A Secure Affine Frequency Division Multiplexing for Wireless Communication Systems

Ping Wang, Zulin Wang, Yuanfang Ma, Xiaosi Tian and Yuanhan Ni*
School of Electronic and Information Engineering, Beihang University, Beijing, 100191, China
Email:wangping_119@buaa.edu.cn, wzulin@buaa.edu.cn, yuanfangma@buaa.edu.cn,
xiaosi_tian@buaa.edu.cn, yuanhanni@buaa.edu.cn

***Abstract*—This paper introduces a secure affine frequency division multiplexing (SE-AFDM) for wireless communication systems to enhance communication security. Besides configuring the parameter c_1 to obtain communication reliability under doubly selective channels, we also utilize the time-varying parameter c_2 to improve the security of the communications system. The derived input-output relation shows that the legitimate receiver can eliminate the nonlinear impact introduced by the time-varying c_2 without losing the bit error rate (BER) performance. Moreover, it is theoretically proved that the eavesdropper cannot separate the time-varying c_2 and random information symbols, such that the BER performance of the eavesdropper is severely deteriorated. Meanwhile, the analysis of the effective signal-to-interference-plus-noise ratio (SINR) of the eavesdropper illustrates that the SINR decreases as the value range of c_2 expands. Numerical results verify that the proposed SE-AFDM waveform has significant security while maintaining good BER performance in high-mobility scenarios.**

I. Introduction

Sixth-generation (6G) wireless communication networks are expected to provide plentiful usage scenarios, enabling advanced capabilities such as wide area coverage, low latency of 0.1 ms, peak throughput of 1 Tb/s, etc. With ubiquitous connectivity, extended coverage and increased terminals expose more sensitive information to eavesdropping risks in open wireless communication environments. Furthermore, low latency and high peak throughput in Hyper Reliable and Low-Latency Communications (HRLLC) constrain the application of security strategies with high latency and high complexity [1]. Therefore, the security of 6G has attracted extensive research.

The well-known strategy for wireless communication security is to implement encryption in the network or application layer, which has been widely used in the military, medicine, and other fields. However, key distribution is a challenging task in decentralized and heterogeneous networks, and the high computational complexity of encryption and decryption may lead to extra latency and limited throughput [2]. Thus, it is an open question for implementing encryption to meet the requirements of low latency and peak throughput in 6G, especially in networks with limited computational capabilities and constrained terminal sizes [3].

Besides the network layer and application layer, the physical layer (PHY) can provide wireless communication security, i.e., physical layer security (PLS) [4]. With higher scalability and lower complexity, PLS techniques have caught significant research attention. Due to the advantage of not requiring additional power, ingeniously designed secure waveforms have been widely studied to strengthen PLS security. In the Global Positioning System (GPS), a spread spectrum-based secure waveform based on long-period Pseudo-noise (LPPN) sequences can ensure satellite communication security. The fact of ensuring security is eavesdroppers are unable to synchronize with the LPPN sequence, while the legitimate receiver can [5]. However, the spectrum efficiency of the spread spectrum-based waveform may be decreased. Since orthogonal frequency division multiplexing (OFDM) can achieve high spectrum efficiency, an OFDM-based secure waveform is presented to enhance wireless security by modifying the subcarrier spacing for each information symbol, namely improved spectrum efficient frequency division multiplexing (SEFDM) [6]. However, the bit error rate (BER) performance of the OFDM-based waveform deteriorates in doubly selective channels [7].

Due to the advantage of orthogonal time frequency space (OTFS) in obtaining full diversity over doubly selective channels [8], various OTFS-base secure waveforms have been researched [9], [10]. Specifically, by spreading the information symbols in either the delay or Doppler domain, a secure OTFS-based waveform, namely DS-OTFS, is formed to improve communication security at the expense of diminished spectrum efficiency [9]. Moreover, by rotating information symbols in the delay-Doppler domain based on the legitimate channel, R-OTFS is proposed to achieve secure communication by leveraging the channel diversity to reduce the signal-to-interference-plus-noise ratio (SINR) for the eavesdropper [10]. However, in R-OTFS, the strong correlation between the legitimate and the eavesdropping channels may undermine the security of the communication system. Furthermore, due to the excessive pilot overhead caused by the two-dimensional (2D) structure of OTFS, OTFS-based secure waveforms improve communication security at the cost of reduced spectrum efficiency.

Affine frequency division multiplexing (AFDM) with one-dimensional (1D) pilots is proposed, which can achieve higher spectrum efficiency and the same BER performance compared to OTFS [11]. By adjusting two discrete affine Fourier transform (DAFT) parameters, i.e., c_1 and c_2, AFDM can be fully compatible with OFDM, making AFDM regarded as one of the candidate waveforms for 6G [12]. AFDM-

* Corresponding author.

ICC 2025 - IEEE International Conference on Communications | 979-8-3315-0521-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICC52391.2025.11161021

based researches mainly focus on improving the reliability of communications by tuning c_1, such as channel estimation [13], equalization [14], integrated sensing and communications [15], etc. Recently, the parameter c_2 of AFDM is adjusted to reduce peak-to-average power ratio (PAPR) [7] or improve spectrum efficiency [16]. However, the security of AFDM waveforms is insufficient to meet the demands of 6G.

