Waveform-Defined Security: A Low-Cost Framework for Secure Communications

Tongyang Xu, *Member, IEEE*

***Abstract*—Communication security could be enhanced at physical layer but at the cost of complex algorithms and redundant hardware, which would render traditional physical layer security (PLS) techniques unsuitable for use with resource-constrained communication systems. This work investigates a waveform-defined security (WDS) framework, which differs fundamentally from traditional PLS techniques used in today's systems. The framework is not dependent on channel conditions such as signal power advantage and channel state information (CSI). Therefore, the framework is more reliable than channel dependent beamforming and artificial noise (AN) techniques. In addition, the framework is more than just increasing the cost of eavesdropping. By intentionally tuning waveform patterns to weaken signal feature diversity and enhance feature similarity, eavesdroppers will not be able to identify correctly signal formats. The wrong classification of signal formats would result in subsequent detection errors even when an eavesdropper uses brute-force detection techniques. To get a robust WDS framework, three impact factors, namely training data feature, oversampling factor and bandwidth compression factor (BCF) offset, are investigated. An optimal WDS waveform pattern is obtained at the end after a joint study of the three factors. To ensure a valid eavesdropping model, artificial intelligence (AI) dependent signal classifiers are designed followed by optimal performance achievable signal detectors. To show the compatibility in available communication systems, the WDS framework is successfully integrated in IEEE 802.11a with nearly no adding computational complexity. Finally, a low-cost software-defined radio (SDR) experiment is designed to verify the feasibility of the WDS framework in resource-constrained communications.**

***Index Terms*—Waveform-defined security (WDS), waveform, encryption, secure communications, physical layer security, Internet of things, non-orthogonal, signal classification, deep learning, machine learning, software-defined radio.**

I. Introduction

SECURITY in communications is a hot research topic aiming to prevent confidential information leakage. The challenges of secure communications exist in various open systems interconnection (OSI) layers as explained in work [1]. The lowest layer is physical layer, which deals with radio signal transmission and reception. Since radio signals are commonly broadcasted over the air, therefore the physical layer is more vulnerable to eavesdropping.

Channel dependent defence strategies [2], such as millimeter wave, beamforming, artificial noise and directional modulation are proposed to mitigate unauthorized eavesdropping. These solutions intend to degrade performance at eavesdroppers by exploiting channel environments. However, unlike perfect channel state information (CSI) assumptions in theoretical simulations, imperfect or blind CSI [3] is a common situation in practical communications. Therefore, channel dependent physical layer security (PLS) solutions would be unreliable without accurate CSI. Beamforming has a potential beam leakage risk [4] due to imperfect beam shaping especially when legitimate users and eavesdroppers are spatially close. Moreover, beamforming does not work practically in long distance communications since radio beams would become wide at far field. Artificial noise [5] is regarded as an efficient solution but it wastes extra power on noise generation.

Internet of things (IoT) security [6] is challenging since IoT connects a massive number of devices with practical constraints such as low-cost hardware, low-power consumption, limited signal processing capability and small size on-board memory. Most of existing physical layer security techniques are initially designed for sophisticated systems and are not suitable for resource-constrained IoT. In IoT applications, most of the traffic occurs in uplink channels, which is from IoT devices to a central receiver. Due to limited size, limited complexity, limited power and low data rate requirements, each IoT device is typically equipped with a single antenna. In this case, a multiple input multiple output (MIMO) architecture [7] is not possible for IoT devices and therefore the traditional beamforming is not achievable. This is also the case for millimeter wave since sending a high frequency modulated signal would complicate each IoT device and consume more power. In addition, the accurate acquisition of legitimate instantaneous CSI at the transmitter (CSIT) [8] is not practical for resource-constrained IoT applications since frequently sending pilot symbols for channel estimation would reduce power efficiency and waste spectral resources. Furthermore, since eavesdroppers are normally external to IoT networks and would passively intercept signals [6], the location and CSIT of eavesdroppers are hardly to know by the transmitter. With the development of artificial intelligence (AI), deep learning based adversarial attacks [9], [10] are increasingly detrimental to communication security. This situation is more challenging in resource-constrained IoT applications since simple hardware architectures and software protocols cannot provide advanced countermeasures. All the mentioned challenges in resource-constrained IoT applications indicate the development of a new physical layer security framework.

This work proposes a waveform-defined security (WDS) framework, aiming to use a non-orthogonality concept in physical layer signal waveform to improve communication

T. Xu is with the Department of Electronic and Electrical Engineering, University College London (UCL), London, WC1E 7JE, UK (e-mail: tongyang.xu.11@ucl.ac.uk). This work was supported by the Engineering and Physical Sciences Research Council ”Impact Acceleration Discovery to Use” Award under Grant EP/R511638/1.

security. The fundamental waveform is based on spectrally efficient frequency division multiplexing (SEFDM) [11], [12], which intentionally creates inter carrier interference (ICI) via packing sub-carriers closer. The self-created interference complicates signal recovery but meanwhile increases the cost for eavesdropping. A similar concept was attempted by [13] via overlapping two orthogonal frequency division multiplexing (OFDM) signals to get a composite non-orthogonal signal. However, with the hardware advancement, brute-force maximum likelihood (ML) signal detection becomes realistic in low-cost hardware resulting in the security risk of eavesdropping.

