A Low-Cost Multi-Band Waveform Security Framework in Resource-Constrained Communications

Tongyang Xu, *Member, IEEE*, Zhongxiang Wei, *Member, IEEE*, Tianhua Xu, *Member, IEEE* and Gan Zheng, *Fellow, IEEE*

***Abstract*—Traditional physical layer secure beamforming is achieved via precoding before signal transmission using channel state information (CSI). However, imperfect CSI will compromise the performance with imperfect beamforming and potential information leakage. In addition, multiple RF chains and antennas are needed to support the narrow beam generation, which complicates hardware implementation and is not suitable for resource-constrained Internet-of-Things (IoT) devices. Moreover, with the advancement of hardware and artificial intelligence (AI), low-cost and intelligent eavesdropping to wireless communications is becoming increasingly detrimental. In this paper, we propose a multi-carrier based multi-band waveform-defined security (WDS) framework, independent from CSI and RF chains, to defend against AI eavesdropping. Ideally, the continuous variations of sub-band structures lead to an infinite number of spectral features, which can potentially prevent brute-force eavesdropping. Sub-band spectral pattern information is efficiently constructed at legitimate users via a proposed chaotic sequence generator. A novel security metric, termed signal classification accuracy (SCA), is used to evaluate the security robustness under AI eavesdropping. Communication error probability and complexity are also investigated to show the reliability and practical capability of the proposed framework. Finally, compared to traditional secure beamforming techniques, the proposed multi-band WDS framework reduces power consumption by up to six times.**

***Index Terms*—Waveform, secure communication, power efficiency, signal classification, deep learning, non-orthogonal, physical layer security, Internet of things.**

I. Introduction

COMMUNICATION security is an increasingly important research topic with the commercialization of 5G and the rapid development of its beyond. In typical radio frequency (RF) based communications, due to the broadcast nature of wireless channels, legitimate user communications are vulnerable to eavesdropping. In traditional eavesdropping scenarios, physical layer secure beamforming [1], [2], [3] is a commonly used physical layer security (PLS) technique, which can prevent eavesdroppers from intercepting confidential data via optimizing spatial signal beams according to channel conditions. However, the secure beamforming techniques are showing limitations [4], [5], [6]. Firstly, confidential data is vulnerable in the presence of multi-antenna eavesdroppers or distributed eavesdroppers and extra processing complexity is required to mitigate the challenges [7], [8]. Experiments in [9] even revealed that an eavesdropper can capture confidential data from directional millimeter waves via using small-scale reflection objects. Moreover, existing security techniques require additional hardware complexity in utilizing multiple antennas and multiple RF chains, which are energy inefficient and against net zero sustainable development objectives [10]. Therefore, the high energy consumption from extra hardware utilization prevents the use of secure beamforming in low-cost Internet of things (IoT) applications [11], [12], [13], [14]. More importantly, traditional secure beamforming techniques require the knowledge of channel state information (CSI). However, CSI could be inaccurate [15] due to pilot spoofing attacks, pilot contamination, and pilot jamming. Therefore, extra processing complexity is required to mitigate the challenges [16], [17]. However, the acquisition of CSI is becoming more costly [18] especially for resource and power limited IoT applications.

Due to the advancement of artificial intelligence (AI), a passive eavesdropper could become an active attacker resulting in AI based threats to communication security. As an attacker, adversarial machine learning [19], [20], [21] can intelligently eavesdrop and further manipulate legitimate user signal characteristics over the air, which could cause signal processing failure at a legitimate user. The adversarial attack challenges end-to-end autoencoder deep learning systems in [22], orthogonal frequency division multiplexing (OFDM) channel estimation and signal detection in [23], multiple input multiple output (MIMO) channel estimation in [24], deep learning MIMO power allocation in [25] and cooperative spectrum sensing in [26]. A more detrimental type of attack is termed generative adversarial network (GAN) [27], which can simultaneously learn legitimate user signal patterns and channel/hardware impairment models to starve scarce over-the-air resources [28] via spoofing attacks. Existing countermeasures for adversarial machine learning attacks is either sending fake

This work was supported in part by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/Y000315/1, EP/X04047X/1, in part by the Natural Science Foundation of China under Grants 62101384, in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2022B1515120018, in part by EU Horizon 2020 MSCA Grant 101008280 (DIOR) and EU Horizon Europe Grant 101131146 (UPGRADE), in part by UK Royal Society Grant (IES/R3/223068). *(Corresponding authors: Tongyang Xu, Zhongxiang Wei.)*

T. Xu is with the School of Engineering, Newcastle University, Newcastle upon Tyne, NE1 7RU, U.K. (e-mail: tongyang.xu@newcastle.ac.uk).

Z. Wei is with the School of Electronics and Information Engineering, Tongji University, China (e-mail: z_wei@tongji.edu.cn).

T. Xu is with the School of Engineering, University of Warwick, Coventry CV4 7AL, United Kingdom (e-mail:tianhua.xu@warwick.ac.uk).

G. Zheng is with the School of Engineering, University of Warwick, Coventry CV4 7AL, United Kingdom (e-mail:gan.zheng@warwick.ac.uk).

data and labels to fool adversaries [29] or proactively applying adversarial attacks to intruders to prevent signal detections [30]. However, the above methods would reduce spectral efficiency and increase system complexity.

The motivation of this work is to prevent AI based eavesdropping and subsequent AI attacks, especially for resource-constrained secure communication scenarios, from a waveform design perspective. Typical 4G/5G systems employ the OFDM waveform [31], [32], which is simple for signal generation and detection but at the cost of security vulnerability. Further investigations on waveform security lead to the study of new waveform design. There are some existing research works on designing waveforms in physical layer security. Masked-OFDM [33] combines two OFDM signals with overlapping to produce a composite non-orthogonal signal and therefore complicates eavesdropping signal detections. However, this approach also results in high complexity at legitimate user side signal detection. Work in [34] employs variable time interval patterns to complicate eavesdropping. However, with the advancement of AI, eavesdroppers could easily identify different patterns using intelligent algorithms. The recent work in [35] proposed a waveform-defined security (WDS) framework, but the framework is still vulnerable to AI based eavesdropping.

This work focuses on optimizing WDS, which is the initial waveform candidate proposed to defend against AI based eavesdropping. To enhance the traditional WDS scheme's robustness to AI eavesdropping, this work proposes an adaptive multi-band WDS framework aiming to further improve communication security. Multi-band waveform architectures can separate a single-band signal into multiple sub-bands. In this case, more spectral ambiguity will be introduced since each sub-band can have independent and unique spectral features. The enhanced spectral ambiguity will prevent AI based eavesdropping and therefore avoid adversarial attacks. It is noted that this work aims for single user scenarios where a user occupies all sub-bands. The use of multi-band architectures is to simplify signal detection and enhance ambiguity rather than supporting multiple users using a multiple access scheme. The fundamental principle behind WDS is the utilization of non-orthogonal waveform spectrally efficient frequency division multiplexing (SEFDM) [36], which introduces feature ambiguity via intentionally tuning sub-carrier packing patterns. As indicated by [37], [38], increased number of antennas or RF chains are the main energy consumption source. Therefore, the proposed multi-band WDS framework, although requiring extra signal processing, can prevent AI based interception for resource-constrained IoT scenarios while available PLS techniques are too costly to implement.

The main contributions of this work are as follows:

- A multi-band WDS secure communication framework is proposed for over-the-air PLS scenarios aiming to defend against AI eavesdropping. Typically, coding can encrypt signals but it cannot prevent AI eavesdropping and the variations of coding rates will complicate signal frame design and hardware implementation. Unlike traditional beamforming PLS approaches that require multiple antennas, the proposed framework is able to enhance PLS security for single-antenna transceivers, which is particular suitable to resource-constrained IoT applications. Sub-carriers are packed non-orthogonally and the packing schemes are adaptively adjustable in each sub-band, thus significantly complicating eavesdropping signal detection. Ideally, the continuous variations of sub-band spectral compression features further enhance the PLS by introducing an infinite number of signal patterns, which prevents accurate signal identifications at the eavesdropper and is robust to exhaustive brute-force eavesdropping. Therefore, the proposed multi-band WDS has further enhanced security than single-band WDS by jointly complicating eavesdropping signal detection and preventing accurate signal pattern identification.
- AI security metric, termed signal classification accuracy (SCA), is proposed to replace the traditional non-AI security metric signal-to-noise ratio (SNR). The eavesdropping classification accuracy approximation model is derived for the adaptive multi-band WDS framework. It shows a perfect match between the analytical model and actual results. It also reveals that the classification accuracy will further degrade by increasing the number of signal patterns and sub-bands.
- A paired-key generator is designed to ensure fast and reliable pattern information generation at both legitimate users. Prior to the key generation, the same bifurcation parameter, initial state, chaotic mapping and pattern threshold should be pre-shared and stored at both legitimate users. Using identical parameter initializations, two identical pattern generators will continuously output identical chaotic sequences, which will be used as pattern keys to produce a correlation matrix. The key generation scheme is practical since only four parameters are needed and stored in memory in advance.
- Lower implementation complexity is achieved by the multi-band waveform security framework such that the framework is suitable for low-cost and resource-constrained communication scenarios where RF chains, antennas and carrier frequency are limited. This work also reveals that the waveform security framework can reduce power consumption by up to six times compared to traditional secure beamforming techniques indicating the suitability of the framework in net-zero communications.

Notations: Unless otherwise specified, matrices are denoted by bold uppercase letters (i.e., $\mathbf{F}$), vectors are represented by bold lowercase letters (i.e., $\mathbf{x}$, $\mathbf{s}$), and scalars are denoted by normal font (i.e., ρ). Subscripts indicate the location of the entry in the matrices or vectors (i.e., $c_{i,j}$ and s_n are the (i,j)-th and the n-th element in $\mathbf{C}$ and $\mathbf{s}$, respectively)

II. The Principle of WDS Framework

The principle of the waveform-defined security communication framework is demonstrated in Fig. 1. Traditional PLS techniques aim to weaken the wiretap link while enhancing the legitimate link using beamforming. However, they require channel state information at the transmitter (CSIT) from both eavesdroppers and legitimate users, which are commonly unavailable in most cases. The proposed WDS framework

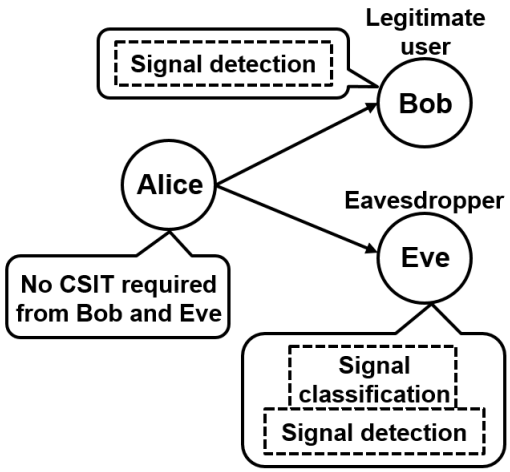

Fig. 1. The waveform based secure communication model for legitimate user and eavesdropper.

avoids CSIT and therefore simplifies the entire system design. Unlike traditional multi-antenna based beamforming defence techniques, a WDS communication system will employ an omni-directional communication format using a single antenna. In this case, the WDS framework saves antennas and RF chains leading to reduced hardware complexity. It is noted that the WDS framework is also applicable in multi-antenna systems, in which it can enhance the over-the-air encryption of beamforming. The eavesdropper is assumed to be passive in this work, therefore it will firstly learn to identify signal patterns and then detect signals. In this case, the aim of WDS is to design signal patterns that will prevent accurate signal classification and complicate signal detection at eavesdroppers.

