}^{(j)} \Sigma_{\mathrm{z}}^{(j)} \mathbf{O}^{(j)*} \mathbf{S}^{(k)} \right) \right)^{-1} \right) \tag{62}$$

By dividing the data power equally across the N data samples, each sample will have a power of $p_{\mathrm{x}}^{(k)} = \frac{\alpha^{(k)} p_{\mathrm{t}}}{N}$. Similarly, by performing equal power allocation across the $L_{\mathrm{u}}^{(k)}$ AN samples, each sample will have a power of $p_{\mathrm{z}}^{(j)} = (1-\alpha^{(j)}) \frac{p_{\mathrm{t}}}{L_{\mathrm{u}}^{(j)}}$.

$$R_{\mathrm{E}}^{(k)} = \log_2 \det \left(\mathbf{I}_N + \alpha^{(k)} \frac{p_{\mathrm{t}}}{N} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \times \left(\kappa_{\mathrm{E}} \mathbf{I}_N + \left(\sum_{j=1}^{K} (1-\alpha^{(j)}) \frac{p_{\mathrm{t}}}{L_{\mathrm{u}}^{(j)}} \mathbf{S}^{(k)\top} \mathbf{O}^{(j)} \mathbf{O}^{(j)*} \mathbf{S}^{(k)} \right) \right)^{-1} \right) \tag{63}$$

Since the matrix $\left(\mathbf{S}^{(k)\top} \mathbf{O}^{(j)} \mathbf{O}^{(j)*} \mathbf{S}^{(k)} \right)$ is positive semi-definite, the term $\left(\sum_{j=1}^{K} p_{\mathrm{z}}^{(j)} \mathbf{S}^{(k)\top} \mathbf{O}^{(j)} \mathbf{O}^{(j)*} \mathbf{S}^{(k)} \right)$ can be factored as $\left(\sum_{j=1}^{K} p_{\mathrm{z}}^{(j)} \mathbf{S}^{(k)\top} \mathbf{O}^{(j)} \mathbf{O}^{(j)*} \mathbf{S}^{(k)} \right) = \tilde{\mathbf{Q}} \tilde{\mathbf{Q}}^*$ where $\tilde{\mathbf{Q}}$ in an $N \times N$ matrix which represents the combined AN term at Eve. By performing the SVD on $\tilde{\mathbf{Q}}$, we get, $\tilde{\mathbf{Q}} = \mathbf{U}_{\mathrm{z}} \Lambda_{\mathrm{z}} \mathbf{V}_{\mathrm{z}}^*$, where Λ_{z} is an $N \times N$ diagonal matrix with at least $L_{\mathrm{u}}^{\max} = \max_k \{L_{\mathrm{u}}^{(k)}\}$ non-zero singular values. The instantaneous data rate of the $\mathrm{A}_k - \mathrm{E}$ link is given by

$$\begin{aligned} R_{\mathrm{E}}^{(k)} &= \log_2 \det \Big(\mathbf{I}_N + p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \\ &\quad \times \left(\kappa_{\mathrm{E}} \mathbf{I}_N + \mathbf{U}_{\mathrm{z}} \Lambda_{\mathrm{z}} \Lambda_{\mathrm{z}}^* \mathbf{U}_{\mathrm{z}}^* \right)^{-1} \Big) \\ &= \log_2 \det \Big(\mathbf{I}_N + p_{\mathrm{x}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \\ &\quad \times \mathbf{U}_{\mathrm{z}} \left(\kappa_{\mathrm{E}} \mathbf{I}_N + \Lambda_{\mathrm{z}} \Lambda_{\mathrm{z}}^* \right)^{-1} \mathbf{U}_{\mathrm{z}}^* \Big) \\ &= \log_2 \det \Big(\mathbf{I}_N + p_{\mathrm{x}}^{(k)} \mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}} \\ &\quad \times \left(\kappa_{\mathrm{E}} \mathbf{I}_N + \Lambda_{\mathrm{z}} \Lambda_{\mathrm{z}}^* \right)^{-1} \Big) \end{aligned} \tag{64}$$