Rather than a simple waveform design, the WDS framework designs a waveform tuning mechanism aiming to confuse eavesdroppers to misidentify signals. In this case, eavesdroppers can not recover signals even with the brute-force ML detector. Therefore, only the legitimate user who knows exactly the signal format can recover signals. The work in [14] initially revealed the feasibility of using the non-orthogonal SEFDM signal waveform in secure communications. However, further optimizations and practical experiments should be investigated to comprehensively verify the robustness of the framework.

The main contributions of this work are as the following.

- To deal with physical layer security in resource-constrained IoT, a WDS framework is proposed. WDS outperforms the recent PLS achievements in [15]. Firstly, WDS avoids CSIT leading to a simpler solution compared to beamforming and artificial noise. Secondly, the non-orthogonal waveform structure in WDS adds ICI leading to a more secure solution relative to OFDM. Thirdly, WDS only modifies waveform and thus its hardware is simpler than MIMO and millimeter wave solutions. Fourthly, WDS supports omni-directional communications while non-orthogonal multiple access (NOMA) is limited to protected zone due to potential eavesdropping successive decoding. Finally, WDS has higher spectral efficiency than channel coding schemes via compressing occupied spectral bandwidth.
- An efficient WDS waveform pattern is obtained after a joint study on three waveform tuning impact factors, namely training data feature, oversampling factor and bandwidth compression factor (BCF) offset.
- The WDS framework can be easily incorporated into existing communication standards such as wireless local area network (WLAN) IEEE 802.11a. A compatible WLAN-WDS frame is designed to preserve most of the original WLAN frame structure, which enables a straightforward deployment of the WDS framework in practice.
- A dual WDS security mechanism is designed. Firstly, the WLAN-WDS frame is so similar to the standard WLAN frame such that an eavesdropper would mistakenly decode WLAN-WDS frames using the standard WLAN protocol. Secondly, even the proper protocol is applied to decode WLAN-WDS frames, eavesdroppers cannot separate different signal patterns in the WDS framework, resulting in failed signal demodulation and detection.
- Low-cost software-defined radio (SDR) prototyping experiments are designed to validate the proposed WDS framework over the air. Experiments verify the feasibility of WDS framework in low-cost hardware and pave the way for applications in resource-constrained IoT scenarios. In addition, the experiments reveal the robustness of WDS framework even when eavesdroppers have advantages in signal power and channel conditions.

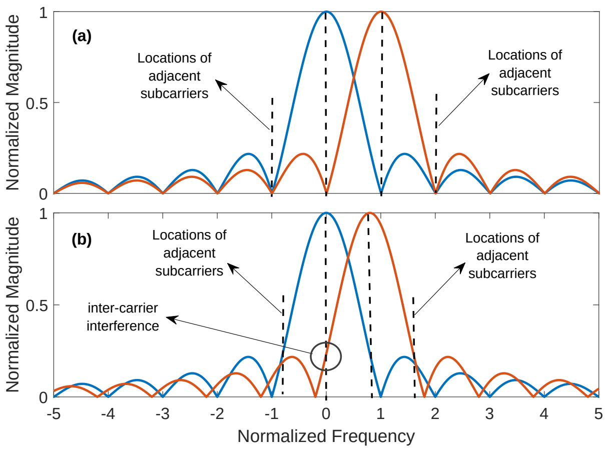


Fig. 1. Illustration of self-created inter carrier interference within SEFDM signal waveform. (a) OFDM sub-carrier packing. (b) SEFDM sub-carrier packing.

The rest of this paper is organized as follows. Section II will introduce the fundamentals of the waveform. In Section III, eavesdropping models applying maximum likelihood classifier, machine learning classifier and deep learning classifier, are investigated, followed by a brief description of signal detection. In Section IV, three waveform tuning impact factors, namely training data feature, oversampling factor and BCF offset, are studied to show their impacts on the WDS framework. A WLAN coexistent scheme is studied in Section V showing the compatible integration of the WDS framework. A low-cost experiment is implemented in Section VI to verify the feasibility of the proposed WDS framework in low-cost hardware, which further indicates its possibility in resource-constrained IoT applications. Finally, Section VII concludes the work.

II. Waveform Fundamentals

Non-orthogonal SEFDM waveform aims to compress signal spectral bandwidth while maintaining the same data rate. This is achieved by packing sub-carriers closer via breaking the orthogonality principle in OFDM. The graphic explanation of SEFDM waveform is illustrated in Fig. 1 where the same sub-carrier bandwidth is employed in OFDM and SEFDM except that the sub-carrier spacing in SEFDM is closer resulting in self-created ICI.

A simplified mathematical format of one SEFDM symbol is expressed as

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

where the parameters are defined as

- X_k, the time sample with the index of $k = 0, 1, ..., Q-1$.
- $Q = \rho N$, the number of time samples.
- N, the number of sub-carriers.
- ρ, the oversampling factor.
- $\frac{1}{\sqrt{Q}}$, the scaling factor.
- s_n, the n^{th} single-carrier symbol in one SEFDM symbol.
- $\alpha = \Delta f \cdot T$, the bandwidth compression factor where Δf is the sub-carrier spacing and T is the time duration of one SEFDM symbol.