A. Signal Pattern Principle

The traditional OFDM is a multi-carrier signal with sub-carrier spacing of $\Delta f = 1/T$ where T is the time duration of one OFDM symbol. The principle of SEFDM is to pack sub-carriers closer in a non-orthogonal format while maintaining the bandwidth for each sub-carrier. Therefore, the sub-carrier spacing becomes $\Delta f = \alpha/T$ where α <1 is the bandwidth compression factor (BCF), which determines the bandwidth compression ratio. The spectral bandwidth compression principle for SEFDM is illustrated in Fig. 2 (reused from [35]) where the spectral efficiency improvement of SEFDM over OFDM is given by

$$\eta = (\frac{1}{\alpha} - 1) \times 100. \tag{1}$$

The mathematical expression of an SEFDM signal is obtained by adding α in a typical OFDM signal as

$$x_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{N-1} s_n \exp\left(\frac{j2\pi nk\alpha}{Q}\right), \tag{2}$$

where $\frac{1}{\sqrt{Q}}$ is the power scaling factor, $Q = \rho N$ is the number of time samples where ρ is an oversampling factor and N is the number of sub-carriers. x_k is the k^{th} time sample with the

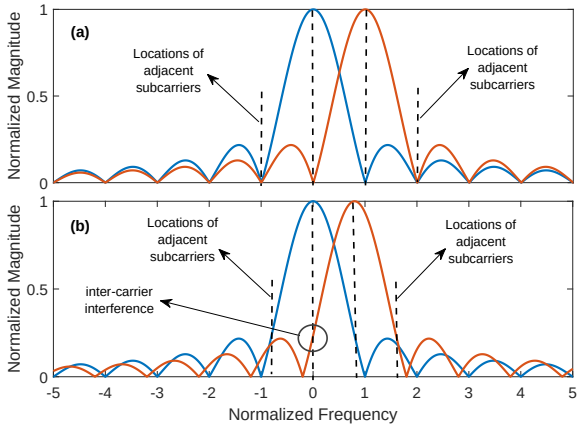

Fig. 2. Principle of non-orthogonal SEFDM signal waveform. (a) OFDM sub-carrier packing. (b) SEFDM sub-carrier packing.

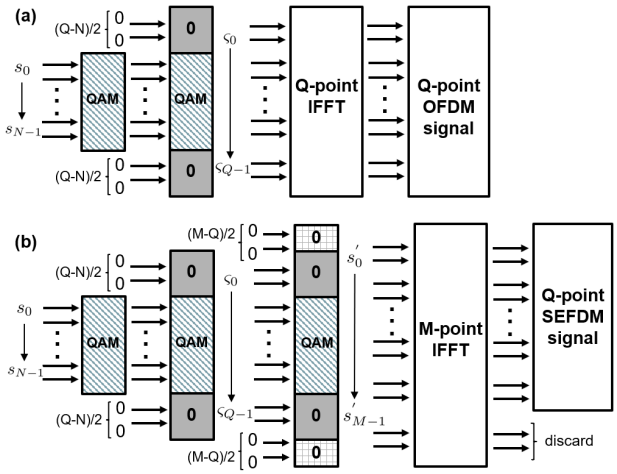

Fig. 3. Signal generation block diagram. (a) OFDM. (b) SEFDM.

index $k = 0, 1, ..., Q-1$. s_n is the n^{th} single-carrier symbol modulated on the n^{th} sub-carrier.

Commonly, a signal requires protection guard bands on both sides. Therefore, in Fig. 3, the original input symbol vector $[s_0, s_1, ..., s_{N-1}]$ is expanded to a Q-dimensional vector as

$$[\varsigma_0, \varsigma_1, ..., \varsigma_{Q-1}] = [\underbrace{0, ..., 0}_{(Q-N)/2}, s_0, s_1, ..., s_{N-1}, \underbrace{0, ..., 0}_{(Q-N)/2}]. \tag{3}$$

Then a Q-point inverse fast Fourier transform (IFFT) is applied in Fig. 3(a) to modulate the vector $[\varsigma_0, \varsigma_1, ..., \varsigma_{Q-1}]$ leading to a Q-point OFDM symbol. For SEFDM signal generation, equation (2) will be transformed into

$$x_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} \varsigma_n \exp\left(\frac{j2\pi nk\alpha}{Q}\right). \tag{4}$$

It is clear that the direct operation of (4) will result in high computational complexity due to the existence of α. To remove the effect of α and directly use IFFT for SEFDM signal generation, the vector $[\varsigma_0, \varsigma_1, ..., \varsigma_{Q-1}]$ has to be further

expanded to a longer vector as shown in Fig. 3(b) with the following operation

$$[s_0^{'}, s_1^{'}, ..., s_{M-1}^{'}] = [\ \underbrace{0, ..., 0}_{(M-Q)/2}, \varsigma_0, \varsigma_1, ..., \varsigma_{Q-1}, \ \underbrace{0, ..., 0}_{(M-Q)/2}\ ], \quad (5)$$

where a new parameter $M = Q/\alpha$ is defined. M should be rounded to its closest integer. A vector of $(M-Q)/2$ zeros are padded on both sides of ς. Therefore, the original signal generation expression will be transformed into an M-point IFFT operation demonstrated in Fig. 3(b) as

$$x_k^{'} = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} s_n^{'} \exp\left(\frac{j2\pi nk}{M}\right), \quad (6)$$

where $n, k = [0, 1, ..., M-1]$. The output will be truncated with only Q samples reserved while the rest of the samples are discarded.

To simplify the expression, a matrix format of the signal generation in (2) is defined as

$$\mathbf{x} = \mathbf{F}\mathbf{s}, \quad (7)$$

where $\mathbf{s}$ is the N-dimensional signal vector, $\mathbf{F}$ is the $Q \times N$ sub-carrier matrix, in which each element is represented by $\exp\left(\frac{j2\pi nk\alpha}{Q}\right)$.

After going through a wireless channel denoted by a $Q \times Q$ channel matrix $\mathbf{H}$ and additive white Gaussian noise (AWGN) $\mathbf{w}$, the received signal is expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}. \quad (8)$$

It is noted that before any further signal processing after (8), the channel effect of $\mathbf{H}$ has to be equalized by multiplying with the inverse of the channel matrix as

$$\hat{\mathbf{y}} = \mathbf{H}^{-1}\mathbf{H}\mathbf{x} + \mathbf{H}^{-1}\mathbf{w} = \mathbf{x} + \mathbf{z}. \quad (9)$$

By multiplying the signal using the complex conjugate demodulation matrix $\mathbf{F}^* = \exp\left(\frac{-j2\pi nk\alpha}{Q}\right)$, the demodulated signal is expressed

$$\mathbf{r} = \mathbf{F}^*\mathbf{x} + \mathbf{F}^*\mathbf{z} = \mathbf{F}^*\mathbf{F}\mathbf{s} + \mathbf{F}^*\mathbf{z} = \mathbf{C}\mathbf{s} + \mathbf{z}_{\mathbf{F}^*}, \quad (10)$$

where $\mathbf{C}$ is the $N \times N$ correlation matrix, which includes the self-created ICI information as

$$c_{m,n} = \frac{sinc[\pi\alpha(m-n)]}{sinc[\pi\alpha(m-n)/Q]} \times \exp\left(\frac{j\pi\alpha(Q-1)(m-n)}{Q}\right). \quad (11)$$

When $m = n$, all the auto-correlation diagonal elements $c_{m,n}$ equal one. When $m \neq n$, all the cross-correlation non-diagonal elements are not zero indicating the self-created inter carrier interference (ICI). It is apparent that the ICI term is related to the value of α, which is the principle for the WDS communication security.

B. Security Metric

The principle of this work is to design waveform patterns that can confuse eavesdroppers. Therefore, to evaluate the robustness, instead of using non-AI security metric SNR, we use AI security metric SCA to indicate the capability of eavesdroppers to correctly identify a signal.

$$SCA = \frac{1}{\lambda} \sum_{\nu=1}^{\lambda} \frac{N_C(\nu)}{N_T(\nu)}, \quad (12)$$

where the number of signal classes is defined by λ. The larger value of λ, the more difficult for an eavesdropper to successfully identify a signal pattern. To have solid evaluations, in each signal class with the index of ν, a total number of N_T symbols are tested. Among N_T symbols, N_C symbols can be correctly identified by an eavesdropper. The ratio of N_C and N_T indicates classification accuracy for one signal class. The final accuracy is obtained by averaging the results from λ signal classes. A small value of SCA indicates a low classification accuracy at Eve, which leads to the failure of signal detection and prevents accurate adversarial AI attacks.

C. Signal Classification Principle

Signal classification is to identify different signal formats associated with the value of α. A perfect signal classification will determine the accurate demodulation matrix $\mathbf{F}^*$ in (10) and further determine the characteristics of $\mathbf{C}$. An imperfect signal classification will mistakenly use a wrong demodulation matrix as

$$\tilde{\mathbf{r}} = \tilde{\mathbf{F}}^*\mathbf{x} + \tilde{\mathbf{F}}^*\mathbf{z} = \tilde{\mathbf{F}}^*\mathbf{F}\mathbf{s} + \tilde{\mathbf{F}}^*\mathbf{z} = \tilde{\mathbf{C}}\mathbf{s} + \mathbf{z}_{\tilde{\mathbf{F}}^*}, \quad (13)$$

where $\tilde{\mathbf{F}}^*$ is the incorrect demodulation sub-carrier matrix caused by misclassification. Compared to the ideal matrix $\mathbf{F}^*$ in (10), a BCF offset $\Delta\alpha$ will exist in the imperfect $\tilde{\mathbf{F}}^*$ with the new expression as $\tilde{\mathbf{F}}^* = \exp\left(\frac{-j2\pi nk(\alpha+\Delta\alpha)}{Q}\right)$. The mismatch between $\tilde{\mathbf{F}}^*$ and $\mathbf{F}$ will cause an imperfect estimate of $\tilde{\mathbf{C}}$ as

$$\tilde{c}_{m,n} = \frac{sinc[\pi(\alpha_T m - \alpha_R n)]}{sinc[\pi(\alpha_T m - \alpha_R n)/Q]} \times \exp\left(\frac{j\pi(Q-1)(\alpha_T m - \alpha_R n)}{Q}\right), \quad (14)$$

where α_T is the BCF at the transmitter and $\alpha_R = \alpha_T + \Delta\alpha$ is the incorrect BCF at the receiver.

The traditional and optimal classification method is maximum likelihood, which has been investigated for modulation classification in [39], [40]. The likelihood function, with perfect knowledge of all parameters except modulation format, is expressed as

$$L_f(r|\mathfrak{M}, \sigma) = \frac{1}{P} \prod_{n=0}^{N-1} \sum_{p=0}^{P-1} \frac{1}{2\pi\sigma^2} \exp\left(-\frac{|r_n - \mathfrak{M}(i,p)|^2}{2\sigma^2}\right), \quad (15)$$

where $\mathfrak{M}$ represents the modulation class, $\mathfrak{M}(i,p)$ indicates the p^{th} constellation symbol in the i^{th} modulation scheme. There are P constellation points for each modulation. σ^2 is noise variance when AWGN is considered and r_n is the n^{th} single-carrier complex symbol.