In this paper, we propose a secure affine frequency division multiplexing (SE-AFDM) with time-varying c_2 to enhance security while maintaining the reliability of communications systems. In SE-AFDM system, the time-varying c_2 is generated from a codebook with a value range according to an index controlled by a LPPN sequence. The LPPN sequence can be reconstructed by the legitimate receiver to synchronize the time-varying c_2, while the eavesdropper cannot generate synchronized c_2 due to the unknown of the LPPN sequence. The theoretical derivation confirms that the impact of the time-varying c_2 can be eliminated at the legitimate receiver with the synchronized c_2, but the eavesdropper cannot separate the time-varying c_2 and random information symbols. Furthermore, the analysis of the effective SINR of the eavesdropper reveals that expanding the value range of c_2 can decrease the effective SINR of the eavesdropper. The simulation results demonstrate the BER performance of the eavesdropper approaches 0.5 with an appropriately designed value range of c_2, while the legitimate receiver achieves the same BER performance and spectrum efficiency compared to the existing AFDM system.

II. Preliminaries

A. Basic Concepts of AFDM

Firstly, the basic concepts of AFDM proposed in [11] are briefly reviewed. We use $\mathbf{x}$ to denote an $N\times 1$ vector of quadrature amplitude modulation (QAM) symbols. The N points inverse discrete affine Fourier transform (IDAFT) is performed to map $\mathbf{x}$ from the affine Fourier transform (AFT) domain to the time domain, i.e., [11]

$$s\left[n\right]=\frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}x\left[m\right]e^{j2\pi\left(c_1n^2+\frac{mn}{N}+c_2m^2\right)}, \tag{1}$$

where c_1 and c_2 are the AFDM parameters, and $n=0,\ldots,N-1$. Then, a chirp-periodic prefix (CPP) with a length of N_{cp} is added, which is defined as [11]

$$s\left[n\right]=s\left[n+N\right]e^{-i2\pi c_1\left(N^2+2Nn\right)}, n=-N_{cp},\ldots,-1. \tag{2}$$

Then, AFDM signal is transmitted over a communication channel with P paths, in which the gain coefficient, time delay and Doppler shift of the i-th path are denoted by h_i, τ_i, $f_{d,i}$, respectively. The received signal vector in the time domain is given by [17, Eq. (6)]

$$r\left[n\right]=\sum_{i=1}^{P}\tilde{h}_i s\left[n-l_i\right]e^{j2\pi f_i n}+w_t\left[n\right], \tag{3}$$

where $\mathbf{w}_t\sim\mathcal{CN}\left(0,\sigma_c^2\mathbf{I}\right)$ is an additive Gaussian noise vector, $\tilde{h}_i=h_ie^{-j2\pi f_{d,i}\tau_i}$, $l_i=\tau_i/t_s$, $f_i=f_{d,i}t_s$ with t_s denoting the sampling interval, and $n\in[-N_{cp},N-1]$.

After discarding CPP and performing N points discrete affine Fourier transform (DAFT), the resulted signal in the AFT domain can be written as [11]

$$\mathbf{y}=\mathbf{H}_{\text{eff}}\mathbf{x}+\mathbf{w}_a=\sum_{i=1}^{P}\tilde{h}_i\mathbf{H}_{A,i}\mathbf{x}+\mathbf{w}_a, \tag{4}$$

where $\mathbf{H}_{\text{eff}}=\mathbf{A}\mathbf{H}_{c,t}\mathbf{A}^H$ with $\mathbf{H}_{c,t}=\sum_{i=1}^{P}\tilde{h}_i\mathbf{\Gamma}_i\mathbf{\Delta}_{f_i}\mathbf{\Pi}^{(l_i)}$ being the communication channel matrix in the time domain, $\mathbf{\Pi}$ is the forward cyclic-shift matrix, $\mathbf{\Gamma}_i=\text{diag}\left(\begin{cases}e^{-i2\pi c_1\left(N^2-2N(l_i-n)\right)}, & n<l_i,\\ 1, & n\geq l_i.\end{cases}\right)$, $\mathbf{\Delta}_{f_i}=\text{diag}\left(e^{i2\pi f_i n}, n\in[0,N-1]\right)$, $\mathbf{H}_{A,i}=\mathbf{A}\mathbf{\Gamma}_i\mathbf{\Delta}_{f_i}\mathbf{\Pi}^{(l_i)}\mathbf{A}^H$, $\mathbf{A}=\mathbf{\Lambda}_{c_2}\mathbf{F}\mathbf{\Lambda}_{c_1}$, $\mathbf{F}$ is the discrete Fourier transform (DFT) matrix, $\mathbf{\Lambda}_{c_i}=\text{diag}\left(e^{-j2\pi c_i n^2}, n=0,\ldots,N-1, i=1,2\right)$, and $\mathbf{w}_a=\mathbf{A}\mathbf{w}_t$. $H_{A,i}\left[p,q\right]$ is given by [11]

$$H_{A,i}\left[p,q\right]=\frac{1}{N}e^{j\frac{2\pi}{N}\left(Nc_1l_i^2-ql_i+Nc_2\left(q^2-p^2\right)\right)}\mathcal{F}_i\left[p,q\right], \tag{5}$$

where $\mathcal{F}_i\left[p,q\right]=\frac{e^{-j2\pi\left(p-q-\nu_i+2Nc_1l_i\right)}-1}{e^{-j\frac{2\pi}{N}\left(p-q-\nu_i+2Nc_1l_i\right)}-1}$ with $\nu_i=Nf_i=\frac{f_{d,i}}{\Delta f}=\alpha_i+a_i\in[-\nu_{\max},\nu_{\max}]$ being the Doppler shift normalized with respect to the subcarrier spacing Δf, and $\alpha_i\in[-\alpha_{\max},\alpha_{\max}]$ and $a_i\in\left(-\frac{1}{2},\frac{1}{2}\right]$ represent the integral and fractional part of ν_i, respectively. p and $q\in[0,N-1]$,