ICI will be introduced when $\alpha < 1$. To mathematically show the impact of ICI, the instantaneous power for one SEFDM symbol, X_k, is computed as

$$\begin{aligned} |X_k|^2 &= \frac{1}{Q} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} s_n s_m^* \exp\left(\frac{j2\pi(n-m)k\alpha}{Q}\right) \\ &= \underbrace{\frac{1}{Q} \sum_{n=0}^{N-1} |s_n|^2 +}_{Signal} \\ &\underbrace{\frac{1}{Q} \sum_{n=0}^{N-1} \sum_{m\neq n, m=0}^{N-1} s_n s_m^* \exp\left(\frac{j2\pi(n-m)k\alpha}{Q}\right)}_{ICI}. \end{aligned} \tag{2}$$

The signal power representation includes a signal term and an ICI term. When $\alpha = 1$ for OFDM, the ICI term equals zero. However, for SEFDM signals with $\alpha < 1$, the ICI term is not cancelled, which is the main factor that enables the non-orthogonal waveform a candidate for physical layer security.

An inverse discrete Fourier transform (IDFT) architecture is applicable to SEFDM signal generation. The general idea has been implemented in very large scale integration (VLSI) [16] and successfully applied in practical experiments [12]. The basic principle is to pad zeros at the end of each vector s. Thus a longer symbol vector is achieved as

$$s_n^{'} = \begin{cases} s_n & 0 \le n < N \\ 0 & N \le n < M \end{cases}, \tag{3}$$

where $M = Q/\alpha$ should be rounded to its closest integer. The direct modulation in (1) is therefore transformed to a typical IDFT format as

$$X_k^{'} = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} s_n^{'} \exp\left(\frac{j2\pi nk}{M}\right), \tag{4}$$

where $n, k = [0, 1, ..., M-1]$. The output is 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 is given by

$$X = \mathbf{F}S = \underbrace{\mathbf{F}^{'}S^{'}}_{truncate}, \tag{5}$$

where X is a Q-dimensional vector of time samples, S is an N-dimensional vector of transmitted symbols and $\mathbf{F}$ is a $Q \times N$ sub-carrier matrix with elements equal to $\exp(\frac{j2\pi nk\alpha}{Q})$. $S^{'}$ is an M-dimensional vector of transmitted symbols and $\mathbf{F}^{'}$ is an $M \times M$ sub-carrier matrix with elements equal to $\exp(\frac{j2\pi nk}{M})$. It is noted that the symbol vector obtained from the second multiplicative term should be truncated to Q samples.

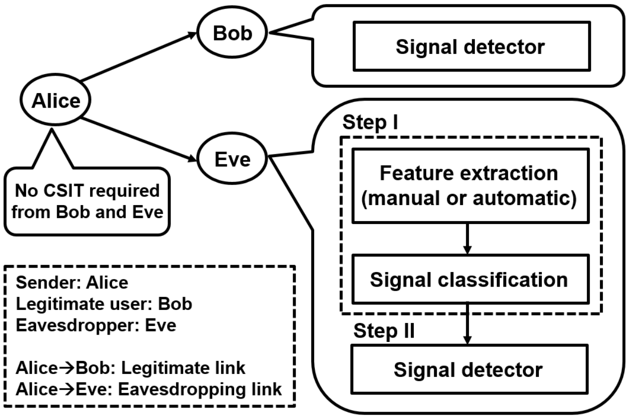

Bob
Signal detector
Alice
Eve
Step I
Feature extraction (manual or automatic)
Signal classification
Step II
Signal detector
No CSIT required from Bob and Eve
Sender: Alice
Legitimate user: Bob
Eavesdropper: Eve
Alice→Bob: Legitimate link
Alice→Eve: Eavesdropping link

Fig. 2. Waveform defined secure communication.

At the receiver side, the signal Y is obtained via additive white Gaussian noise (AWGN) channel as

$$Y = X + Z, \tag{6}$$

where Z is an Q-dimensional vector of noise samples. After signal demodulation via multiplying (6) with the conjugate sub-carrier matrix $\mathbf{F}^*$, an N-dimensional vector of demodulated symbols R is obtained as

$$R = \mathbf{F}^* X + \mathbf{F}^* Z = \mathbf{F}^* \mathbf{F} S + \mathbf{F}^* Z = \mathbf{C} S + Z_{\mathbf{F}^*}, \tag{7}$$

where $\mathbf{C}$ is an $N \times N$ correlation matrix defined as $\mathbf{C} = \mathbf{F}^* \mathbf{F}$. To recover original signals S from R, the ICI caused by the correlation matrix $\mathbf{C}$ has to be mitigated using specially designed signal detectors.

Similar to the operations in (3) and (4), a discrete Fourier transform (DFT) architecture is applicable to SEFDM signal demodulation. After padding zeros at the end of Y, a longer symbol vector $Y^{'}$ is therefore obtained with its elements defined below

$$y_n^{'} = \begin{cases} y_n & 0 \le n < Q \\ 0 & Q \le n < M \end{cases}. \tag{8}$$

The M-point DFT for SEFDM signal demodulation is thus given by

$$R_k^{'} = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} y_n^{'} \exp\left(\frac{-j2\pi nk}{M}\right), \tag{9}$$

where the output has to be truncated to Q samples similar to the operation in (4). In fact, to get the original symbol vector S, the output can be truncated to N symbols directly.