Table I: Hardware Complexity Analysis (uplink channel from Alice to Bob)

Framework	Hardware
Traditional PLS (digital beamforming)	RF Chain(multiple) Antenna(multiple)
Traditional PLS (hybrid analog-digital beamforming)	RF Chain(multiple) Antenna(multiple)
Traditional PLS (analog beamforming)	RF Chain(single) Antenna(multiple)
WDS(Alice): User	RF Chain(single) Antenna(single)
WDS(Bob): Base Station	RF Chain(single) Antenna(single)
WDS(Eve): Eavesdropper	RF Chain(single/multiple) Antenna(single/multiple)

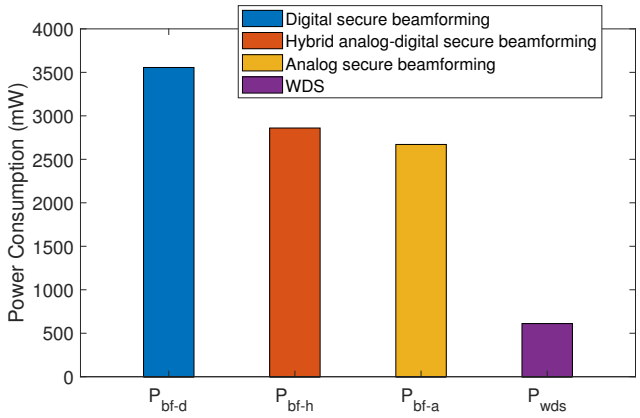

Fig. 4. Power consumption comparison for full-digital secure beamforming, hybrid analog-digital secure beamforming, analog secure beamforming and WDS frameworks.

The optimal solution is obtained via maximizing the likelihood function (15) by attempting all the potential modulation candidates as

$$\hat{\mathfrak{M}} = \arg \max_{\mathfrak{M}(i)\in\Theta} L_f(r|\mathfrak{M}, \sigma), \tag{16}$$

where Θ indicates all the potential candidates for the i^{th} modulation format.

The traditional maximum likelihood method is not realistic for non-orthogonal signal classification. Therefore, intelligent classification using artificial intelligence would be a potential solution. Deep learning based convolutional neural network (CNN) has been investigated for single-carrier modulation classification in [41] with competitive accuracy relative to the maximum likelihood method. The automatic learning CNN classifier has also been tested for non-orthogonal multi-carrier signal classification in [42]. Therefore, the CNN model will be used for eavesdropping signal classification in this work.

D. Power Consumption Comparison

The WDS framework aims for low-cost and resource-constrained communications where IoT is a matched application scenario. Most IoT traffic occurs at uplink channels where each IoT unit sends information back to base stations. Therefore, we consider power consumption for uplink channel communications with the complexity comparison in Table I where hardware utilization for each scenario is compared. In the column of 'Hardware', detailed hardware utilization is presented. In the bracket, 'single' indicates one such component is needed while 'multiple' indicates several such components have to be used. There is no specific data associated with Table I where this table only shows general hardware utilization for different scenarios. The proposed multi-band WDS framework utilizes single-RF chain while traditional PLS has to employ multiple RF chains for digital beamforming, where the traditional solution consume more power [37], [38].

Based on the studies in [43], [44], the power consumption for digital beamforming P_{bf-d}, hybrid analog-digital beamforming P_{bf-h}, analog beamforming P_{bf-a} and WDS P_{wds} could be computed in the following

$$P_{bf-d} = P_{lo} + N_{rf-f}(P_{dac} + P_{mixer} + P_f + \frac{P_t}{\xi}), \tag{17}$$

$$P_{bf-h} = P_{lo} + N_{rf-h}(P_{dac} + P_{mixer} + P_f) + N_{ps}(P_{ps} + \frac{P_t}{\xi}), \tag{18}$$

$$P_{bf-a} = P_{lo} + P_{dac} + P_{mixer} + P_f + N_{ps}(P_{ps} + \frac{P_t}{\xi}), \tag{19}$$

$$P_{wds} = P_{lo} + P_{dac} + P_{mixer} + P_f + \frac{P_t}{\xi}, \tag{20}$$

where P_{lo}, P_{dac}, P_{mixer}, P_f, P_t and P_{ps} indicate the power consumption for the local oscillator, digital-to-analogue converter (DAC), mixer, filter, transmit signal and phase shifter. N_{rf-d} is the number of RF chains for digital beamforming, N_{rf-h} is the number of RF chains for hybrid beamforming and N_{ps} is the number of phase shifters. ξ indicates the efficiency of a power amplifier. Based on [43], [44], we set P_{lo}=22 mW, P_{dac}=170 mW, P_{mixer}=5 mW, P_f=14 mW, P_t=200 mW, P_{ps}=10 mW, ξ=50%. Based on [45], [46], we set N_{rf-f}=6, N_{rf-h}=2, N_{ps}=6. The power consumption for each system design is compared in Fig. 4, in which our proposed WDS framework can reduce power consumption by up to six times compared to traditional multi-antenna based secure beamforming techniques.

III. Signal Detection

In the framework in Fig. 1, the legitimate user Bob has correct signal detection because the signal pattern information is pre-known between Alice and Bob. However, signal detection at Eve would fail due to signal misclassification.

A. WDS Signal Detection

Once the correlation matrix $\mathbf{C}$ is determined via either paired-key information at Bob or signal classification at Eve, signal detection has to be operated to recover original signals from ICI. The optimal signal detection method is maximum likelihood (ML) while its computational complexity is exponentially increased when the number of sub-carriers increases. Its simplified version is sphere decoding (SD) [47], which searches for the optimal solution within a pre-defined space.

The SD search for the optimal estimate $\mathbf{s}_{SD}$ is defined as

$$\mathbf{s}_{SD} = \arg \min_{\mathbf{s}\in O^N} \|\mathbf{r} - \mathbf{C}\mathbf{s}\|^2 \leq g, \tag{21}$$

where O is the constellation cardinality and O^N covers all possible solutions. g is the pre-defined search radius and it equals the distance between the demodulated $\mathbf{r}$ and the hard-decision $\mathbf{s}_{ZF}$. It is noted that the hard-decision $\mathbf{s}_{ZF}$ is computed based on the zero forcing (ZF) criterion using a rounding function $\lfloor . \rceil$ as $\mathbf{s}_{ZF} = \lfloor \mathbf{C^{-1}r} \rceil$. Therefore, the search radius is defined as

$$g = \|\mathbf{r} - \mathbf{C}\mathbf{s}_{ZF}\|^2 . \tag{22}$$

The norm calculation in (21) can be re-formatted in (23) by substituting $\mathbf{p} = \mathbf{C^{-1}r}$ where $\mathbf{p}$ is the soft-decision estimate of $\mathbf{s}$.

$$\mathbf{s}_{SD} = \arg \min_{\mathbf{s} \in O^N} \{(\mathbf{p}-\mathbf{s})^* \mathbf{C}^* \mathbf{C} (\mathbf{p}-\mathbf{s})\} \leq g. \tag{23}$$

The expression can be further simplified using Cholesky decomposition [48] via $chol\{\mathbf{C}^*\mathbf{C}\} = \mathbf{L}^*\mathbf{L}$, where $\mathbf{L}$ is an $N \times N$ upper triangular matrix. Therefore, (23) can be re-written as

$$\mathbf{s}_{SD} = \arg \min_{\mathbf{s} \in O^N} \|\mathbf{L}(\mathbf{p}-\mathbf{s})\|^2 \leq g. \tag{24}$$

The triangular structure of $\mathbf{L}$ can simplify (24) into N steps with the following expression

$$\begin{aligned} g \geq & (l_{N-1,N-1}(p_{N-1} - s_{N-1}))^2 + (l_{N-2,N-2}(p_{N-2} - \\ & s_{N-2}) + l_{N-2,N-1}(p_{N-1} - s_{N-1}))^2 + ..., \end{aligned} \tag{25}$$

where $l_{i,j}$, p_i and s_i are the elements of $\mathbf{L}$, $\mathbf{p}$ and $\mathbf{s}$ in (24), respectively. To study each term in (25), the N-dimensional expression is divided into N independent one-dimensional terms. The $(N-1)^{th}$ inequality term is thus represented as

$$l^2_{N-1,N-1}(p_{N-1} - \mathbf{s}_{N-1})^2 \leq g_{N-1} = g. \tag{26}$$

Therefore, the search range for the $(N-1)^{th}$ dimension is derived as

$$\lceil -\frac{\sqrt{g_{N-1}}}{l_{N-1,N-1}} + p_{N-1} \rceil \leq s_{N-1} \leq \lfloor \frac{\sqrt{g_{N-1}}}{l_{N-1,N-1}} + p_{N-1} \rfloor, \tag{27}$$

where $\lceil \cdot \rceil$ $\lfloor \cdot \rfloor$ denote rounding operations to the nearest larger and smaller integers, respectively.

Therefore, the left term of (27) indicates a hard lower bound (H-LB) while the right term indicates a hard upper bound (H-UB). It is clearly seen that an accurate estimate of s_{N-1} is related to g_{N-1}, $l_{N-1,N-1}$ and p_{N-1}, which are all determined by the accurate estimate of $\mathbf{C}$.

After the search at the $(N-1)^{th}$ dimension, the search radius g_{N-2} for the next dimension is updated as

$$g_{N-2} = g_{N-1} - l^2_{N-1,N-1}(p_{N-1} - s_{N-1})^2. \tag{28}$$

The search principle in (27) and the radius update in (28) will be repeated until the last dimension. The final solution $\mathbf{s}_{SD}$ is obtained as an N-dimensional vector that meets the condition in (21). Each element estimation in $\mathbf{s}_{SD}$ is dependent on the elements from its previous dimensions. The perfect knowledge of $\mathbf{C}$ plays an important role since an imperfect estimate of $\mathbf{C}$ will give a wrong decision interval in (27) and might cause no solution at the end. Therefore, the first step signal classification is crucial to an eavesdropper who aims to decode signals.

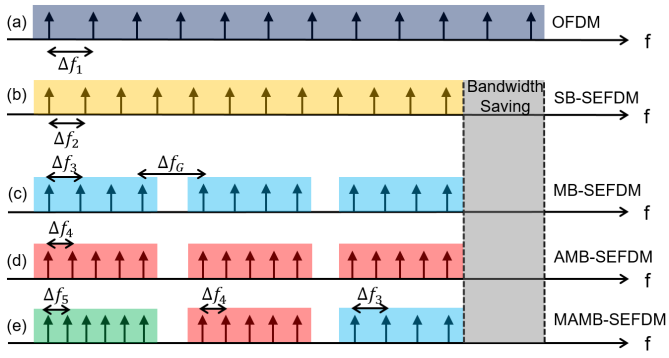

Fig. 5. Spectral illustration for (a) OFDM, (b) SB-SEFDM, (c) MB-SEFDM, (d) AMB-SEFDM, (e) MAMB-SEFDM. Each impulse in each sub-figure indicates one sub-carrier and each coloured rectangular block indicates a signal band or a sub-band.

B. Impact of Imperfect Classification

An imperfect signal classification will mislead the estimate of $\mathbf{C}$, which further gives inaccurate calculation of $\mathbf{L}$ in Cholesky decomposition. Therefore, the element $l_{i,j}$ in $\mathbf{L}$ will become $l_{i,j} + \Delta l$, where Δl is the offset caused by imperfect signal classification. Meanwhile, since the soft-decision estimation follows $\mathbf{p} = \mathbf{C^{-1}r}$, the new estimate of each element will become $p_i + \Delta p$ where Δp is the offset caused by imperfect signal classification. It should be noted that signal misclassification will cause inaccurate $\hat{\mathbf{s}}_{ZF} = \lfloor (\mathbf{C} + \Delta\mathbf{C})^{-1}\mathbf{r} \rceil$ as well. Therefore, the search space g_i in (22) will become $g_i + \Delta g$ where Δg is the offset caused by imperfect signal classification.