For the integral normalized Doppler shift case, i.e., $a_i=0$, there is only one non-zero element in each row of $\mathbf{H}_{A,i}$, i.e.,

$$H_{A,i}\left[p,q\right]=\begin{cases}e^{j\frac{2\pi}{N}\left(Nc_1l_i^2-ql_i+Nc_2\left(q^2-p^2\right)\right)}, & q=\langle p+loc_i\rangle_N,\\ 0, & otherwise,\end{cases} \tag{6}$$

where $loc_i=\langle 2Nc_1l_i-\alpha_i\rangle_N$. Hence, the input-output relation in the AFT domain is given by

$$y\left[p\right]=\sum_{i=1}^{P}\tilde{h}_ie^{j\frac{2\pi}{N}\left(Nc_1l_i^2-ql_i+Nc_2\left(q^2-p^2\right)\right)}x\left[q\right]+w_a\left[p\right], \tag{7}$$

where $q=\langle p+loc_i\rangle_N$ and $p\in[0,N-1]$. For the fractional normalized Doppler shift case, there are some non-zero elements and the peak is still at $q=\langle p+loc_i\rangle_N$ in each row of $\mathbf{H}_{A,i}$ [11].

III. Secure Affine Frequency Division Multiplexing

In this section, we introduce an SE-AFDM system to improve the security of communication systems. The input-output relation of SE-AFDM at the Bob is derived.

A. Proposed SE-AFDM System

In this paper, we use Alice, Bob and Eve to denote the transmitter, the legitimate receiver and the eavesdropper, respectively.

(1) Modulation at the Alice

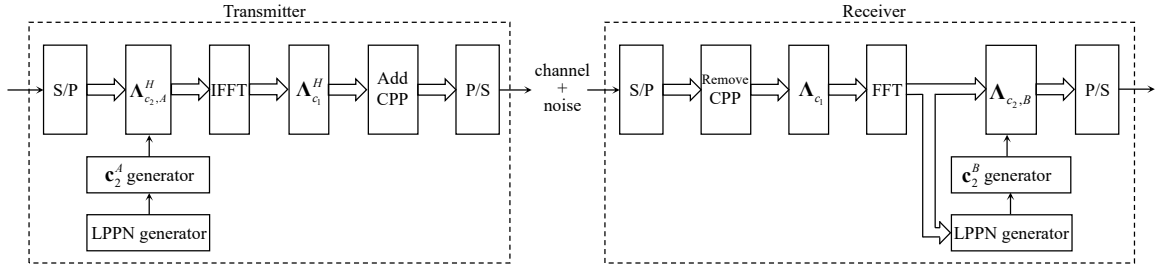

Fig. 1: Block diagram of SE-AFDM communication system.

The corresponding block diagram of the SE-AFDM communication system is shown in Fig. 1. Consider an $N \times 1$ information symbol vector $x[n]$, $n = 0, 1, \ldots, N-1$ from a modulation alphabet $\mathbb{A} = \{a_1, \ldots, a_{|\mathbb{A}|}\}$ (e.g. QAM), which are arranged on the affine domain. Firstly, the vector $\mathbf{x}$ is multiply by a matrix $\mathbf{\Lambda}^H_{c_2,A}$=diag $\left(e^{-j2\pi c_2^A[m]m^2}, m = 0, \ldots, N-1\right)$, where $\mathbf{c}_2^A$ is an $N \times 1$ parameter vector at the Alice, and $c_2^A[m]$ denotes the parameter c_2 corresponding the m-th subcarrier. Each element of $\mathbf{c}_2^A$ is chosen from a codebook $\mathbb{C}_2 = \{c_{2,1}, c_{2,2}, \cdots, c_{2,M}\}$ according to an index that is generated by converting a $log_2 M$-bit binary sequence to decimal, where M denotes the size of $\mathbb{C}_2$. The $log_2 M$-bit binary sequence is obtained by sequentially truncating a LPPN sequence that is produced by the LPPN generator at the Alice. And the codebook $\mathbb{C}_2$ is pre-designed by uniformly discretizing the value range of c_2 within $[-c_{2,\max}, c_{2,\max}]$ which is public to everyone (including Alice, Bob and even Eve).

And then, subsequent operations are the same as the existing AFDM waveform, i.e., performing IDFT, multiplying by matrix $\mathbf{\Lambda}^H_{c_1}$, adding CPP. The resulting SE-AFDM waveform at the Alice in the time domain can be written as

$$s_A[n] = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} x[m]\, e^{j2\pi\left(c_1 n^2 + c_2^A[m]m^2 + \frac{mn}{N}\right)}, \quad (8)$$

where $n = -N_{cp}, \ldots, N-1$.

(2) Demodulation at the Bob

After transmission over the channel with P paths whose gain coefficient, time delay and Doppler shift of the i-th path are denoted by h_i^B, τ_i^B, $f_{d,i}^B$, respectively, the received signal vector at the Bob in the time domain is given by

$$r_B[n] = \sum_{i=1}^{P} \tilde{h}_i^B s_A\left[n - l_i^B\right] e^{j2\pi f_i^B n} + w_B[n], \quad (9)$$

where $\tilde{h}_i^B = h_i^B e^{-j2\pi f_{d,i}^B \tau_i^B}$, $l_i^B = \tau_i^B / t_s$, $f_i^B = f_{d,i}^B t_s$ with t_s denoting the sampling interval, and $\mathbf{w}_B \in \mathbb{C}^{N\times 1}$ is an additive Gaussian noise vector with power spectral density $\sigma_{n,B}^2$.