III. Eavesdropper Model

The proposed waveform based secure communication topology is presented in Fig. 2. As commonly defined, Alice is the information sender, Bob is the legitimate user and Eve is the eavesdropper. The eavesdropper Eve is configured to be passive in this work, which only listens to signals and would not actively manipulate legitimate signals. As shown in Fig. 2,

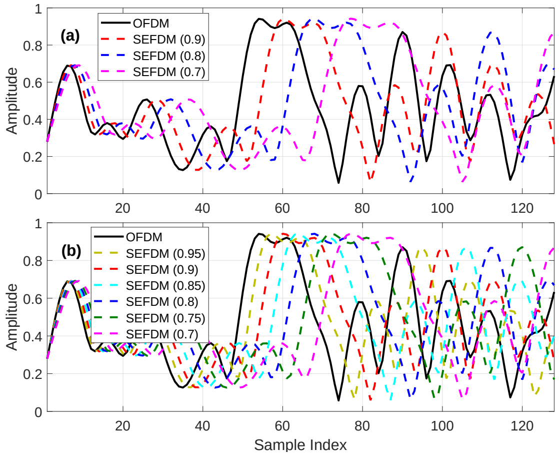


Fig. 3. Visualization of signal feature diversity and similarity via tuning SEFDM patterns. (a) Type-I signal pattern. (b) Type-II signal pattern. Values in the bracket indicate the bandwidth compression factor α. To have a fair illustration comparison, the same QPSK single-carrier symbols are modulated by both Type-I and Type-II signals. In the rest of this work, random QPSK symbols will be used for each signal.

there are two steps for a successful eavesdropping interception. Firstly, an eavesdropper should know the full information of signal formats. This could be achieved by manually or automatically extracting signal features followed by signal classification algorithms. Secondly, an efficient signal detector is required to recover signals based on the confirmed signal format from the first step. The specifically designed signal patterns, reused from [17], are illustrated in Fig. 3. The Type-I signal pattern has strong signal diversity since the feature difference between adjacent signals is obvious. However, the Type-II signal pattern shows closer BCF patterns and therefore strong signal feature similarity, resulting in more challenging signal classification at Eve. In terms of the legitimate communication link, the BCF pattern is pre-known between Alice and Bob. Therefore, Bob will not need signal classification and will go through signal detection straightforwardly. In practice, the BCF pattern could be privately pre-shared between Alice and Bob. Another solution could design a BCF pattern generator that can reproduce identical BCF patterns at Alice and Bob. This work will consider pre-known BCF knowledge and skip the BCF pattern synchronization between Alice and Bob.

Each signal type has multiple BCF patterns. Therefore, in either one communication session or different communication sessions, BCF patterns will be dynamically changed. In this case, each transmitted symbol will use a different BCF configuration and this random-like BCF transmission strategy will confuse eavesdroppers and enhance the security level of WDS.

It should be noted that Alice does not need any CSIT from Bob and Eve. The WDS secure communication framework is therefore less sensitive to channel environment variations and more robust than any other channel dependent physical layer security techniques. In addition, the avoidance of CSIT can simplify the entire system design, benefiting low-cost and resource-constrained communications.

A. Learning and Classification Strategies

Eavesdropping signal format classification models can be classified into maximum-likelihood based classifier, manual-feature based classifier and automatic-feature based classifier. Unlike the commonly used root mean square error (RMSE) metric in regression models, the performance of a classification model will be measured by accuracy rate, which is the ratio of the number of correct classifications to the total number of classifications.

The maximum-likelihood classifier provides an optimal solution. It was initially applied in modulation classification using single-carrier symbol-level likelihood functions [18], [19]. In an AWGN channel with perfect knowledge of all parameters except the modulation format, the likelihood function is expressed as

$$L(r|\mathfrak{M},\sigma)=\frac{1}{P}\prod_{n=0}^{N-1}\sum_{p=0}^{P-1}\frac{1}{2\pi\sigma^2}\exp\left(-\frac{|r(n)-\mathfrak{M}(i,p)|^2}{2\sigma^2}\right), \tag{10}$$

where $\mathfrak{M}$ indicates modulation candidates, $\mathfrak{M}(i,p)$ represents the p^{th} constellation symbol in the i^{th} modulation scheme. Each modulation scheme has up to P constellation symbols. N is the number of symbols for each observation, which indicates the number of sub-carriers in multicarrier signals. σ^2 is noise variance and $r(n)$ is the n^{th} single-carrier complex symbol.