The last equality holds due to Sylvester's identity. Notice that the diagonal matrix $\Lambda_{\mathrm{z}} \Lambda_{\mathrm{z}}^*$ represents the AN power at Eve. Define the AN-plus-AWGN covariance matrix, denoted by $\mathbf{V} = (\kappa_{\mathrm{E}} \mathbf{I}_N + \Lambda_{\mathrm{z}} \Lambda_{\mathrm{z}}^*)$, then the k-th Alice-Eve's instantaneous data rate is given by

$$\begin{aligned} R_{\mathrm{E}}^{(k)} &= \log_2 \det \left(\mathbf{I}_N + p_{\mathrm{x}}^{(k)} \mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}} \mathbf{V}^{-1} \right) \\ &= \log_2 \det \left(\mathbf{V} + p_{\mathrm{x}}^{(k)} \mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}} \right) - \log_2 \det (\mathbf{V}) \end{aligned} \tag{65}$$

The matrix $\mathbf{V} + p_{\mathrm{x}}^{(k)} \mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}}$ is Hermitian, hence, we can apply the Hadamard inequality to derive an upper bound on the data rate of the Alice-Eve link as follows

$$R_{\mathrm{E}}^{(k)} \le \sum_{i=1}^{N} \log_2 \left([\mathbf{V}]_{i,i} + p_{\mathrm{x}}^{(k)} [\mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}}]_{i,i} \right) - \log_2 \det (\mathbf{V}) \tag{66}$$

Defining the i-th row of $\mathbf{U}_{\mathrm{z}}^*$ as $\mathbf{u}_i = [u_{i,1}, u_{i,2}, \cdots, u_{i,N}]$, the i-th diagonal element of $\left(\mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}} \right)$ is thus given by $[\mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}}]_{i,i} = \sum_{j=1}^{N} |u_{i,j}|^2 |G_j^{(k)}|^2$ with $G_j^{(k)}$ denoting the j-th frequency-domain channel coefficient of the k-th Alice-Eve link. Applying Jensen's inequality to the concave function $\sum_{i=1}^{N} \log_2 \left([\mathbf{V}]_{i,i} + p_{\mathrm{x}}^{(k)} [\mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}}]_{i,i} \right)$, the achieved average rate of the k-th Alice-Eve link can be upper-bounded as follows

$$\begin{aligned} \mathbb{E}\{R_{\mathrm{E}}^{(k)}\} &\le \sum_{i=1}^{N} \mathbb{E} \Big\{ \log_2 \Big([\mathbf{V}]_{i,i} + p_{\mathrm{x}}^{(k)} \\ &\quad \times \mathbb{E}_{\mathrm{G_j}^{(\mathrm{k})}} \left\{ [\mathbf{U}_{\mathrm{z}}^* \mathbf{G}_{\mathrm{f}}^{(k)} \mathbf{G}_{\mathrm{f}}^{(k)*} \mathbf{U}_{\mathrm{z}}]_{i,i} \right\} \Big) \Big\} \\ &\quad - \mathbb{E} \left\{ \log_2 \det (\mathbf{V}) \right\} \\ &= \sum_{i=1}^{N} \mathbb{E} \Big\{ \log_2 \det \Big([\mathbf{V}]_{i,i} + p_{\mathrm{x}}^{(k)} \\ &\quad \times \mathbb{E}_{\mathrm{G_j}^{(\mathrm{k})}} \Big\{ \sum_{j=1}^{N} |u_{i,j}|^2 |G_j^{(k)}|^2 \Big\} \Big) \Big\} \\ &\quad - \mathbb{E} \left\{ \log_2 \det (\mathbf{V}) \right\} \end{aligned} \tag{67}$$

where we averaged only over the channel $G_j^{(k)}$ (and not over the other random variables) to obtain a tight bound. In other words, the outside expectation is over all random variables except $G_j^{(k)}$. Due to the channel independence from one link to another, the random variable $|G_j^{(k)}|^2$ is independent from $|u_{i,1}|^2$. Hence, we have