After serial to parallel conversion (S/P) and discarding CPP, the received SE-AFDM signal at the Bob in the time domain is given by

$$\mathbf{r}_B = \sum_{i=1}^{P} \tilde{h}_i^B \mathbf{\Gamma}_{\mathrm{cpp}_i} \mathbf{\Delta}_{f_i^B} \mathbf{\Pi}^{l_i^B} \mathbf{s}_A + \mathbf{w}_B. \quad (10)$$

Then, multiplying by matrix $\mathbf{\Lambda}_{c_1}$ and performing DFT, we can get

$$\mathbf{r}'_B = \sum_{i=1}^{P} \tilde{h}_i^B \mathbf{F} \mathbf{\Lambda}_{c_1} \mathbf{\Gamma}_{\mathrm{cpp}_i} \mathbf{\Delta}_{f_i^B} \mathbf{\Pi}^{l_i^B} \mathbf{\Lambda}^H_{c_1} \mathbf{F}^H \mathbf{\Lambda}^H_{c_2,A} \mathbf{x} + \mathbf{w}'_B, \quad (11)$$

where $\mathbf{w}'_B = \mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{w}_B$.

After that, $\mathbf{r}'_B$ is multiplied by the matrix $\mathbf{\Lambda}_{c_2,B}$=diag $\left(e^{-j2\pi c_2^B[m]m^2}, m = 0, \ldots, N-1\right)$, where $\mathbf{c}_2^B$ is an $N \times 1$ parameter vector at the Bob. Each element of $\mathbf{c}_2^B$ is also chosen from the codebook $\mathbb{C}_2$ according to an index that is controlled by a $log_2 M$-bit random sequence. The random sequence is produced by another LPPN generator at the Bob. Now, the received matrix at the Bob in the affine domain can be written in matrix form as

$$\begin{aligned}\mathbf{y}_B &= \sum_{i=1}^{P} \tilde{h}_i^B \mathbf{\Lambda}_{c_2,B} \mathbf{F} \mathbf{\Lambda}_{c_1} \mathbf{\Gamma}_{\mathrm{cpp}_i} \mathbf{\Delta}_{f_i^B} \mathbf{\Pi}^{l_i^B} \mathbf{\Lambda}^H_{c_1} \mathbf{F}^H \mathbf{\Lambda}^H_{c_2,A} \mathbf{x} + \bar{\mathbf{w}}_B \\ &= \mathbf{H}_{\mathrm{eff},B}\mathbf{x} + \bar{\mathbf{w}}_B, \end{aligned} \quad (12)$$

where $\bar{\mathbf{w}}_B = \mathbf{\Lambda}_{c_2,B}\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{w}_B$.

B. Input-Output Relation of SE-AFDM Between Alice and Bob

Based on Eq. (12), we can get

$$H_i^0[p,q] = \frac{1}{N} e^{j\frac{2\pi}{N}\left(Nc_1(l_i^B)^2 - ql_i^B\right)} \mathcal{F}_{i,B}[p,q], \quad (13)$$

and

$$\begin{aligned} H_{i,B}[p,q] &= H_i^0[p,q] e^{j2\pi\left[c_2^A[q]q^2 - c_2^B[p]p^2\right]} \\ &= \frac{1}{N} e^{j2\pi\left[c_2^A[q]]q^2 - c_2^B[p]p^2\right]} e^{j\frac{2\pi}{N}\left(Nc_1(l_i^B)^2 - ql_i^B\right)} \mathcal{F}_{i,B}[p,q], \end{aligned} \quad (14)$$

where $\mathcal{F}_{i,B}[p,q] = \frac{e^{-j2\pi\left(p-q-\nu_i^B+2Nc_1 l_i^B\right)}-1}{e^{-j\frac{2\pi}{N}\left(p-q-\nu_i^B+2Nc_1 l_i^B\right)}-1}$ with $\nu_i^B = N f_i^B$. Thus, the input-output relation can be expressed as (15) on the next page. We can see from (15) that the vector $\mathbf{c}_2^A$ generated at the Alice affects every received symbol at the Bob.

Since vectors $\mathbf{c}_2^A$ and $\mathbf{c}_2^B$ are controlled by two different LPPN generators, respectively, if these two LPPN generators are synchronized, we can get synchronized $\mathbf{c}_2^A$ and $\mathbf{c}_2^B$, i.e., $c_2^A[q] = c_2^B[q], q \in [0, N-1]$. As a result, the effective channel $\mathbf{H}_{\mathrm{eff},B}$ can be rewritten as

$$\begin{aligned} H_{\mathrm{eff},B}[p,q] &= \sum_{i=1}^{P} \tilde{h}_i^B H_{i,B}[p,q] \\ &= \sum_{i=1}^{P} \frac{1}{N} \tilde{h}_i^B e^{j2\pi\left[c_2^B[q]q^2 - c_2^B[p]p^2\right]} \times e^{j\frac{2\pi}{N}\left(Nc_1(l_i^B)^2 - ql_i^B\right)} \mathcal{F}_{i,B}[p,q]. \end{aligned} \quad (16)$$

$$y[p]=\sum_{i=1}^{P}h_i^B\sum_{q=0}^{N-1}H_i[p,q]x[q]+w[p]=\sum_{i=1}^{P}h_i^B e^{-j2\pi c_2^B[p]p^2}\sum_{q=0}^{N-1}e^{j2\pi c_2^A[q]q^2}e^{j\frac{2\pi}{N}\left(Nc_1(l_i^B)^2-ql_i^B\right)}\mathcal{F}_{i,B}[p,q]x[q]+w[p]. \quad (15)$$