The above imperfect estimates will jointly cause inaccurate estimate of $\mathbf{s}$. The lower bound and upper bound in (27) will be improperly biased to

$$LB = \lceil -\frac{\sqrt{g_{N-1} + \Delta g}}{l_{N-1,N-1} + \Delta l} + p_{N-1} + \Delta p \rceil. \tag{29}$$

$$UB = \lfloor \frac{\sqrt{g_{N-1} + \Delta g}}{l_{N-1,N-1} + \Delta l} + p_{N-1} + \Delta p \rfloor. \tag{30}$$

Therefore, the variations of Δg, Δl and Δp, due to imperfect signal classification, will cause signal detection failure.

IV. Secure Multi-Band Framework

To ensure a joint secure and detectable communication system, the signal waveform has to be modified. This section will investigate four WDS signal waveform architectures in Fig. 5, namely single-band SEFDM (SB-SEFDM), multi-band SEFDM (MB-SEFDM), adaptive multi-band SEFDM (AMB-SEFDM) and mixed adaptive multi-band SEFDM (MAMB-SEFDM).

A. Single-Band

The WDS framework was initially designed for single-band signals. In this case, sub-carriers are packed consecutively without empty guard bands. The traditional SB-SEFDM signal

architecture is presented in Fig. 5(b). To simplify the illustration, each impulse represents a sub-carrier. For a better demonstration, only a partial number of sub-carriers and sub-bands are presented. It should be noted that all the designs in Fig. 5 have the same sub-carrier bandwidth. The only difference is the sub-carrier spacing. In order to achieve bandwidth compression, the sub-carrier spacing for SB-SEFDM should satisfy $\Delta f_2 < \Delta f_1$, where Δf_1 and Δf_2 indicate the sub-carrier spacing of OFDM and SB-SEFDM, respectively.

According to 4G [49] and 5G [50] standards, a multi-carrier signal bandwidth is defined by the multiplication of sub-carrier spacing Δf and the number of sub-carriers N. Therefore, the spectral bandwidths for the cases in Fig. 5(a) and Fig. 5(b) are defined by $B_{_{OFDM}} = N\Delta f$ and $B_{_{SB-SEFDM}} = \alpha N\Delta f$ respectively.

The single-band SB-SEFDM signal architecture might challenges signal detection since the sophisticated SD detector has to be applied resulting in exponentially increased computational complexity especially when the size of a signal is scaled up. Thus, communication security is ensured such that eavesdroppers cannot decode signals easily but at the cost of complicating legitimate user signal recovery as well.

B. Multi-Band

The principle of the multi-band signal architecture, shown in Fig. 5(c), is to partition the single-band signal into multiple sub-bands with an empty sub-carrier between two adjacent sub-bands. The purpose of the protection gap is to mitigate inter-band interference. In this case, each sub-band signal can be recovered separately using the SD detector leading to reduced computational complexity.

The total occupied spectral bandwidth of the multi-band signal is equivalent to that of a typical single-band signal. Due to one empty sub-carrier as the protection gap $\Delta f_G = 2\Delta f_3$ between two adjacent sub-bands in Fig. 5(c), the sub-carrier spacing in each sub-band has to be further squeezed leading to the spacing $\Delta f_3 < \Delta f_2 < \Delta f_1$. The effective spectral bandwidth of MB-SEFDM is defined as

$$B_{_{MB-SEFDM}} = \beta(N + \frac{N}{N_B} - 1)\Delta f, \tag{31}$$

where N_B is the number of sub-carriers in each sub-band and β indicates the sub-band bandwidth compression factor. To ensure the same occupied spectral bandwidth $B_{_{MB-SEFDM}} = B_{_{SB-SEFDM}}$, the sub-band β is calculated as

$$\beta = \frac{\alpha N}{N + \frac{N}{N_B} - 1}. \tag{32}$$

The mathematical expression of the multi-band SEFDM signal is given by

$$x_k = \frac{1}{\sqrt{Q}} \sum_{l_B=0}^{\frac{N}{N_B}-1} \sum_{i=0}^{N_B-1} s_{_{i+l_B N_B}} \exp\left(\frac{j2\pi k\beta(i + l_B(N_B+1))}{Q}\right), \tag{33}$$

where $s_{_{i+l_B N_B}}$ is the i^{th} single-carrier symbol modulated in the ${l_B}^{th}$ sub-band.

To directly use IFFT for the multi-band SEFDM signal generation, the raw symbol mathematical expression in (33) has to be updated to

$$s_m^{''} = s_{n+\lfloor \frac{n}{N_B} \rfloor}^{''} = \begin{cases} s_n & 0 \le n < N \\ 0 & otherwise \end{cases}, \tag{34}$$

where related parameters are defined below

$$\begin{cases} n & = i + l_B N_B \\ m & = i + l_B(N_B+1) = n + l_B \\ l_B & = \lfloor \frac{n}{N_B} \rfloor \end{cases}. \tag{35}$$

Therefore, the original multi-band signal expression in (33) is converted to a new expression as

$$x_k = \frac{1}{\sqrt{Q}} \sum_{m=0}^{N+\frac{N}{N_B}-2} s_m^{''} \exp\left(\frac{j2\pi mk\beta}{Q}\right). \tag{36}$$

Following the same zero padding method in (5), a new input symbol vector is generated as

$$s_m^{'''} = \begin{cases} 0 & 0 \le m < (M - Q^{'})/2 \\ s_m^{''} & (M - Q^{'})/2 \le m < (M + Q^{'})/2 \\ 0 & (M + Q^{'})/2 \le m < M \end{cases}, \tag{37}$$

where $Q^{'} = N + \frac{N}{N_B} - 1$, $M = Q/\beta$ is rounded to its closest integer. The expression in (36) is therefore adjusted to a new form as

$$x_k^{''} = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} s_m^{'''} \exp\left(\frac{j2\pi mk}{M}\right), \tag{38}$$

where $m, k = [0, 1, ..., M-1]$. The output is truncated with only Q samples reserved while the rest of the samples are discarded.

C. Adaptive Multi-Band

The multi-band signal architecture simplifies signal detection. However, the challenge of the multi-band signal architecture is that eavesdroppers can filter and extract each sub-band and operate signal classification for each one. To enhance multi-band communication security, an adaptive multi-band signal architecture is proposed in Fig. 5(d).

Modifying spectral features of a signal would effectively prevent unauthorized signal feature learning and format identification. It is observed from Fig. 5(d) that the overall occupied spectral bandwidth is similar to the traditional MB-SEFDM but with further reduced bandwidth compression factor leading to $\Delta f_4 < \Delta f_3 < \Delta f_2 < \Delta f_1$. The scheme in Fig. 5(d) would mislead eavesdroppers to classify an AMB signal of β_0 into an MB signal of β_1 due to their similar spectral characteristics. Meanwhile, the AMB signal architecture in Fig. 5(d) achieves a higher data rate than the MB signal in Fig. 5(c).

Considering an example comparison including three types of signals where the bandwidth compression factors for the signals in each sub-band satisfy $\beta_2 < \beta_1 < \beta_0$. To make three signals similar, more sub-carriers will be packed in β_1, β_2 relative to β_0. The sub-carrier packing strategy is

$$B_{_{sub}} = \beta_0 N_B \Delta f = \beta_1(N_B + \Delta N_1)\Delta f = \beta_2(N_B + \Delta N_2)\Delta f, \tag{39}$$

where $B_{_{sub}}$ is the bandwidth for one sub-band, ΔN_1 is the number of additional sub-carriers per sub-band that have to

be packed for β_1 relative to β_0 and ΔN_2 is the number of additional sub-carriers per sub-band that have to be packed for β_2 relative to β_0. In this case, the spectral bandwidth per sub-band for the three SEFDM signals would be similar and can easily cause eavesdropping misclassification.

Due to additional sub-carrier packing, the original multi-band signal in (33) is modified to a new format as

$$x_k = \frac{1}{\sqrt{Q}} \sum_{l_B=0}^{\frac{N+\Delta N}{N_B+\Delta N_B}-1} \sum_{i=0}^{N_B+\Delta N_B-1} s_{i+l_B(N_B+\Delta N_B)} \times \exp\left(\frac{j2\pi k\beta(i+l_B(N_B+\Delta N_B+1))}{Q}\right), \tag{40}$$

where the number of sub-carriers in each sub-band is increased to $N_B+\Delta N_B$ and the total number of sub-carriers is increased to $N+\Delta N$. However, the number of sub-bands maintains the same with the following relationship

$$\frac{N+\Delta N}{N_B+\Delta N_B} = \frac{N}{N_B}. \tag{41}$$

Signal generation for the AMB signal in (40) is straightforward via IFFT following the similar operations from (34) to (38) except that more data sub-carriers are required by (40).

D. Mixed Adaptive Multi-Band

To enhance further communication security, a mixed adaptive multi-band (MAMB) signal waveform design is considered to flexibly tune BCF in each sub-band, where each sub-band has different BCF configurations but the overall effective BCF maintains the same. In Fig. 5(e), each independent sub-band has different number of sub-carriers, by adjusting sub-carrier spacing, the spectral bandwidth for each sub-band and the total occupied spectral bandwidth maintain the same leading to more confusions to eavesdroppers.

To confuse eavesdroppers, the sub-band BCF can be intentionally tuned with various patterns. Since each sub-band has a unique BCF, signal generation using a single-IFFT might be unrealistic. Therefore, multiple IFFTs have to be used and the number of IFFTs depends on the number of sub-bands. The composite MAMB signal, including all sub-bands, is represented as the following

$$\begin{aligned} x_k =& \frac{1}{\sqrt{Q}} \sum_{i=0}^{N_B+\Delta N_0-1} s_{0i} \times \exp\left(\frac{j2\pi k\beta_0 i}{Q}\right) \\ &+ \frac{1}{\sqrt{Q}} \sum_{i=0}^{N_B+\Delta N_1-1} s_{1i} \times \exp\left(\frac{j2\pi k\beta_1(i+\varepsilon_0))}{Q}\right) \\ &+ ... \\ &+ \frac{1}{\sqrt{Q}} \sum_{i=0}^{N_B+\Delta N_\Theta-1} s_{\Theta i} \times \exp\left(\frac{j2\pi k\beta_\Theta(i+\varepsilon_\Theta))}{Q}\right), \end{aligned} \tag{42}$$

where $\Theta = N/N_B - 1$ is the maximum number of sub-band index, s_{0i} indicates the i^{th} symbol in the first sub-band and $s_{\Theta i}$ indicates the i^{th} symbol in the Θ^{th} sub-band. β_0 is the sub-band BCF in the first sub-band and β_Θ is the sub-band BCF in the Θ^{th} sub-band.

Since each sub-band has to be perfectly aligned without causing any spectral feature difference, each sub-band has to uniquely pack extra sub-carriers (i.e. $\Delta N_0, \Delta N_1, ..., \Delta N_\Theta$) and has to be adaptively offset in frequency domain (i.e. $\varepsilon_0, \varepsilon_1, ..., \varepsilon_\Theta$). It should be noted that the frequency offset for each sub-band alignment can be easily implemented by adaptively adding zeros to input symbol vectors (i.e. $s_{0i}, s_{1i}, ..., s_{\Theta i}$) similar to the operations in (3) and (5). Then similar operations will be followed from (34) to (38) before the direct use of IFFT for signal generation.