$$\begin{aligned} \mathbb{E}_{\mathrm{G_j}^{(\mathrm{k})}} \Big\{ \sum_{j=1}^{N} |u_{i,j}|^2 |\mathrm{G_j}^{(k)}|^2 \Big\} &= \Big\{ \sum_{j=1}^{N} |u_{i,j}|^2 \mathbb{E}_{\mathrm{G_j}^{(\mathrm{k})}} \{ |G_j^{(k)}|^2 \} \Big\} \\ &= \Big\{ \sum_{j=1}^{N} |u_{i,j}|^2 {\sigma_{\mathrm{A-E}}^{(k)}}^2 \left(L_{\mathrm{E}}^{(k)} + 1 \right) \Big\} \end{aligned} \tag{68}$$

where $\mathbb{E}_{G_j^{(k)}}\{|G_j^{(k)}|^2\} = \mathbb{E}\{\sum_{i=1}^{L_{\mathrm{E}}^{(k)}} |g(i)|^2\} = {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1)$ with $g(i)$ denoting the i-th tap of the Alice-Eve link CIR. Accordingly,

$$\mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \leq \sum_{i=1}^{N} \mathbb{E}\left\{\log_2\left([\mathbf{V}]_{i,i} + p_{\mathrm{x}}^{(k)} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1) \times \sum_{j=1}^{N} |u_{i,j}|^2\right)\right\} - \mathbb{E}\left\{\log_2 \det(\mathbf{V})\right\} \tag{69}$$

Let σ_i^2 denote the i-th diagonal entry of the diagonal matrix $\mathbf{V}$. Considering the worst-case scenario where $\tilde{\mathbf{Q}}$ has only $L_{\mathrm{u}}^{\max}$ non-zero singular values, the i-th diagonal entry is given by

$$\sigma_i^2 = [\mathbf{V}]_{i,i} = \begin{cases} \kappa_{\mathrm{E}} + \delta_{z,i}^2, & i \leq L_{\mathrm{u}}^{\max} \\ \kappa_{\mathrm{E}}, & \text{otherwise} \end{cases} \tag{70}$$

where $\delta_{z,i}$ denotes the i-th diagonal entry of Λ_{z} and $\delta_{z,i}^2$ represents the AN power at Eve which can be expressed as a fraction of the total transmit power. Hence, $\delta_{z,i}^2 = \beta_i\, K\, p_t$ where $0 \leq \beta_i \leq 1, \forall i$. On the other hand, $\det(\mathbf{V}) = \prod_{i=1}^{N} [\mathbf{V}]_{i,i} = \prod_{i=1}^{N} \sigma_i^2$. Since $\mathbf{U}_z$ is unitary, $\sum_{j=1}^{N} |u_{i,j}|^2 = \sum_{i=1}^{N} |u_{i,j}|^2 = 1$. Hence,

$$\mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \leq \sum_{i=1}^{N} \mathbb{E}\left\{\log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1)}{\sigma_i^2}\right)\right\} \tag{71}$$

The average secrecy rate is thus lower bounded by

$$\begin{aligned} &\mathbb{E}\{R_{\mathrm{B}}^{(k)}\} - \mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \\ &\quad \geq \sum_{i=1}^{N} \mathbb{E}\left\{\log_2\left(1 + \frac{|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2\, p_{\mathrm{x}}^{(k)}}{\kappa_{\mathrm{B}}}\right)\right\} \\ &\qquad - \sum_{i=1}^{N} \mathbb{E}\left\{\log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1)}{\sigma_i^2}\right)\right\} \end{aligned} \tag{72}$$