Now, the effective channel is only affected by the vector $\mathbf{c}_2^B$ at the Bob. Hence, Bob can detect the $\mathbf{x}$ in the minimum mean square error (MMSE) criterion as follows

$$\hat{\mathbf{x}}_B=\mathbf{H}_{\text{eff},B}^H\left(\mathbf{H}_{\text{eff},B}\mathbf{H}_{\text{eff},B}^H+\sigma_{n,B}^2\mathbf{I}_N\right)^{-1}\mathbf{y}_B. \quad (17)$$

It is shown that Bob can recover the transmitted symbols $\mathbf{x}$ from the received $\mathbf{y_B}$, after two LPPN generators of the Alice and the Bob are synchronized. The synchronization methods of LPPN have been widely studied [5]. Thus, we will discuss the synchronization methods in our future work due to page limits.

IV. Security Analyses of SE-AFDM System

In this section, we analyze the security of the proposed SE-AFDM system. Specifically, the input-output relation of SE-AFDM between Alice and Eve is derived. Based on this, we reveal that the effect of the vector $\mathbf{c}_2^A$ can not be eliminated at the Eve. Moreover, the effective SINR of Eve is analyzed, which shows the security is enhanced by reducing the eavesdropping quality of Eve.

A. Input-Output Relation of SE-AFDM at the Eve

Assumption 1: It is assumed that Eve has a very strong capability, that is, it knows the fixed waveform parameters, e.g., c_1, N and the codebook $\mathbb{C}_2$. However, Eve does not know the detailed structure of the LPPN generator of Alice, which means that Eve is unable to reconstruct and synchronize $\mathbf{c}_2^A$.

The received SE-AFDM signal at the Eve in the time domain can be expressed as

$$\mathbf{r}_E=\sum_{i=1}^{P}\tilde{h}_i^E\mathbf{\Gamma}_{\text{cpp}_i}\mathbf{\Delta}_{f_i^E}\mathbf{\Pi}^{l_i^E}\mathbf{s}_A+\mathbf{w}_E, \quad (18)$$

where $\mathbf{w}_E\in\mathbb{C}^{N\times 1}$ is an additive Gaussian noise vector with power spectral density $\sigma_{n,E}^2$.

Similar to (11), after serial to parallel conversion (S/P) and discarding CPP, multiplying by matrix $\mathbf{\Lambda}_{c_1}$ and performing DFT, we can get

$$\mathbf{r}'_E=\sum_{i=1}^{P}\tilde{h}_i^E\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{\Gamma}_{\text{cpp}_i}\mathbf{\Delta}_{f_i^E}\mathbf{\Pi}^{l_i^E}\mathbf{\Lambda}_{c_1}^H\mathbf{F}^H\mathbf{\Lambda}_{c_2,A}^H\mathbf{x}+\mathbf{w}'_E, \quad (19)$$

where $\mathbf{w}'_E=\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{w}_E$.

Then, $\mathbf{r}'_E$ is multiplied by matrix $\mathbf{\Lambda}_{c_2,E}=\text{diag}\left(e^{-j2\pi c_2^E[m]m^2},m=0,\ldots,N-1\right)$, where $\mathbf{c}_2^E$ is the parameter vector at the Eve, the received matrix at the Evea in the affine domain can be written in matrix form as

$$\begin{aligned}\mathbf{y}_E&=\sum_{i=1}^{P}\tilde{h}_i^E\mathbf{\Lambda}_{c_2,E}\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{\Gamma}_{\text{cpp}_i}\mathbf{\Delta}_{f_i^E}\mathbf{\Pi}^{l_i^E}\mathbf{\Lambda}_{c_1}^H\mathbf{F}^H\mathbf{\Lambda}_{c_2,A}^H\mathbf{x}+\bar{\mathbf{w}}_E\\&=\mathbf{H}'_{\text{eff},E}\mathbf{x}'+\bar{\mathbf{w}}_E,\end{aligned} \quad (20)$$

where $\mathbf{H}'_{\text{eff},E}=\sum_{i=1}^{P}\tilde{h}_i^E\mathbf{\Lambda}_{c_2,E}\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{\Gamma}_{\text{cpp}_i}\mathbf{\Delta}_{f_i^E}\mathbf{\Pi}^{l_i^E}\mathbf{\Lambda}_{c_1}^H\mathbf{F}^H$, $\mathbf{x}'=\mathbf{x}\odot\boldsymbol{x}_c$, $x_c[q]=e^{j2\pi c_2^A[q]q^2}, q\in[0,N-1]$, and $\bar{\mathbf{w}}_E=\mathbf{\Lambda}_{c_2,E}\mathbf{F}\mathbf{\Lambda}_{c_1}\mathbf{w}_E$.