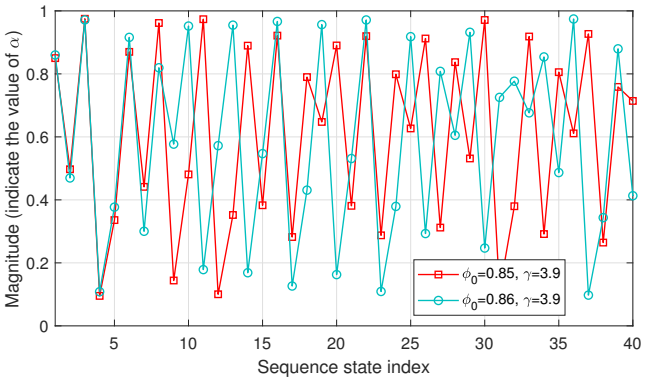

Fig. 6. Chaotic sequence illustration for two configurations with the minor difference in initial state ϕ_0.

V. Pattern Key Generation

To ensure the communication reliability between legitimate users, the signal pattern key, has to be known between Alice and Bob. However, it is impractical to exchange a large number of pattern information between legitimate users in each communication session. Therefore, an efficient way to generate pattern keys at both sides is of great importance.

A paired-key generator is proposed in this work. The idea is to design a signal pattern generator that will be deployed at both the transmitter and the receiver. A chaotic dynamic system [51] can generate a random-like but reproducible chaotic sequence, which will be a simple solution for the WDS signal pattern generator. A discrete-time dynamical system is defined with the following state equation

$$\phi_{k+1} = f(\phi_k), \tag{43}$$

where $0 < \phi_k < 1$ indicates the value at the k^{th} state and $0 < \phi_{k+1} < 1$ indicates the value at the $(k+1)^{th}$ state. $f(\cdot)$ represents a chaotic map, which is used to produce sequence bits at different states. It is noted that the value of next state is highly dependent on its previous state. There are various chaotic maps and the commonly used one is logistic map, which is defined in [51] as

$$\phi_{k+1} = \gamma \cdot \phi_k(1-\phi_k), \tag{44}$$

where γ is the bifurcation parameter with values $1 < \gamma < 4$ defined by [52]. The value of γ determines the feature of a generated sequence. With a larger value of γ, the generated sequence is non-periodic and non-converging. The studies in [52] have proved that a minor change of the three factors will produce a completely different sequence.

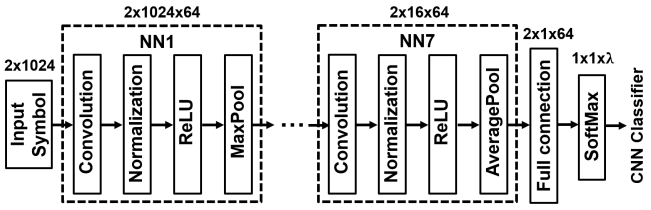

Fig. 7. CNN signal classifier architecture.

To show the pattern sequence generation mechanism, we compare two systems in Fig. 6. The first one is configured with γ=3.9, initial state ϕ_0=0.85 and the logistic map following (44). The second system has the same configurations except that the initial state is slightly increased to ϕ_0=0.86. With such a minor difference, two systems will produce different sequences in Fig. 6, which can effectively prevent eavesdroppers from using exhaustive methods to guess the sequence.

The random-like sequence, as shown in Fig. 6, helps to generate pattern key α. To implement the generation algorithm, a threshold $0 < \eta < 1$ is introduced to decide which pattern key should be generated. For example, to generate a pattern key sequence with α=(0.9, 0.85, 0.8) using Fig. 6, a threshold η=0.75 could be used where only the values beyond the threshold η is considered. For any values between 0.75 and 0.8, the key is α=0.8; for any values between 0.8 and 0.85, the key is α=0.85; for any values between 0.85 and 0.9, the key is α=0.9. In this case, a pattern key sequence including α=(0.9, 0.85, 0.8), is obtained.

The cooperation of the bifurcation parameter γ, chaotic map $f(\cdot)$, initial state ϕ_0 and pattern threshold η will enable an efficient and secure pattern index generation scheme. An eavesdropper will not easily obtain an accurate pattern index sequence since a minor change of each parameter will produce a completely different sequence.

VI. Classifier Training and System Performance

A. Classifier Training

The trained CNN architecture is presented in Fig. 7 where seven convolutional layers are stacked for automatic feature extraction. The dimension of each layer is presented above each neural network sub-block. Each training symbol is configured to have 2048 complex time samples. To have a robust classifier, 1024 training samples is randomly captured out of the 2048 time samples. Therefore, the input training symbol size is 2×1024 since a complex symbol has real and imaginary parts. To avoid overfitting in the neural network training, a 50% dropout ratio is configured. To have a universal classifier that can generally identify signals at different noise conditions, the training signals will go through a wide range of noise impacts with Es/N0 ranging from -20 dB to 50 dB with a 10 dB increment step. To extract rich features, the CNN classifier applies 64 feature filters and therefore the first neural network (NN) sub-block outputs a three-dimensional 2×1024×64 feature matrix. To reduce the size of a feature matrix, downsampling functions such as MaxPool and AveragePool are applied. The full connection layer will resize the 2×1×64 input feature matrix to a 1×1×λ output feature vector with λ indicating the number of signal classes. In the end, the SoftMax layer computes the probability of each predicted signal class using the SoftMax function as

$$P_r(\psi_i) = \frac{e^{\psi_i}}{\sum_{j=1}^{\lambda} e^{\psi_j}}, \tag{45}$$

where $\Psi = (\psi_1, \psi_2, ..., \psi_\lambda) \in \mathbb{R}^\lambda$ indicates the input feature vector to the SoftMax function and it includes λ real numbers with the element index $i = 1, 2, ..., \lambda$. The computation in (45) ensures each output from the SoftMax is within the interval $[0, 1]$ and the sum of each output equals one.

To find a classifier that works well for all the signal classes, cross entropy is computed as an indicator for the total loss as

$$Loss = -\sum_{i=1}^{\lambda} P_r^T(\psi_i) \cdot \ln(P_r(\psi_i)), \tag{46}$$

where $P_r^T(\psi_i)$ is the true probability that the i^{th} input signal belongs to the i^{th} signal class while $P_r(\psi_i)$ is the predicted probability that the i^{th} input signal belongs to the i^{th} signal class. With the cross entropy calculation, the neural network can optimize its architecture via backward propagation using the Adam optimizer. The maximum number of epochs is limited to 30 and the mini-batch size is 128. To fully extract features from a dataset, a learning rate of 0.01 is configured through the training.

The signal pattern for each framework should be designed according to the pattern keys generated by the proposed chaotic sequence generator in section V. Ideally, the key, in other words the bandwidth compression factor α, is continuous and therefore has an infinite number of values. This will advantageously show the robustness of our proposed framework in practice but the infinite number of values also complicate the evaluations of the proposed framework in simulations. Therefore, in this work, we use discrete values of α instead of using continuous values. The effect of a relatively small change of α has been studied in [35] where the work showed that the narrower gap between adjacent values of α, the lower classification accuracy is achieved. It is therefore expected that continuous values of α will lead to an infinite number of signal patterns, which will significantly decrease eavesdropping signal classification accuracy.

The single-band WDS framework might be designed with the following SB signal pattern.

$$\begin{cases} SB-OFDM \\ SB-SEFDM \quad (\alpha\text{=}0.95,\ 0.9,\ 0.85,\ 0.8,\ 0.75,\ 0.7) \end{cases}, \tag{47}$$

where the values in the bracket indicate the value of α for each signal class. The SB signal pattern has λ=7 signal classes and the BCF gap between adjacent classes is $\Delta\alpha$=0.05. Each signal class has 2,000 OFDM/SEFDM symbols and there are overall 14,000 symbols for the SB signal pattern neural network training.

In terms of multi-band signals, this work will select sub-band BCF β=0.9, 0.85, 0.8, which are a subset of the SB-SEFDM α pattern in (47). The bandwidth compression factor

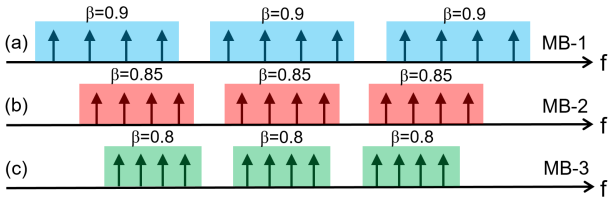

Fig. 8. Spectral packing characteristics for MB-SEFDM signal patterns. (a) MB-1. (b) MB-2. (c) MB-3.

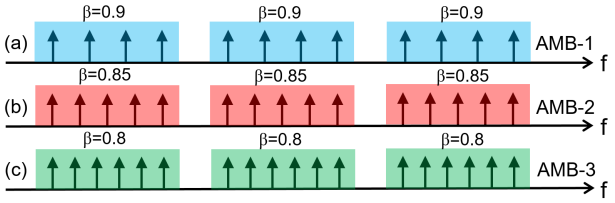

Fig. 9. Spectral packing characteristics for AMB-SEFDM signal patterns. (a) AMB-1. (b) AMB-2. (c) AMB-3.

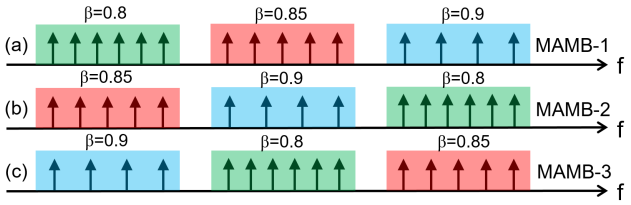

Fig. 10. Spectral packing characteristics for MAMB-SEFDM signal patterns. (a) MAMB-1. (b) MAMB-2. (c) MAMB-3.

and the number of sub-carriers for each multi-band signal architecture is configured as the following.

$$\begin{cases} MB-1 & (\beta\text{=}0.9,\ N_B\text{=}16) \\ MB-2 & (\beta\text{=}0.85,\ N_B\text{=}16) \\ MB-3 & (\beta\text{=}0.8,\ N_B\text{=}16) \end{cases}. \tag{48}$$

The MB-SEFDM signal pattern with λ=3 signal classes is designed in (48) and illustrated in Fig. 8, in which β=0.9, 0.85, 0.8 are allocated to Fig. 8(a), Fig. 8(b) and Fig. 8(c), respectively. Each sub-band has the same number of sub-carriers N_B=16 but the variations of β result in different spectral bandwidth. Each signal class has 2,000 symbols and there are overall 6,000 symbols for neural network training.

$$\begin{cases} AMB-1 & (\beta\text{=}0.9,\ N_B\text{=}16) \\ AMB-2 & (\beta\text{=}0.85,\ N_B\text{=}17) \\ AMB-3 & (\beta\text{=}0.8,\ N_B\text{=}18) \end{cases}. \tag{49}$$

The AMB-SEFDM signal pattern with λ=3 signal classes is designed in (49) and illustrated in Fig. 9. In order to have approximately similar occupied spectral bandwidth for each AMB signal, each sub-band in Fig. 9(a) with β=0.9 packs 16 sub-carriers, Fig. 9(b) and Fig. 9(c) should pack 17 and 18 sub-carriers, respectively. Each signal class has 2,000 symbols and there are overall 6,000 symbols for neural network training.

$$\begin{cases} MAMB-1 & (\beta\text{=}0.9,\ 0.85,\ 0.8,\ N_B\text{=}16,\ 17,\ 18) \\ MAMB-2 & (\beta\text{=}0.9,\ 0.85,\ 0.8,\ N_B\text{=}16,\ 17,\ 18) \\ MAMB-3 & (\beta\text{=}0.9,\ 0.85,\ 0.8,\ N_B\text{=}16,\ 17,\ 18) \end{cases}. \tag{50}$$

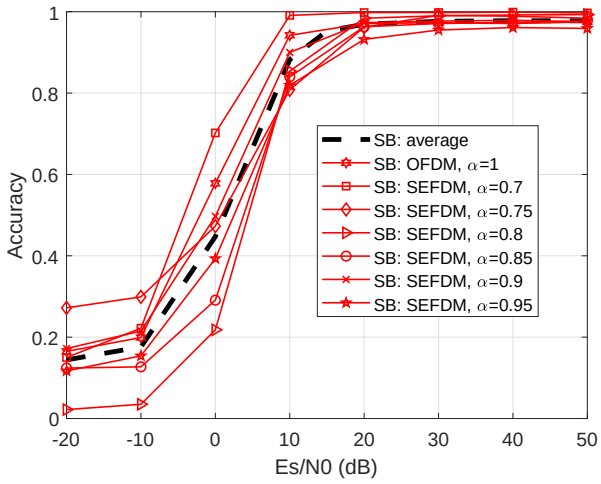

Fig. 11. Classification accuracy for SB based signal patterns and their average accuracy.