The maximum-likelihood classification is to maximize the likelihood function among all the modulation candidates. Assuming the entire potential solution set is Θ, the maximum likelihood based solution $\hat{\mathfrak{M}}$ is give by

$$\hat{\mathfrak{M}}=\arg\max_{\mathfrak{M}(i)\in\Theta} L(r|\mathfrak{M},\sigma). \tag{11}$$

It is clearly seen from (10) and (11) that the maximum-likelihood classification is limited to single-carrier symbols. It is also well noticing that this work focuses on signal format classification rather than modulation classification. The latter one can straightforwardly use the optimal maximum-likelihood function. However, signal format classification is more complex since most of the signals are based on multi-carrier structures. Without an accurate signal format classification as the first step, the subsequent modulation classification [18], [19] will not be achievable. To convert a multi-carrier signal into its baseband single-carrier symbols, the multi-carrier signal format has to be known, which is the challenge to be solved in this section.

The optimality of non-orthogonal signal classification has not been mathematically achieved since the conventional maximum-likelihood function is not applicable to multicarrier signals. In addition, the continuous variations of BCF values can theoretically lead to infinite classification solutions. Therefore, this section investigates two alternatives, which can classify multicarrier signals using manual-feature machine learning and automatic-feature deep learning.

Manual-feature classifiers rely on manual feature extractions followed by traditional machine learning classification methods. Professional domain-knowledge has to be applied to manually extract features, which could be time-domain characteristics, frequency-domain characteristics, wavelet trans-

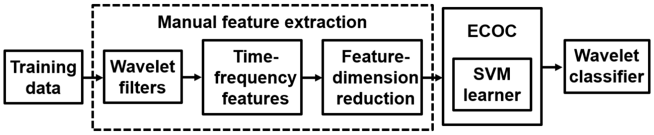


Fig. 4. Wavelet classifier training framework for the non-orthogonal signal classification.

formed time-frequency characteristics and other statistical characteristics. Commonly used machine learning algorithms for classification tasks are support vector machine (SVM), k-nearest neighbours (KNN), decision trees, naive Bayes and neural networks. Feature engineering is required to manually extract signal features at the first step. Previous work [20] revealed that wavelet time-frequency features with statistical feature dimensionality reduction schemes achieve the optimal classification accuracy. Therefore, the manual-feature classifier in this work will collect the dimensionality reduced wavelet time-frequency features for SVM classification.

The wavelet classifier training framework in this work is presented in Fig. 4 where time-frequency features are obtained after using multiple wavelet filters on the training data. Since the extracted time-frequency features are two-dimensional, a statistical based dimension reduction scheme is applied to convert the two-dimensional feature matrix into a one-dimensional feature vector. As verified by [20], the most efficient dimension reduction scheme relies on variance-interquartile-range statistical features. At the end, the error-correcting output codes (ECOC) model with SVM learners are used to train the wavelet classifier on the one-dimensional feature vector. It is clear that professional knowledge is required for the manual feature extraction process, which might be challenging for non-experts in this area. However, the manual feature extraction scheme will be more beneficial when the training data size is limited.

Automatic-feature classification, relying on deep learning, is becoming a popular approach to operate eavesdropping attack [9], [10] since deep learning can simplify the training process without any professional domain knowledge for feature extractions. However, a large amount of data will be required by deep learning to automatically learn signal features and output a signal classifier model. A representative deep learning based classifier is convolutional neural network (CNN) [21], in which it proved 20% higher modulation classification accuracy than traditional baseline classifiers. There are some other commonly used deep learning classification algorithms such as long short-term memory (LSTM) and Autoencoder. However, they both have limitations in flexible feature extractions. CNN is a general deep learning method for classification tasks. It was initially applied in image classification and was later used in communication signals since a complex signal can be converted into a two-dimensional image with separate real and imaginary signal parts. A deep CNN would consist of several convolutional layers that will be used to automatically learn hidden features in a more flexible way than LSTM and Autoencoder. In addition, the implementation of CNN is more efficient since multiple nonlinear filters can work in parallel. Therefore, this work will focus on the CNN method and skip other deep learning algorithms. Previous work [17] designed an efficient CNN classifier for different non-orthogonal signals. In this work, the neural network architecture will be reused to test the robustness of the proposed WDS framework.

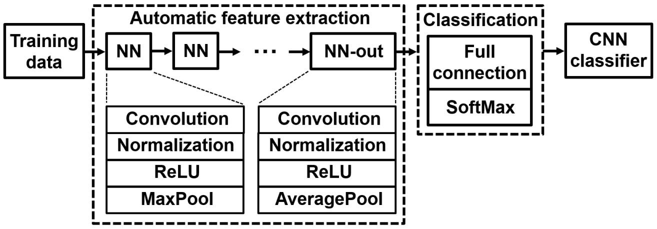


Fig. 5. CNN classifier training framework for the non-orthogonal signal classification.

The CNN neural network layer architecture in this work is presented in Fig. 5, in which multiple neural network (NN) modules are stacked to automatically learn signal features. There are additional sub-layers in each NN module, namely convolutional layer, Batch-normalization layer, ReLU layer and MaxPool layer. The last NN module is responsible for outputting features. Therefore, an AveragePool layer is applied instead of the MaxPool layer. The classification is operated using a full-connection neural layer with SoftMax outputs. The optimal CNN classifier will be trained and updated iteratively via minimizing the cross-entropy loss between predicted values and true values.

It should be noted that the investigated IoT system in this work only includes legitimate users Alice and Bob. Since the eavesdropper Eve is not a part of the IoT system, its computational complexity is not considered in this work. In addition, the aim of Eve is to exhaustively identify legitimate user signals. In this case, both the machine learning and deep learning algorithms in this work are applied only at Eve. Therefore, the computational complexity of intelligent signal classifiers has nothing to do with the IoT system.