B. Analyzing of the Effect of $\mathbf{c}_2^A$ on Eve

According to Assumption 1, Eve can know the matrix $\mathbf{H}'_{\text{eff},E}$. Hence, the vector $\mathbf{x}'$ can be estimated by Eve using MMSE method as

$$\hat{\mathbf{x}}'_E=\mathbf{H}'^H_{\text{eff},E}\left(\mathbf{H}'_{\text{eff},E}\mathbf{H}'^H_{\text{eff},E}+\sigma_{n,E}^2\mathbf{I}_N\right)^{-1}\mathbf{y}_E. \quad (21)$$

Consequently, it can get

$$\begin{cases}e^{j2\pi c_2^A[0]0^2}\cdot x[0] &= \hat{x}_E^{'}[0]\\ &\vdots\\ e^{j2\pi c_2^A[N-1](N-1)^2}\cdot x[N-1] &= \hat{x}_E^{'}[N-1].\end{cases} \quad (22)$$

We can see from (22) that the received $\hat{x}_E^{'}[q]$ consists of both transmitted information symbol $x[q]$ and $c_2^A[q]$ for $q\in[1,N-1]$. If both $\mathbf{x}$ and $\mathbf{c}_2^A$ are varying and unknown to the Eve, the Eve cannot recover $\mathbf{x}$ and $\mathbf{c}_2^A$ according to received $\hat{\mathbf{x}}_E^{'}$, since each equation has two unknowns when $q\geq 1$.

C. Analysis of Effective SINR of Eve

This paper reveals the security of SE-AFDM system by analyzing the effective SINR degradation of Eve. The effective SINR at the receiver is an important measure to characterize the system performance [18]. When the effective SINR of Eve decreases, less information is eavesdropped due to the reduced BER at Eve. The effective SINR analysis is based on the additive white Gaussian noise (AWGN) channel [1]. The analysis of the effective SINR of Eve in multi-path fading channel will be presented in our future work.

The output SINR at the Bob can be expressed as

$$\text{SINR}_B=\frac{p_s\alpha_B^2}{\sigma_{n,B}^2}=\gamma_B, \quad (23)$$

where p_s is the transmit power of Alice, α_B represents the large-scale fading from Alice to Bob, and $\gamma_B=p_s\alpha_B^2/\sigma_{n,B}^2$ denoting the output signal-to-noise ratio (SNR) of the received signal at Bob.

At the Eve, the estimation of the p-th symbol can be rewritten as

$$\begin{aligned}\hat{x}'_E[p]&=x'_E[p]+w_E[p]=x[p]e^{j2\pi c_2^A[p]p^2}+w_E[p]\\&=x[p]+(e^{j2\pi c_2^A[p]p^2}-1)x[p]+w_E[p],\end{aligned} \quad (24)$$

where $w_E[p]$ denotes the residual noise after symbol detection.

[1]The characteristics obtained in AWGN channel is still consistent with our simulation results in the multipath fading channel.

Therefore, the effective output SINR of the p-th symbol at Eve after signal processing is given by [18, Eq. (16)]

$$\mathrm{SINR}_{E,p} = \frac{\mathbb{E}\left\{|x\,[p]|^2\right\}}{\mathbb{E}\left\{|x\,[p]|^2\right\}\mathbb{E}\left\{|\,e^{j2\pi c_2^A[p]p^2}-1\,|^2\right\}+\sigma_{n,E}^2}. \tag{25}$$

Through theoretical derivation, Eq.[25] is reformulated as

$$\mathrm{SINR}_{E,p} \overset{a}{=} \frac{p_s\alpha_E^2}{2p_s\alpha_E^2\left(1-\mathrm{Sa}\left(2\pi p^2 c_{2,\max}\right)\right)+\sigma_{n,E}^2}, \tag{26}$$

where α_E represents the large-scale fading from Alice to Eve, $\mathrm{Sa}\,(\mathrm{x}) = \frac{\sin(\mathrm{x})}{\mathrm{x}}$ denoting the Sa function, and the equality of (a) holds when $c_2^A(p)$ is uniformly distributed over $[-c_{2,\max}, c_{2,\max}]$.

The average effective SINR at the Eve is expressed as

$$\mathrm{SINR}_E = \frac{1}{N}\sum_{p=0}^{N-1}\frac{\gamma_E}{2\gamma_E\left(1-\mathrm{Sa}\left(2\pi p^2 c_{2,\max}\right)\right)+1}, \tag{27}$$

where $\gamma_E = p_s\alpha_E^2/\sigma_{n,E}^2$ denotes the SNR of the received signal at Eve.

Discussion about effective SINR of Eve: We can see from (26) and (27) that the effective SINR of Eve in SE-AFDM system is affected by $c_{2,\max}$, according to the property of the Sa function.

(i) When $c_{2,\max}$ is very small and tends to zero, i.e., $c_{2,\max} \to 0$, $\mathrm{Sa}\left(2\pi p^2 c_{2,\max}\right) = 1$, and then $\mathrm{SINR}_E = \gamma_E = p_s\alpha_E^2/\sigma_{n,E}^2$. When the transmission power p_s at Alice increases, the SNR of Bob γ_B and the SNR of Eve γ_E rise. At this time, there is a high risk of eavesdropping, which means that there is no security.

(ii) Except for $p = 0$, when $c_{2,\max}$ is large enough, $\mathrm{Sa}\left(2\pi p^2 c_{2,\max}\right) \to 0$, and then $\mathrm{SINR}_{E,p} = \frac{\gamma_E}{2\gamma_E+1}$. Furthermore, when $\gamma_E = p_s\alpha_E^2/\sigma_{n,E}^2 \gg 1$, $\mathrm{SINR}_{E,p} \approx 0.5$. At this time, as the transmission power p_s at Alice increases, the SNR of Bob γ_B grows while the SNR of Eve γ_E remains relatively stable. With the amplified p_s, the relative stability of γ_E enhances communication security by preventing eavesdropping quality from rapidly increasing.