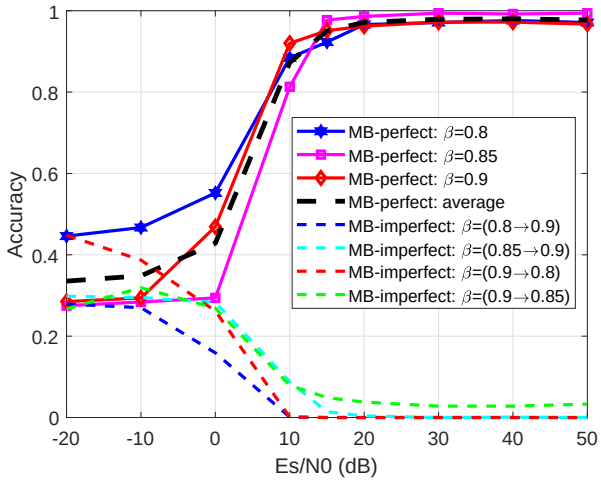

Fig. 12. Classification accuracy for MB based signal patterns and their average accuracy.

The MAMB-SEFDM signal pattern with λ=3 signal classes is designed in (50) and illustrated in Fig. 10. Similar to the AMB signal pattern, three different values of β are employed. However, different β would be mixed together in each signal class. Therefore, MAMB waveforms are similar to AMB waveforms in terms of occupied bandwidth but with different sub-band spectral features. The sub-band spectral ambiguity will cause misclassification at eavesdroppers. Each signal class has 2,000 symbols and there are overall 6,000 symbols for neural network training.

B. Performance and Processing Complexity

Due to the black-box learning mechanism of CNN, there is no analytical theory to justify the generality of the particular neural network in all security scenarios. To justify the feasibility of our trained CNN model in security analysis, we choose a benchmark for the reference. We firstly train a CNN

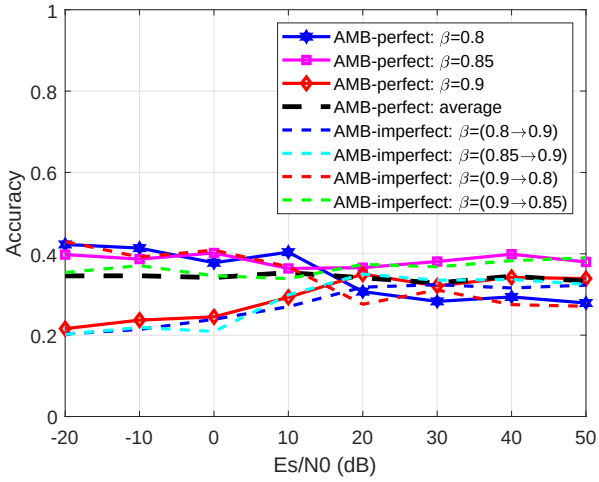

Fig. 13. Classification accuracy for AMB based signal patterns and their average accuracy.

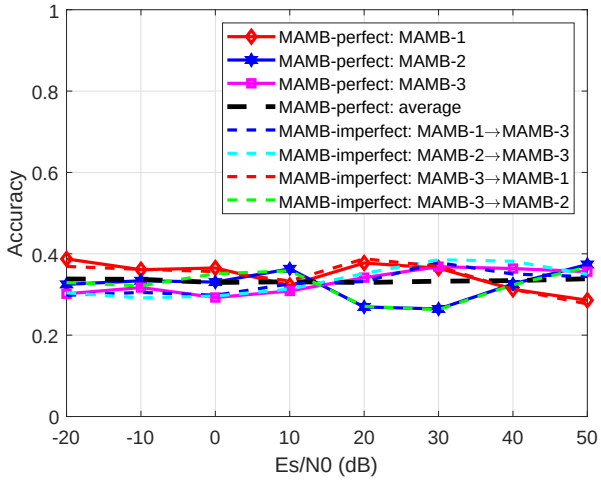

Fig. 14. Classification accuracy for MAMB based signal patterns and their average accuracy. The sub-band signal configuration follows the example in Table II.

model that can correctly classify the existing signal patterns. Then the CNN architecture will be re-trained for the newly proposed waveform scheme. In this case, we can have a fair justification that this particular CNN network is appropriate for the security analysis since the eavesdropping CNN model can eavesdrop conventional signals but it cannot identify the newly proposed signal patterns. Although an analytical justification is not available, the intensive training process for a CNN model results in time delay and will prevent eavesdropping in time-critical communications, which is a suitable application scenario that justifies the utility of our proposed framework.

The classification accuracy of single-band signal patterns is shown as a benchmark in Fig. 11, in which all the signals can be identified at nearly 100% accuracy rates with the increase of Es/N0. The classification accuracy results for multi-band signals are presented in Fig. 12. Since there is no need for OFDM signals using a multi-band signal architecture, OFDM is not considered in the MB scenario. As expected from Fig. 12, all the MB structured signals with perfect classification can converge to nearly 100% accuracy at high Es/N0 regime. The imperfect classification for the target signal β=0.9 is also evaluated. The notation, $\beta = (\beta_0 \rightarrow \beta_1)$, indicates an imperfect classification from a signal class of β_0 to another signal class of β_1. The imperfect classification accuracy shows a complementary trend relative to its perfect accuracy.

So far, both single-band and multi-band signal patterns are able to be identified by properly trained CNN classifiers. Compared to the single-band signal format, the multi-band signal architecture is a hardware-friendly signal format and its signal detection is implementable in hardware. However, they are both vulnerable to eavesdropping since eavesdroppers can apply deep learning to identify signals and employ proper algorithms to recover signals.

The classification accuracy for the AMB signal pattern is investigated in Fig. 13. As usual, both perfect and imperfect classification results are presented. Unlike the complementary results observed from Fig. 12, both perfect and imperfect

Table II: MAMB-WDS sub-band architecture (an example used in this work)

Sub-band Index	MAMB-1 β	MAMB-2 β	MAMB-3 β
0	0.90	0.80	0.85
1	0.80	0.90	0.85
2	0.85	0.80	0.90
3	0.90	0.90	0.80
4	0.90	0.85	0.90
5	0.80	0.90	0.85
6	0.85	0.80	0.90
7	0.80	0.80	0.90
8	0.90	0.85	0.80
9	0.85	0.85	0.85
10	0.90	0.80	0.80
11	0.85	0.90	0.85
12	0.90	0.85	0.85
13	0.80	0.90	0.80
14	0.85	0.80	0.90
15	0.80	0.85	0.80

classification accuracy rates are distributed around a static accuracy rate, 1/3. It is due to the fact that the three signal classes have strong feature similarity and each signal class would be equally classified into three signal classes resulting in the static 1/3 accuracy rate.

To enhance further the ambiguity of classifying AMB signal patterns, the mixed signal pattern MAMB from (50) is evaluated with classification accuracy presented in Fig. 14, in which three mixed signal patterns are designed with the BCF characteristics in Table II. The 256 sub-carrier MAMB signal is divided into 16 sub-bands and each sub-band is allocated with a specific sub-band BCF β and an associated number of sub-carriers. In this case, three MAMB signal patterns effectively have the similar occupied spectral bandwidth. It should be noted that the combination pattern of sub-bands is flexible and Table II only shows an example. It is clearly seen from Fig. 14 that due to the randomness of each sub-band features, the enhanced ambiguity complicates MAMB signal

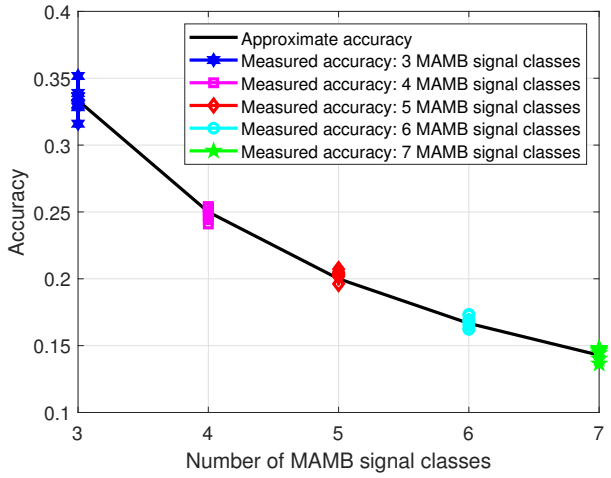

Fig. 15. Approximate accuracy and measured accuracy for MAMB signal patterns.

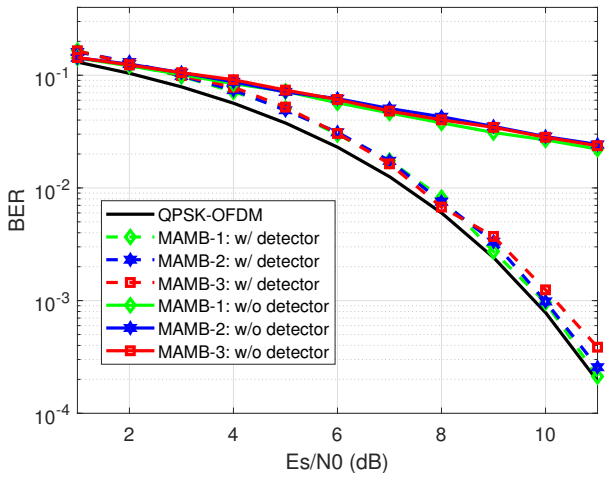

Fig. 16. BER performance for legitimate user MAMB signals with and without the uniquely designed SD detector.

classification resulting in the 1/3 accuracy rate at all Es/N0.

The results observed in Fig. 14 come with an assumption that the accuracy rate would be reduced further when more MAMB signal patterns are considered. The approximate accuracy rate to classify an arbitrary MAMB pattern is expressed in a mathematical model as

$$\psi = \frac{1}{\varpi}, \qquad \varpi \in [1, 2, 3, ..., b^{N/N_B}], \tag{51}$$

where ϖ indicates the number of MAMB signal classes, b represents the number of BCF candidates and N/N_B indicates the number of sub-bands. Considering the example from Table II, it is clear that the example has b=3 due to β=0.9, 0.85, 0.8 and N/N_B=16 sub-bands. Therefore, the maximum number of MAMB signal classes is $\varpi = 3^{16}$. In practice, the value of ϖ would be infinite since the value of b could be infinite due to continuous combinations of BCF. In addition, the number of sub-bands N/N_B is also flexible and the increase of the value will exponentially cut the classification accuracy rate.