Splitting each summation into two sums from 1 to $L_{\mathrm{u}}^{\max}$ and from $L_{\mathrm{u}}^{\max} + 1$ to N, we get

$$\begin{aligned} &\mathbb{E}\{R_{\mathrm{B}}^{(k)}\} - \mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \\ &\quad \geq \mathbb{E}\left\{\sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(1 + \frac{|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2\, p_{\mathrm{x}}^{(k)}}{\kappa_{\mathrm{B}}}\right)\right. \\ &\qquad + \sum_{i=L_{\mathrm{u}}^{\max}+1}^{N} \log_2\left(1 + \frac{|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2\, p_{\mathrm{x}}^{(k)}}{\kappa_{\mathrm{B}}}\right) \\ &\qquad - \sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1)}{\sigma_i^2}\right) \\ &\qquad \left. - \sum_{i=L_{\mathrm{u}}^{\max}+1}^{N} \log_2\left(1 + \frac{p_{\mathrm{x}}^{(k)} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)} + 1)}{\sigma_i^2}\right)\right\} \end{aligned} \tag{73}$$

At very high input SNR levels $\sigma_i^2 \approx \delta_{z,i}^2\ \forall i \leq L_{\mathrm{u}}^{\max}$, the average secrecy rate is thus given by

$$\begin{aligned} &\mathbb{E}\{R_{\mathrm{B}}^{(k)}\} - \mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \\ &\quad \geq \mathbb{E}\left\{\sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(\frac{\alpha^{(k)} p_t |\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{N\kappa_{\mathrm{B}}}\right)\right. \\ &\qquad + \sum_{i=L_{\mathrm{u}}^{\max}+1}^{N} \log_2\left(\frac{\alpha^{(k)} p_t |\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{N\kappa_{\mathrm{B}}}\right) \\ &\qquad - \sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(1 + \frac{\alpha^{(k)} \frac{p_t}{N} \sigma_{\mathrm{A-E}}^2 (L_{\mathrm{E}} + 1)}{\beta_i\, K\, p_t}\right) \\ &\qquad \left. - \sum_{i=L_{\mathrm{u}}^{\max}+1}^{N} \log_2\left(\frac{\alpha^{(k)} p_t \sigma_{\mathrm{A-E}}^2 (L_{\mathrm{E}} + 1)}{N\kappa_{\mathrm{E}}}\right)\right\} \end{aligned} \tag{74}$$

Using the logarithmic function properties, we get

$$\begin{aligned} &\mathbb{E}\{R_{\mathrm{B}}^{(k)}\} - \mathbb{E}\{R_{\mathrm{E}}^{(k)}\} \\ &\quad \geq \mathbb{E}\left\{\sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(\frac{p_t}{N\kappa_{\mathrm{B}}}\right)\right. \\ &\qquad + \sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2\right) \\ &\qquad + \sum_{i=L_{\mathrm{u}}^{\max}+1}^{N} \log_2\left(\frac{\frac{|\mathbf{H}_{\mathrm{f}}^{(k)}{}_{i,i}|^2}{\kappa_{\mathrm{B}}}}{\frac{{\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)}+1)}{\kappa_{\mathrm{E}}}}\right) \\ &\qquad \left. - \sum_{i=1}^{L_{\mathrm{u}}^{\max}} \log_2\left(\frac{1 + \frac{\frac{\alpha^{(k)}}{N} {\sigma^{(k)}_{\mathrm{A-E}}}^{2} (L_{\mathrm{E}}^{(k)}+1)}{\beta_i\, K}}{\alpha^{(k)}}\right)\right\} \end{aligned} \tag{75}$$

where $\frac{p_t}{N\kappa_{\mathrm{B}}}$ is the input SNR level per data sample, which is assumed to be very high. Since the first term in (75) is very large and monotonically increasing with p_t and all the other terms are very small, we can further ignore all terms except the first term. Therefore, the lower bound on the average secrecy rate (in bits/sec/Hz) is given by

$$\frac{1}{M + M_{\mathrm{cp}}}\, \mathbb{E}\left\{\left[R_{\mathrm{B}}^{(k)} - R_{\mathrm{E}}^{(k)}\right]^{+}\right\} \gtrapprox \frac{L_{\mathrm{u}}^{\max}}{M + M_{\mathrm{cp}}} \log_2\left(\frac{p_{\mathrm{t}}}{N\kappa_{\mathrm{B}}}\right) \tag{76}$$