In summary, only a large enough $c_{2,\max}$ can provide security in SE-AFDM system. Numerical results will verify this conclusion.

Next, we briefly analyze the complexity of brute force at the Eve and the spectrum efficiency of our SE-AFDM system. If Eve searches for $\mathbf{c}_2^A$ in brute force method, the search space size is M^N for the proposed SE-AFDM system. As a comparison, the search space size for a direct sequence spread spectrum (DSSS) system using N-length LPPN sequence is 2^N. Moreover, our SE-AFDM system enjoys the same spectrum efficiency as the existing AFDM system.

V. Simulation Results

In this section, numerical results based on Monte Carlo simulations are presented. In our simulation, the carrier frequency $f_c = 24$ GHz, and the subcarrier spacing $\Delta_f = 15$ kHz. The QPSK symbols are transmitted. Unless otherwise specified, we consider a channel with $P = 3$ paths, whose delays $l = [0, 1, 2]$ and maximum integer part of the normalized Doppler shift is $\alpha_{\max} = 2$ corresponding to a maximum speed of 1350 km/h [11]. Each path has a different Doppler shift generated by the Jakes model, i.e., $\nu_i = \alpha_{\max} cos(\theta_i)$, where θ_i is uniformly distributed over $[-\pi, \pi]$ [11]. The complex gain of the i-th path h_i is set to be independent complex Gaussian random variables with zero mean and $1/P$ variance. We compare performances of our SE-AFDM and the existing AFDM [11].

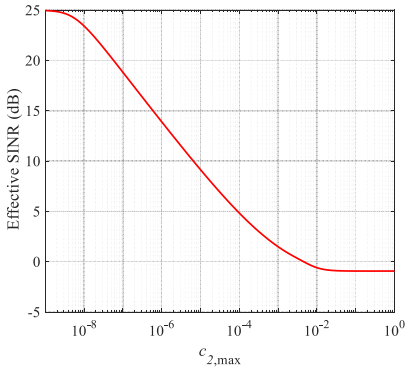

Fig. 2: The effective SINR at Eve versus $c_{2,\max}$ of SE-AFDM with γ_E = 25 dB.

Firstly, based on Eq. (27), the effective SINR at Eve in the SE-AFDM system with different $c_{2,\max}$ is shown in Fig. 2, where $\gamma_E = 25$ dB and $P = 1$. It shows that the effective SINR of Eve declines with the increase of $c_{2,\max}$. Consistent with the theoretical analysis, the effective SINR eventually approaches -0.93 dB as $c_{2,\max}$ continues to increase.

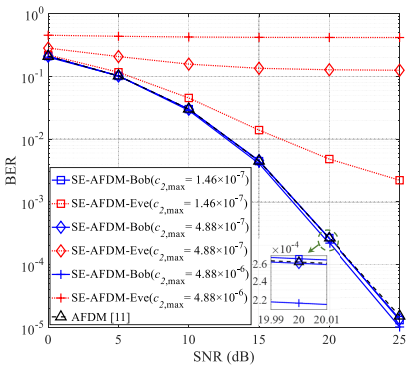

Fig. 3: The BER performances versus SNR with different $c_{2,\max}$ of our SE-AFDM and the existing AFDM.

The BER performances versus SNR with different $c_{2,\max}$ are shown in Fig. 3. In our proposed SE-AFDM system, the BER performances at the Bob are almost the same as that of the existing AFDM system for any $c_{2,\max}$. However, as $c_{2,\max}$ increases, the BER performance at the Eve deteriorates severely, tending to 0.5. These BER performances shows the security performance of the SE-AFDM system improves with the growth of $c_{2,\max}$, which is consistent with Fig. 2.

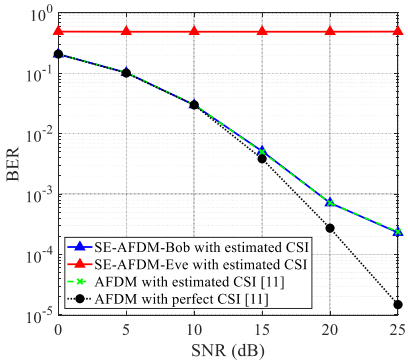

Fig. 4: The BER performances of SE-AFDM and AFDM with estimated CSI at $\mathrm{SNR_p}$ = 30dB.

Next, the impact of channel estimation errors on the BER performance of the SE-AFDM system is explored in Fig. 4 by adopting the channel estimation method [11]. In this case, $c_{2,\max}$ is set as 4.88×10^{-6} and the SNR of pilot symbol, i.e., $\mathrm{SNR_p}$, is 30 dB. With estimated CSI, the BER of our SE-AFDM system at the Bob coincides with that of the AFDM system in [11], both of which are slightly worse than the ideal BER performance. And the BER of the SE-AFDM system at the Eve still tends to be 0.5 with estimated CSI. It is shown that our SE-AFDM system still works in practically estimated channel scenarios.