Fig. 15 compares the approximate accuracy and measured accuracy for MAMB signal patterns with different number of signal classes. Each signal pattern is evaluated ranging from Es/N0=-20 dB to Es/N0=50 dB with a 10 dB increment step. Therefore, each signal pattern will show eight evaluation points in Fig. 15, in which it shows the reduction of classification accuracy with the increase number of signal classes. In addition, the measured accuracy reduction trajectory follows the accuracy approximation in (51) where the accuracy rate drops by 57% from three signal classes to seven signal classes.

In addition to the robustness evaluations of the WDS framework to prevent eavesdropping, Fig. 16 shows communication reliability at legitimate users as well. The MAMB signal pattern, with three signal classes, is selected for BER testing. The legitimate user will use pre-known pattern information to detect signals. It reveals that without a proper signal detector, where matched filter (MF) is applied, all the MAMB signal classes cannot be decoded resulting in high BER results. On the other hand, with the help of a uniquely designed detector,

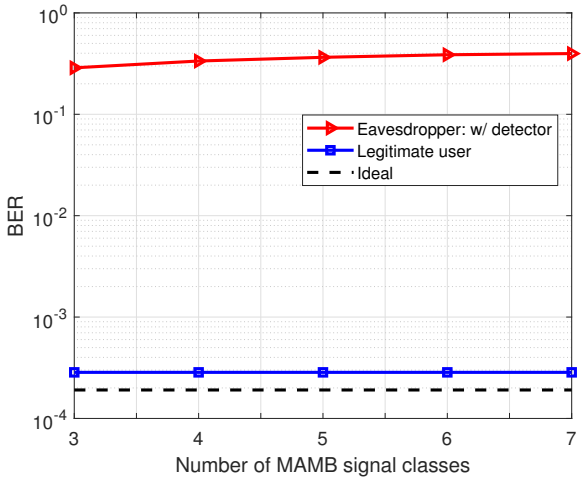

Fig. 17. BER performance for eavesdroppers with knowledge of the uniquely designed SD detector.

where the SD architecture from section III-A is applied for each signal sub-band, all the signal classes are detectable with similar performance to QPSK-OFDM. Based on the results in Fig. 16, it is inferred that even signals are correctly identified by eavesdroppers, they cannot decode signals properly when the uniquely designed SD detector is not known in advance.

To explore the eavesdropping capability on MAMB signals, Fig. 17 shows that the eavesdropping performance approaches a flat BER curve even the multiband SD detector is employed indicating a failure of eavesdropping. Based on the results in Fig. 17, it is inferred that even when the uniquely designed SD detector is known by eavesdroppers in advance, they cannot decode signals properly because signals are not correctly identified by eavesdroppers, which further enhances the physical layer communication security.

The signal processing complexity for WDS and multiband WDS frameworks is compared in Table III. The pattern key generation is one-time processing and is not taken into

Table III: Signal Processing Complexity Analysis (uplink channel from Alice to Bob)

Processing	WDS(Alice) User	WDS(Bob) Base Station	multi-band WDS(Alice) User	multi-band WDS(Bob) Base Station	WDS/multi-band WDS(Eve) Eavesdropper
Tx	IFFT(single)	-	IFFT(multiple)	-	-
Rx	-	FFT(single) Signal Detection	-	FFT(multiple) Signal Detection	FFT(single/multiple) Signal Classification Signal Detection

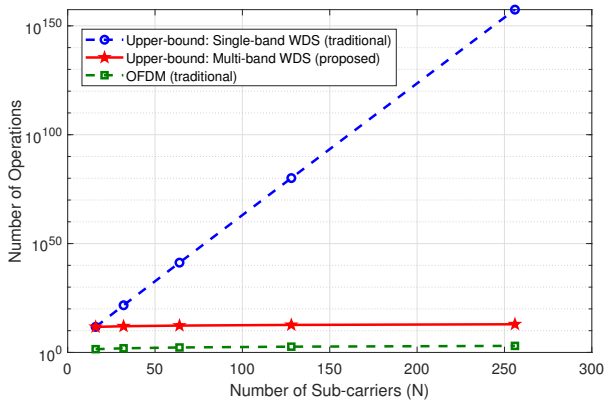

Fig. 18. The upper-bound of signal detection complexity in the number of real-valued multiplication operations.

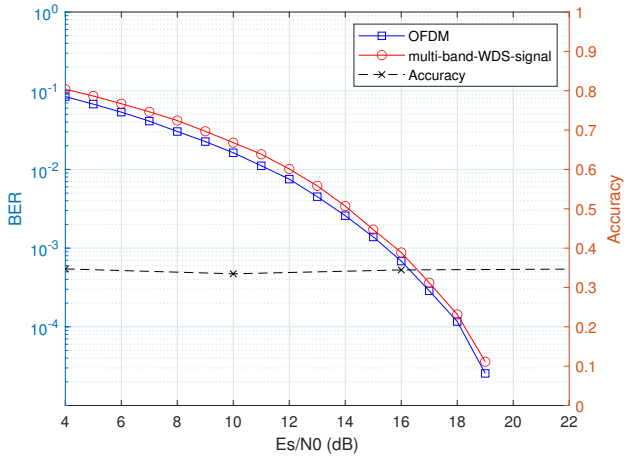

Fig. 19. BER performance and classification accuracy evaluations in multipath fading channels.

account. At the transmitter (Tx), the traditional WDS requires single IFFT while the proposed multi-band WDS requires multiple IFFTs. In terms of receiver side (Rx), both frameworks are for uplink channel communications where complex signal processing is at energy consumption insensitive base stations. Therefore, signal detection complexity is not the limitation to our proposed security framework. In summary, our proposed framework significantly reduces power consumption in Fig. 4 due to the reduced hardware utilization analysed in Table I.

Compared to traditional OFDM, our proposed waveform framework has increased spectral efficiency and higher data rate in a given bandwidth. It is because our proposed waveform framework can compress occupied spectral bandwidth and generate non-orthogonal waveforms. As a result, in a given spectral bandwidth, we can pack more sub-carriers for carrying data, leading to an increased data rate. The obvious limitation of our proposed approach, compared to OFDM, is the increased signal processing complexity at the receiver side, because the system requires complex signal detection algorithms to decode signals at legitimate users. We have implemented a similar signal detector in our previous work [53], which verifies that the data rate can be enhanced using optimized digital circuit design. To evaluate signal detection complexity, real-valued multiplication operations are considered. Since SD has variable computational complexity related to the level of noise power, this work will evaluate the upper-bound complexity. For traditional OFDM based systems, signal detection relies on MF, which is the fast Fourier transform (FFT) operation with the computational complexity of $(N/2)log2(N)$ multiplications. For the traditional single-band WDS framework, a single SD detector is required with the upper bound complexity of $\sum_{n=1}^{2N} 2^n[2n+1]$. For our newly proposed multi-band WDS framework, its signal detection has upper bound complexity of $\frac{N}{N_B}\sum_{n=1}^{2N_B} 2^n[2n+1]$. Fig. 18 clearly shows the complexity difference for the three waveform schemes. It is obvious that the newly proposed multi-band WDS framework has higher detection complexity compared to the traditional OFDM scheme but our proposal has significant complexity reduction compared to the single-band WDS framework.

It is noted that this work obtains the security enhancement capability using non-orthogonal signal waveform ambiguity rather than relying on channel variations. Our previous work [35] has verified that channels have minimal effects on classification since eavesdroppers fail to distinguish signals in both AWGN and wireless channels. For further information on the effect of channels, previous studies in [36], [54] have verified the feasibility of the non-orthogonal signals in practical experiment. To provide a comprehensive evaluation, we test our proposed signal scheme under the multipath fading channel model [36], [55], [56] where each path is configured to experience Rayleigh fading. In Fig. 19, our proposed multi-band WDS signal exhibits close BER performance to OFDM in multipath fading scenarios, suggesting that the proposed non-orthogonal signal can provide good BER performance in fading channels. Fig. 19 also demonstrates the classification accuracy at eavesdropper under multipath fading channels. It is evident that the accuracy is not obviously affected by channels, because the classification relies on waveform spectral ambiguity rather than channel variations.

We include the Masked-OFDM technique [33], the FTN-based technique [34], and the single-band SEFDM-based

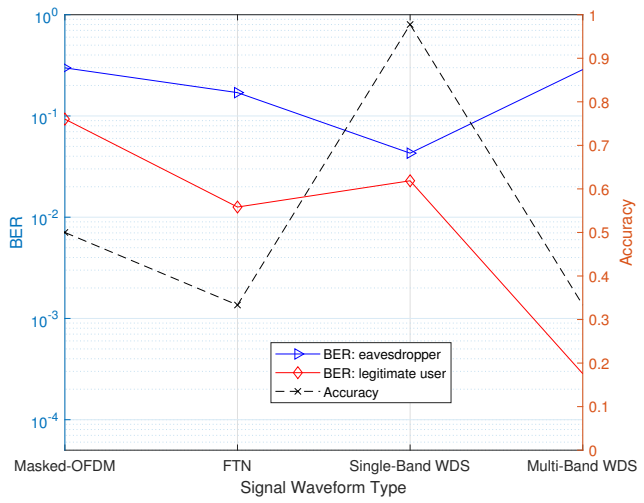

Fig. 20. Comparison with other waveform schemes in terms of classification accuracy, BER at legitimate users and eavesdroppers.

technique [35] for the comparison in this paper. All of these waveforms are incorporated into multicarrier formats similar to the multi-band WDS framework, and they all exhibit higher spectral efficiency compared to OFDM. The classification accuracy results reveal that the eavesdropper achieves the lowest accuracy (therefore better security performance) by our proposed multi-band WDS signal, while the eavesdropper attains the highest accuracy by the single-band WDS signal. For the other two signals, their accuracy is similar to that of the multi-band WDS signal. Concerning BER performance, the aim is to develop a framework that increases the eavesdropper's BER while simultaneously reducing the legitimate user's BER. Based on the results presented in Fig. 20, it is evident that our proposed multi-band WDS framework can meet both requirements while all other waveform candidates degrade both legitimate user and eavesdropper BER performance.

VII. Conclusion

This work investigated a multi-band waveform-defined security (WDS) framework, which avoids CSI at transmitters and can be jointly used with traditional PLS techniques. An adaptive multi-band WDS scheme is able to confuse eavesdropping signal identification since the designed signals occupy the same spectral bandwidth while their sub-band spectral characteristics are variable and unknown by eavesdroppers. With adaptive adjustment of each sub-band spectral feature, the eavesdropping accuracy drops to 33% when only three sub-band signal classes are taken into account. It is noted that spectral features for each sub-band are determined by sub-carrier packing patterns, which theoretically have an infinite number of combinations due to the continuous variations of the packing schemes. Therefore, the potentially infinite combinations of WDS patterns can efficiently prevent brute-force eavesdropping. An accuracy approximation model is derived to reveal that the eavesdropping accuracy will drop further when the number of feature combinations increases. Results show a nearly 57% accuracy drop when the number of combinations goes from three to seven. Signal BER performance is also evaluated and results show nearly perfect signal recovery with lower complexity relative to traditional PLS approaches.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[4] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[5] S. Cho, G. Chen, J. P. Coon, and P. Xiao, "Challenges in physical layer security for visible light communication systems," *Network*, vol. 2, no. 1, pp. 53–65, 2022.

[6] Z. Shaikhanov, F. Hassan, H. Guerboukha, D. Mittleman, and E. Knightly, "Metasurface-in-the-middle attack: From theory to experiment," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2022, pp. 257–267.

[7] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 2918–2931, 2018.

[8] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space-time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electronics*, vol. 4, pp. 827–836, 2021.

[9] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 335–343.