B. Signal Detection

Signal detection is the second step of a complete eavesdropping, which aims to recover signals from ICI once signal formats are confirmed from the first step. The optimal detection algorithm is ML, which searches all possible solutions and determines the optimal one as

$$S_{ML} = \arg \min_{S \in O^N} \|R - \mathbf{C}S\|^2 , \tag{12}$$

where O is the constellation cardinality and O^N indicates the entire candidate solutions. By narrowing the search space, limited by a sphere radius g, the ML solution in (12) can be simplified into the sphere decoding (SD) solution [22] as

$$S_{SD} = \arg \min_{S \in O^N} \|R - \mathbf{C}S\|^2 \leq g, \tag{13}$$

$$g = \|R - \mathbf{C}S_{ZF}\|^2 , \tag{14}$$

where $S_{ZF} = \lfloor \mathbf{C^{-1}} R \rceil$ is a coarse solution based on zero forcing (ZF), which is used here to narrow the entire search space to a partial search space.

The SD detector is simplified relative to ML and it has been proved feasible in SEFDM signals with a large number of sub-carriers [23] and strong ICI. However, its computational complexity is random [24] and is highly related to noise power. Therefore, the work in [25] proposed a simplified interference cancellation method named iterative detection (ID), which can efficiently recover signals with minor ICI when the value of α is approaching one. The iterative cancellation is defined as

$$S_{\zeta} = R - (\mathbf{C} - \mathbf{e})S_{\zeta-1}, \tag{15}$$

where S_{ζ} is the N-dimensional symbol vector after ζ iterations, $S_{\zeta-1}$ indicates the results after $\zeta - 1$ iterations and $\mathbf{e}$ is an $N \times N$ identity matrix.

In summary, the ID detector shows lower computational complexity but it is limited to signals with weak ICI [25]. When signals have strong ICI (i.e. small α), the random-complexity SD has to be used. Therefore, the choice of a signal detector depends on signal conditions, which is determined by the value of BCF α.

IV. Impact Factor Investigations

This section evaluates three impact factors, which will determine the waveform characteristics and therefore affect eavesdropping signal classification accuracy. Channel and hardware impairments are considered for training datasets in this work. A three-path wireless channel power delay profile (PDP) with path delay (s) [0 9e-6 1.7e-5] and path relative power (dB) [0 -2 -10] are reused from [17], [20], [21], [26]. The K-factor is 4 and the frequency offset is configured to be 2 parts per million (PPM). The maximum Doppler frequency is set to 4 Hz considering indoor people walking speed. In addition, the training dataset will cover a wide range of Es/N0 from -20 dB to 50 dB. Signal specifications are flexible and will be detailed in each scenario below.

A. *Impact of Training Data*

In the previous work [17], training dataset is generated based on a data augmentation (DA) principle. This dataset generation mechanism aims at data-limited scenarios. The basic idea is to generate one data symbol, which will go through different feature-diversified wireless channels. The DA method will output multiple channel impaired symbols as a training dataset. Therefore, a symbol could be easily expanded to a large size dataset via time-variant wireless channels. Although the DA based dataset generation has wireless channel diversity, it has limited signal feature diversity. Such a diversity-limited dataset is efficient in machine learning based classifier training [20] where features are manually extracted using expert knowledge. However, it might not be efficient for deep learning based CNN classifier training [17] where a large amount of diversified data has to be used to automatically extract features.

The DA based training methodology is evaluated at the beginning. A source symbol is generated per signal class (i.e. per α). Each OFDM or SEFDM symbol will have 2048 time samples via oversampling 256 single-carrier QPSK symbols by a factor of ρ=8 [17], [20]. Each source symbol within a signal class will be expanded to 2,000 OFDM/SEFDM symbols by going through independent time-variant wireless channels defined at the beginning of this section. Therefore, the Type-I signal pattern will have four independent datasets consisting of overall 8,000 OFDM/SEFDM symbols. The same data generation principle is repeated for the Type-II signal pattern leading to seven datasets and overall 14,000 OFDM/SEFDM symbols. Based on the study in [20], the value of Es/N0 has great effects on the training efficiency where a dataset covering a wide Es/N0 range would train a high accuracy classifier. Therefore, prior to the classifier training, the raw dataset would be contaminated by AWGN ranging from Es/N0=-20 dB to 50 dB with an increment step of 10 dB. Such a dataset with rich AWGN information would help to train a robust classifier.

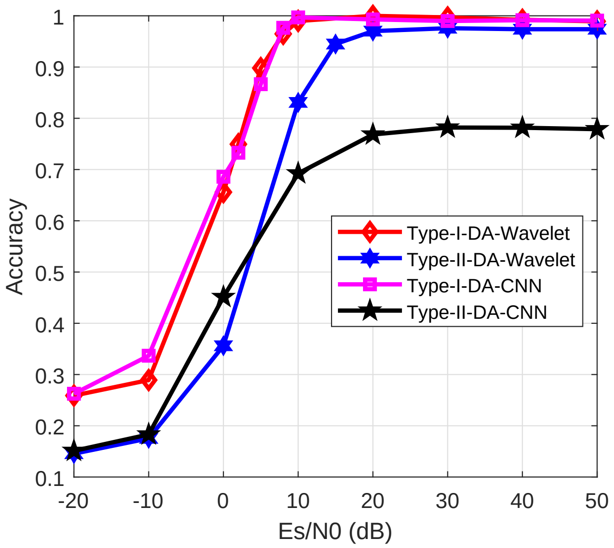


Fig. 6. Classification accuracy comparisons based on the data augmentation (DA) training methodology.