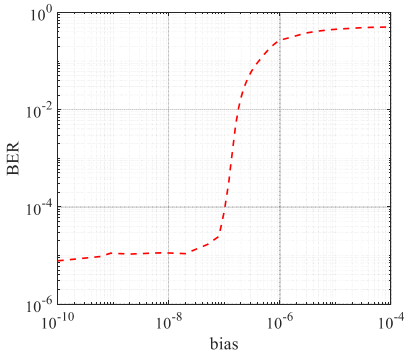

Fig. 5: The BER performance of the Eve versus the bias σ_{c_2} with SNR = 25 dB.

Finally, we investigate the impact of the bias of $\mathbf{c}_2^A$ on BER performance at the Eve, when Eve uses brute force method to search for $\mathbf{c}_2^A$. Here, $c_{2,\max} = 4.88 \times 10^{-5}$, and the bias denotes the difference between actual $\mathbf{c}_2^A$ at the Alice and the $\mathbf{c}_2^E$ searched by Eve, which is defined as $\sigma_{c_2} = \|\mathbf{c}_2^A - \mathbf{c}_2^E\|_\infty$. We can see from Fig. 5 that the BER at the Eve is larger than 0.1 when the bias σ_{c_2} is larger than 4.2×10^{-7}. As the bias decreases, the BER at the Eve reduces. When the bias is less than 2×10^{-8}, the BER remains constant and is close to the BER at the Bob. This result is helpful for designing the codebook $\mathbb{C}_2$, that is, enhanced security can be achieved by setting the interval between the alternative c_2 in the codebook $\mathbb{C}_2$ larger than a threshold, e.g., 4.2×10^{-7}.

VI. Conclusion

This paper introduced a SE-AFDM communication system to improve the security of communication by using the time-varying parameter c_2. Our SE-AFDM system could significantly improve communication security by configuring appropriate parameter c_2. Numerical results showed that there is no lose in BER performance at the Bob compared with the existing AFDM system, but Eve can not eavesdrop on information from Alice.

Acknowledgment

This work was supported in part by the China Postdoctoral Science Foundation under Grant Number 2024M764088, in part by the National Natural Science Foundation of China under Grant 61971025.

References

[1] I. Ara and B. Kelley, "Physical layer security for 6G: Toward achieving intelligent native security at layer-1," *IEEE Access*, vol. 12, pp. 82 800–82 824, 2024.

[2] M. S. J. Solaija, H. Salman, and H. Arslan, "Towards a unified framework for physical layer security in 5G and beyond networks," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 321–343, 2022.

[3] C. Liu, Y. Zhang, J. Xu, J. Zhao, and S. Xiang, "Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher ublock," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5489–5500, 2022.

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

[5] K. S. Raju, Y. Pratap, and P. B. Prasad, "Digital GPS signal generator for L1 band," *Signal Image Process. Int. J.*, vol. 3, no. 6, p. 75, 2012.

[6] T. Xu, "Waveform-defined security: A low-cost framework for secure communications," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10 652–10 667, 2021.

[7] H. Yuan, Y. Xu, X. Guo, T. Ma, H. Li, D. He, and W. Zhang, "PAPR reduction with pre-chirp selection for affine frequency division multiple," *arXiv preprint arXiv:2406.14064*, 2024.

[8] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal time frequency space modulation," in *2017 IEEE Wireless Commun. Netw. Conf. (WCNC)*. IEEE, 2017, pp. 1–6.

[9] J. Sun, Z. Wang, and Q. Huang, "An orthogonal time frequency space direct sequence modulation scheme," in *2021 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.

[10] J. Sun, Z. Wang, and Q. Huang, "Secure precoded orthogonal time frequency space modulation," in *2021 13th Int. Conf. Wireless Commun. Signal Processing (WCSP)*. IEEE, 2021, pp. 1–5.

[11] A. Bemani, N. Ksairi, and M. Kountouris, "Affine frequency division multiplexing for next generation wireless communications," *IEEE Trans. Commun.*, vol. 22, no. 11, pp. 8214–8229, 2023.

[12] Y. Zhou, H. Yin, J. Xiong, S. Song, J. Zhu, J. Du, H. Chen, and Y. Tang, "Overview and performance analysis of various waveforms in high mobility scenarios," in *2024 7th Int. Conf. Commun. Eng. Technol. (ICCET)*. IEEE, 2024, pp. 35–40.

[13] H. Yin and Y. Tang, "Pilot aided channel estimation for AFDM in doubly dispersive channels," in *2022 IEEE/CIC Int. Conf. Commun. China (ICCC)*. IEEE, 2022, pp. 308–313.

[14] A. Bemani, N. Ksairi, and M. Kountouris, "Low complexity equalization for afdm in doubly dispersive channels," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*. IEEE, 2022, pp. 5273–5277.

[15] Y. Ni, Z. Wang, P. Yuan, and Q. Huang, "An AFDM-based integrated sensing and communications," in *2022 Int. Symp. Wireless Commun. Syst. (ISWCS)*. IEEE, 2022, pp. 1–6.

[16] J. Zhu, Q. Luo, G. Chen, P. Xiao, and L. Xiao, "Design and performance analysis of index modulation empowered AFDM system," *IEEE Commun. Lett.*, 2023.

[17] K. Wu, J. A. Zhang, X. Huang, and Y. J. Guo, "Integrating low-complexity and flexible sensing into communication systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1873–1889, Jun 2022.

[18] Q. Zou, A. Tarighat, and A. H. Sayed, "Compensation of phase noise in ofdm wireless systems," *IEEE Trans. Signal Process*, vol. 55, no. 11, pp. 5407–5424, 2007.