[10] J. S. Thompson, S. Fletcher, V. Friderikos, Y. Gao, L. Hanzo, M. Reza Nakhai, T. O'Farrell, and P. D. Wells, "Editorial a decade of green radio and the path to "net zero": A united kingdom perspective," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 2, pp. 657–664, 2022.

[11] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, and B. Ottersten, "Energy- and cost-efficient physical layer security in the era of IoT: The role of interference," *IEEE Communications Magazine*, vol. 58, no. 4, pp. 81–87, 2020.

[12] A. Mukherjee, "Physical-layer security in the Internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[13] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-cost security of IoT sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 327–340, 2018.

[14] Z. Wei, X. Zhu, S. Sun, Y. Huang, L. Dong, and Y. Jiang, "Full-duplex versus half-duplex amplify-and-forward relaying: Which is more energy efficient in 60-GHz dual-hop indoor wireless systems?" *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 12, pp. 2936–2947, 2015.

[15] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

[16] A. Ahmed, M. Zia, N. Bhatti, H. Mahmood, and H.-D. Han, "Higher secrecy capacity by successive pilot contamination and jamming cancellation," *IEEE Access*, vol. 10, pp. 132 040–132 048, 2022.

[17] Y. Tao, X. Wang, B. Li, and C. Zhao, "Pilot spoofing attack detection and localization with mobile eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 22, no. 3, pp. 1688–1701, 2023.

[18] O. L. A. Lopez, N. H. Mahmood, H. Alves, C. M. Lima, and M. Latva-aho, "Ultra-low latency, low energy, and massiveness in the 6G era via efficient CSIT-limited scheme," *IEEE Communications Magazine*, vol. 58, no. 11, pp. 56–61, 2020.

[19] M. Sadeghi and E. G. Larsson, "Adversarial attacks on deep-learning based radio signal classification," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 213–216, Feb. 2019.

[20] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," *CoRR*, vol. abs/1607.02533, 2016. [Online]. Available: http://arxiv.org/abs/1607.02533

[21] B. Flowers, R. M. Buehrer, and W. C. Headley, "Evaluating adversarial evasion attacks in the context of wireless communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1102–1113, 2020.

[22] M. Sadeghi and E. G. Larsson, "Physical adversarial attacks against end-to-end autoencoder communication systems," *IEEE Communications Letters*, vol. 23, no. 5, pp. 847–850, May 2019.

[23] A. Bahramali, M. Nasr, A. Houmansadr, D. Goeckel, and D. Towsley, "Robust adversarial attacks against DNN-based wireless communication systems," 2021, arXiv:2102.00918 [cs.CR].

[24] Q. Liu, J. Guo, C. Wen, and S. Jin, "Adversarial attack on DL-based massive MIMO CSI feedback," *Journal of Communications and Networks*, vol. 22, no. 3, pp. 230–235, 2020.

[25] B. R. Manoj, M. Sadeghi, and E. G. Larsson, "Adversarial attacks on deep learning based power allocation in a massive MIMO network," in *ICC-2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[26] Z. Luo, S. Zhao, Z. Lu, J. Xu, and Y. E. Sagduyu, "When attackers meet AI: Learning-empowered attacks in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2020.

[27] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems*, vol. 27. Curran Associates, Inc., 2014, pp. 2672–2680.

[28] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2020.

[29] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu, and J. H. Li, "Adversarial deep learning for cognitive radio security: Jamming attack and defence strategies," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[30] M. Z. Hameed, A. György, and D. Gündüz, "The best defense is a good offense: Adversarial attacks to avoid modulation detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1074–1087, 2021.

[31] E. Dahlman, S. Parkvall, and J. Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*. Elsevier Ltd., 2011.

[32] ——, *5G NR: The Next Generation Wireless Access Technology*. Academic Press, 2018.

[33] A. Chorti and I. Kanaras, "Masked M-QAM OFDM: A simple approach for enhancing the security of OFDM systems," in *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, Sep. 2009, pp. 1682–1686.

[34] M.-S. Baek, J. Yun, S. Kwak, H. Lim, Y. Kim, and N. Hur, "Physical layer security based on coded FTN signaling for premium services in satellite digital broadcasting system," in *2017 IEEE International Conference on Consumer Electronics (ICCE)*, 2017, pp. 147–148.

[35] T. Xu, "Waveform-defined security: A low-cost framework for secure communications," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 652–10 667, July 2022.

[36] T. Xu and I. Darwazeh, "Transmission experiment of bandwidth compressed carrier aggregation in a realistic fading channel," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4087–4097, May 2017.

[37] C.-L. I, S. Han, and S. Bian, "Energy-efficient 5G for a greener future," *Nature Electronics*, vol. 3, pp. 182–184, 2017.

[38] P. Skrimponis, S. Dutta, M. Mezzavilla, S. Rangan, S. H. Mirfarshbafan, C. Studer, J. Buckwalter, and M. Rodwell, "Power consumption analysis for mobile mmWave and sub-THz receivers," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[39] F. Hameed, O. A. Dobre, and D. C. Popescu, "On the likelihood-based approach to modulation classification," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5884–5892, 2009.

[40] J. L. Xu, W. Su, and M. Zhou, "Likelihood-ratio approaches to automatic modulation classification," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 4, pp. 455–469, 2011.

[41] T. J. O'Shea, T. Roy, and T. C. Clancy, "Over-the-air deep learning based radio signal classification," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168–179, Feb. 2018.

[42] T. Xu and I. Darwazeh, "Deep learning for over-the-air non-orthogonal signal classification," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.

[43] Z. Wei, C. Masouros, and F. Liu, "Secure directional modulation with few-bit phase shifters: Optimal and iterative-closed-form designs," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 486–500, 2021.

[44] L. N. Ribeiro, S. Schwarz, M. Rupp, and A. L. F. de Almeida, "Energy efficiency of mmWave massive MIMO precoding with low-resolution DACs," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 2, pp. 298–312, 2018.

[45] T. Xu, C. Masouros, and I. Darwazeh, "Waveform and space precoding for next generation downlink narrowband IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5097–5107, Jun. 2019.

[46] T. Xu, C. Masouros, and I. Darwazeh, "Design and prototyping of hybrid analogue digital multiuser MIMO beamforming for non-orthogonal signals," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1872–1883, Mar. 2020.

[47] B. Hassibi and H. Vikalo, "On the sphere-decoding algorithm I. expected complexity," *IEEE Transactions on Signal Processing*, vol. 53, no. 8, pp. 2806–2818, Aug. 2005.

[48] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1985.

[49] 3GPP TS 36.213 v.14.2.0, "LTE; evolved universal terrestrial radio access (E-UTRA); physical layer procedures," Rel. 14, Apr. 2017.

[50] 3GPP TS 38.212 v.15.2.0, "5G NR; multiplexing and channel coding," Rel. 15, Jul. 2018.

[51] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, 1976.

[52] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1524–1527, 1994.

[53] T. Xu, R. C. Grammenos, and I. Darwazeh, "FPGA implementations of real-time detectors for a spectrally efficient FDM system," in *ICT 2013*, May 2013, pp. 1–5.

[54] T. Xu, S. Mikroulis, J. E. Mitchell, and I. Darwazeh, "Bandwidth compressed waveform for 60-GHz millimeter-wave radio over fiber experiment," *Journal of Lightwave Technology*, vol. 34, no. 14, pp. 3458–3465, Jul. 2016.

[55] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 5, pp. 963–972, May 2005.

[56] Y. Ma, F. Tian, N. Wu, B. Li, and X. Ma, "A low-complexity receiver for multicarrier faster-than-Nyquist signaling over frequency selective channels," *IEEE Communications Letters*, vol. 24, no. 1, pp. 81–85, 2020.

Tongyang Xu (S'13-M'17) received the B.Eng. degree in electronic information engineering from Xidian University, Xi'an, China, in 2011, the M.Sc. degree (Distinction) in telecommunications, and the Ph.D. degree (Lombardi Prize) in electronic and electrical engineering from University College London (UCL), London, U.K., in 2012 and 2017, respectively.

He is currently a Lecturer (Assistant Professor) and the director of the Communications Systems Lab in the School of Engineering at Newcastle University. He is also the visiting lecturer in the Department of Electronic and Electrical Engineering at University College London (UCL). Dr Xu has published over 80 papers in high impact journals and conferences, as well as 2 invited book chapters, in the areas of signal waveform design, 5G/6G wireless and optical communications, machine learning, Internet of things, secure communications, sensing and communications, MIMO beamforming and transmission, software-defined radio, FPGA, and real-time testbed prototyping. He has more than 10 years of experience in 'Non-Orthogonal Signal' design and has developed a number of pre-commercialization hardware prototyping platforms. He is currently engaged in the intelligent design of advanced signal waveforms to achieve extremely high spectral efficiency for future 6G communication systems. He organised IEEE PIMRC 2020 and will be the TPC chair for IEEE ICT 2024. He is the Associate Editor of IEEE Wireless Communications Letter, and the Associate Editor of Journal Frontiers in Communications and Networks.

Zhongxiang Wei (S'15-M'17) received the Ph.D. degree in electrical and electronics engineering from the University of Liverpool, Liverpool, U.K., in 2017. From March 2016 to March 2017, he was a Research Assistant with the Institution for Infocomm Research, Agency for Science, Technology and Research, Singapore. From March 2018 to March 2021, he was a Research Associate with the Department of Electrical and Electronics Engineering, University College London. He is currently an Associate Professor with the College of Electronic and Information Engineering, Tongji University, China. He has authored or coauthored more than 80 research papers published on top-tier journals and international conferences. His research interests include anonymous communications, constructive interference designs, and MIMO communications. He has been a session/track chair of various international flagship conferences, such as IEEE ICC, GLOBECOM, and ICASSP, and a guest editor for IEEE INTERNET of THINGS JOURNAL. He was a recipient of the Shanghai Leading Talent Program (Young Scientist) in 2021, the Outstanding Self-Financed Students Abroad in 2018, and the A*STAR Research Attachment Program (ARAP) in 2016.

Tianhua Xu (M'17) received his PhD degree in School of Information and Communication Technology, at KTH Royal Institute of Technology, Sweden. His current research interests include optical communication systems and networks, intelligent signal processing, machine learning techniques, optical sensing systems and opto-electronics. He is a Senior Member of the American Physical Society (APS), a Fellow of the Higher Education Academy, and a Fellow of the Royal Statistical Society. He is an Associate Editor of IEEE Access and Journal of the European Optical Society-RP. He has been the Chair of Optics in Digital Systems Technical Group in Optical Society of America (Optica), and the TPC co-chair/members of over 20 IEEE conferences, e.g. GLOBECOM, ICC etc. He has received grants from EU Horizon 2020, EU Horizon Europe, the UK Royal Society, and UK National Grid. He has published over 160 journal and conference papers (including over 30 invited) and 2 invited book chapters.

Gan Zheng (S'05-M'09-SM'12-F'21) received the BEng and the MEng from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, in Electronic and Information Engineering, and the PhD degree in Electrical and Electronic Engineering from The University of Hong Kong in 2008. He is currently Professor in Connected Systems in the School of Engineering, University of Warwick, UK. His research interests include machine learning for wireless communications, reconfigurable intelligent surface, UAV communications and edge computing. He is the first recipient for the 2013 IEEE Signal Processing Letters Best Paper Award, and he also received 2015 GLOBECOM Best Paper Award, and 2018 IEEE Technical Committee on Green Communications & Computing Best Paper Award. He was listed as a Highly Cited Researcher by Thomson Reuters/Clarivate Analytics in 2019. He currently serves as an Associate Editor for IEEE Wireless Communications Letters and IEEE Transactions on Communications.