To evaluate the classification accuracy at eavesdroppers, the wavelet classifiers are trained based on [20] in Fig. 4 and the CNN classifiers are trained according to [17] in Fig. 5. The classification accuracy, based on the DA training data, is presented in Fig. 6. It should be noted that previous works in [17], [20] trained classifiers using the DA training data as well. Therefore, Fig. 6 summarizes what has been achieved in previous works and will be used as benchmarks for this work. It is clearly seen that both the CNN and wavelet Type-I signal classifiers perform well and reach 100% accuracy. For the Type-II signal pattern, the wavelet classifier maintains similar accuracy but the accuracy of the CNN classifier drops by at least 20%. This is expected because a diversity-limited dataset cannot efficiently assist CNN to automatically extract rich signal features while the manual feature extraction based wavelet classifier is not sensitive to the limited data diversity. It indicates that the DA based data generation is more suitable to wavelet classifier training.

To train a robust classifier for non-orthogonal waveforms, data diversity (DD) is enhanced via diversifying source data generation instead of the data augmentation. The basic princi-

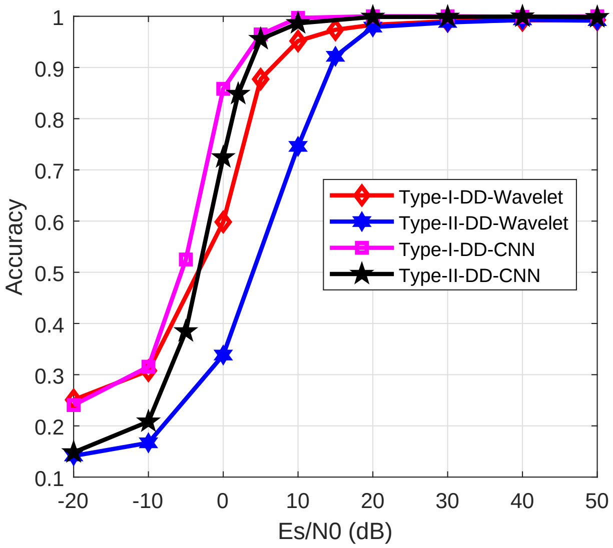


Fig. 7. Classification accuracy comparisons based on the data diversity (DD) training methodology.

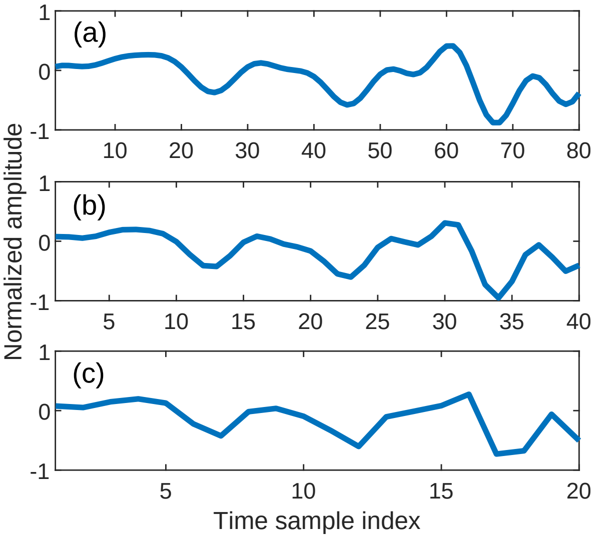


Fig. 8. Time-domain SEFDM sample (α=0.8) illustration to show the impact of oversampling on the same data. (a)ρ=8. (b)ρ=4. (c)ρ=2.

ple for DD is to generate multiple source symbols instead of a single source symbol in DA. Unlike the dataset expansion mechanism in DA, the enhanced feature of DD is that each source symbol will go through an independent channel. Therefore, the generated training dataset will have diversity both in source symbols and channel environments. This subsection will generate 2,000 OFDM/SEFDM source symbols per signal class and each source symbol will be distorted by an independent time-variant wireless channel. Therefore, each signal class will have 2,000 random OFDM/SEFDM symbols with random wireless channel distortions. In this case, both data and channel characteristics have diversity and would be fair to both machine learning and deep learning classifier training.

With the diversity enhanced dataset, both CNN classifiers and wavelet classifiers are re-trained following the same process in [17] and [20], respectively. The results in Fig. 7 reveal that both the CNN and wavelet classifiers can reach 100% classification accuracy at high Es/N0. It indicates that the DD based data generation is suitable to both CNN and wavelet classifiers training. Moreover, the CNN classifiers can even work well at low Es/N0. The significant achievement is at Es/N0=0 dB where the CNN based Type-II signal classification (72% accuracy rate) has approximately 38% higher accuracy than that of the wavelet Type-II signal classification (34% accuracy rate).