APPENDIX C
WIRETAP CODING

Let k-th Alice transmit a source message $W^{(k)}$ in $n^{(k)}$ channel uses. The k-th Alice first generates all sequences in the message set $\mathcal{W}^{(k)} \in \{1, 2, \ldots, 2^{n^{(k)}\mathcal{R}_{\mathrm{s}}^{(k)}}\}$, having length $n^{(k)}\mathcal{R}_{\mathrm{B}}^{(k)}$ where $\mathcal{R}_{\mathrm{B}}^{(k)} = \mathbb{E}\{R_{\mathrm{B}}^{(k)}\} - \epsilon$ and $\mathcal{R}_{\mathrm{s}}^{(k)} = \mathbb{E}\{R_{\mathrm{s}}^{(k)}\} - \epsilon$, for some small ϵ. k-th Alice then divides these sequences randomly and uniformly into $2^{n^{(k)}\mathcal{R}_{\mathrm{s}}^{(k)}}$ bins. This guarantees that any of the sequences is equally probable to be inside any of the bins. Each secret message, $w^{(k)} \in \mathcal{W}^{(k)}$, is then assigned a bin $V^{(k)}(w^{(k)})$. Let m denotes the number of coherence intervals used to transmit $W^{(k)}$. To encode a particular message, the stochastic encoder at k-th Alice, randomly selects a sequence $v^{(k)}$ from the corresponding bin $V(w^{(k)})$, according to a uniform distribution. The sequence, $v^{(k)}$ consisting of $n^{(k)}\mathcal{R}^{(k)}$ bits is then subdivided into m dependent blocks $v^{(k)}(1), \ldots v^{(k)}(m)$, where the block $v^{(k)}(i)$ is transmitted in the i-th coherence interval. For arbitrarily large m, we have

$$\lim_{m\to\infty} \sum_{i=1}^{n/m} R_{\mathrm{B}}^{(k)}(i) = \frac{n}{m}\mathbb{E}\left\{R_{\mathrm{B}}^{(k)}\right\} \tag{77}$$

where $R_{\mathrm{B}}^{(k)}(i)$ is the k-th Alice-Bob link rate at the i-th coherence interval. After that, k-th Alice generates m i.i.d. Gaussian codebooks, each having a length of $\frac{n}{m}$ symbols and is comprised of $2^{\frac{n}{m}\left(R_{\mathrm{B}}^{(k)}(i)-\epsilon\right)}$ codewords. In the i-th coherence interval, the k-th Alice encodes the sub-block $v^{(k)}(i)$, and transmits it over the wireless fading channel. Hence, even with the lack of the eavesdropper's instantaneous channel, the k-th Alice-Bob achievable link rate becomes the average secrecy rate [30], [34].

ACKNOWLEDGMENT

This paper was presented in part at the IEEE ICC 2018 [1].

REFERENCES

[1] M. Marzban, A. El Shafie, R. Chabaan, and N. Al-Dhahir, "Securing SC-FDE uplink transmissions using temporal artificial noise under three detection strategies," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 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] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[5] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.

[6] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[7] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[8] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[9] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *Proc. Commun. Netw. Services Res. Conf. (CNSR)*, 2008, pp. 88–95.

[10] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[12] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.

[13] B. T. Quist and M. A. Jensen, "Bound on the key establishment rate for multi-antenna reciprocal electromagnetic channels," *IEEE Trans. Antennas Propag.*, vol. 62, no. 3, pp. 1378–1385, Mar. 2014.

[14] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar./Apr. 2008, pp. 3013–3016.

[15] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154–162, Jan. 2016.

[16] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[17] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[18] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[19] A. E. Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[20] M. Marzban, A. El Shafie, R. Chabaan, and N. Al-Dhahir, "Securing OFDM-based wireless links using temporal artificial-noise injection," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–6.

[21] A. El Shafie, M. Marzban, R. Chabaan, and N. Al-Dhahir, "A hybrid artificial-noise and secret-key scheme for securing OFDM transmissions in V2G networks," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–6.

[22] F. Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[23] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation*, document 3GPP TS 36.211 V14.2.0, 2017.

[24] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, Dec. 2017.

[25] Y. Miao, W. Li, D. Tian, M. S. Hossain, and M. F. Alhamid, "Narrowband Internet of Things: Simulation and modeling," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2304–2314, Aug. 2017.

[26] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 28–33, Mar. 2017.

[27] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1505–1515, Jun. 2017.

[28] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband Internet of Things: Evolutions, technologies, and open issues," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1449–1462, Jun. 2017.

[29] F. Pancaldi, G. M. Vitetta, R. Kalbasi, N. Al-Dhahir, M. Uysal, and H. Mheidat, "Single-carrier frequency domain equalization," *IEEE Signal Process. Mag.*, vol. 25, no. 5, pp. 37–56, Sep. 2008.

[30] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[31] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[32] A. D. Harper and X. Ma, "MIMO wireless secure communication using data-carrying artificial noise," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8051–8062, Dec. 2016.

[33] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[34] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

MOHAMED F. MARZBAN received the B.Sc. and M.Sc. degrees in electrical engineering from Cairo University, Egypt, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with The University of Texas at Dallas, Richardson, TX, USA. From 2013 to 2014, he was a Systems Research and Development Engineer with Intel Labs, Cairo, Egypt. From 2015 to 2016, he was a Software Engineer with Avidbeam Inc., Cairo. In 2018, he joined Qualcomm Technologies., Santa Clara, CA, USA, as a Cellular-Vehicle-to-Everything (C-V2X) Systems Design Intern. His research interests include physical-layer security, C-V2X communications, advanced driver assistance systems, and machine learning applications.

AHMED EL SHAFIE received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, the M.Sc. degree in communication and information technology from Nile University, Cairo, Egypt, in 2014, and the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2018. Since 2018, he has been a Senior Systems Engineer with Qualcomm Technologies, San Diego, CA, USA. He is an IEEE Senior Member. He was a recipient of the David Daniel Best Doctoral Thesis Award, in 2018, the Jonsson School Industrial Advisory Council Fellowship Award, in 2017, the IEEE Transactions on Communications Exemplary Reviewer, in 2015, 2016, and 2017, and the IEEE Communications Letters Exemplary Reviewer, in 2016. He is nominated for the 2018 CGS/ProQuest Distinguished Dissertation Award. He currently serves as an Editor for IEEE COMMUNICATIONS LETTERS, *Physical Communications*, and the *Transactions on Emerging Technologies in Telecommunications*. In addition, he serves as a Guest Editor for the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

NAOFAL AL-DHAHIR received the Ph.D. degree in electrical engineering from Stanford University. From 1994 to 2003, he was a Principal Member of the Technical Staff with the GE Research and AT&T Shannon Laboratory. He is currently the Erik Jonsson Distinguished Professor with The University of Texas at Dallas. He has co-authored over 400 papers. He is the Co-Inventor of 41 issued U.S. patents. He was a co-recipient of four IEEE best paper awards. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS.

RIDHA HAMILA received the M.Sc. degree, the Licentiate of Technology degree (Hons.), and the Doctor of Technology degree from the Department of Information Technology, Tampere University of Technology (TUT), Tampere, Finland, in 1996, 1999, and 2002, respectively. From 1994 to 2002, he held various research and teaching positions with the Department of Information Technology, TUT. From 2002 to 2003, he was a System Specialist with the Nokia Research Center and Nokia Networks, Helsinki. From 2004 to 2009, he was with the Etisalat University College, Emirates Telecommunications Corporation, UAE. He was a Supervisor of a large number of under/graduate students and Postdoctoral Fellows. He is currently an Associate Professor with the Department of Electrical Engineering, Qatar University, Qatar. He is also an Adjunct Professor with the Department of Communications Engineering, TUT. He has been involved in several past and current industrial projects Qtel, QNRF, Finnish Academy projects, TEKES, Nokia, and EU research and education programs. His current research interests include mobile and broadband wireless communication systems, cellular and satellites-based positioning technologies, and synchronization and DSP algorithms for flexible radio transceivers.