In summary, the typical machine learning based wavelet classification method is robust when training data is generated via augmenting a limited dataset. The deep learning based CNN classifier is however sensitive to training data and its classification accuracy drops with a diversity-limited training dataset. With a diversity enhanced dataset, both the CNN and wavelet based classifiers can identify Type-I and Type-II signals at 100% accuracy. Therefore, in the following, the DD based training data is used for both the CNN and wavelet classifiers while the DA based training data is merely for the wavelet classifiers.

B. Impact of Oversampling

Oversampling factor ρ in wired/wireless communications determines signal resolution. A higher value of ρ leads to a better signal resolution. In addition, it is also a method to introduce spectral protection guard band [27]. Previous works [17], [20] followed a large oversampling factor of ρ=8, which is more than the requirements in practical systems such as 4G-LTE [27], 5G-NR [28] and WLAN 802.11 [29]. Therefore, this section will study the oversampling impact on non-orthogonal signal classification.

An oversampling factor determines the number of samples per symbol, which is expected to have more impacts on SEFDM signals as shown in (2). It is clearly seen that the common signal term in either OFDM ($\alpha = 1$) or SEFDM ($\alpha < 1$) is only related to the raw single-carrier symbol s_n, which is independent from the oversampling factor ρ. The exponential term, $\exp(\frac{j2\pi(n-m)k\alpha}{Q})$, in the ICI part, is zero for OFDM when $\alpha = 1$. However, the term is not zero in SEFDM, which is determined by the factor ρ because of $Q = \rho N$. Therefore, the value of ρ will affect the accurate ICI expression and further determine the resolution of an SEFDM signal representation.

To have a general idea of the oversampling impact on SEFDM, a set of integer values, $\rho = 8, 4, 2$, are evaluated in Fig. 8. For the purpose of illustration, a total number of 20 time samples are truncated for the case of ρ=2. Based on this benchmark, a number of 40 time samples are truncated for the case of ρ=4 and 80 time samples for ρ=8.

The SEFDM signal of α=0.8, with an oversampling factor of ρ=8, is illustrated in Fig. 8(a). The time-domain sample waveform is smooth and indicates a sufficient signal resolution. With the reduction of an oversampling factor to ρ=4, the SEFDM signal resolution is reduced and its time-domain

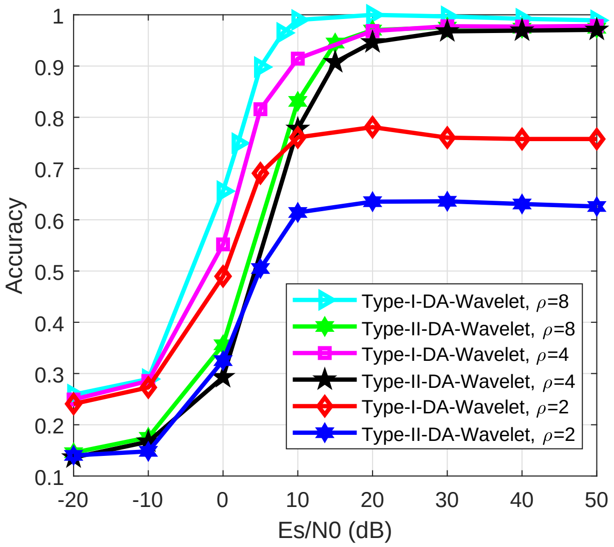


Fig. 9. Wavelet classification accuracy comparisons with various oversampling factors on the DA based training dataset.

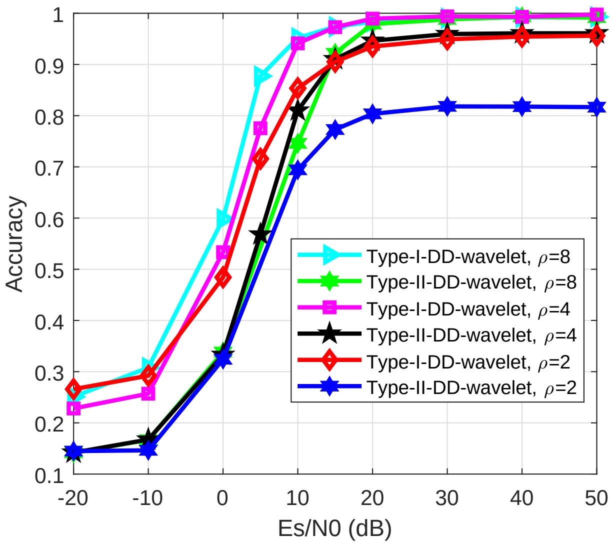


Fig. 10. Wavelet classification accuracy comparisons with various oversampling factors on the DD based training dataset.

waveform is slightly distorted in Fig. 8(b). Further reducing the oversampling factor results in Fig. 8(c). It is clearly seen that the signal shape is greatly changed and the signal profile is not following the one in Fig. 8(a). It is inferred that the reduction of an oversampling factor would have apparent effects on accurate SEFDM signal representations.

For Type-I and Type-II signals of ρ=8, 4, the DA based wavelet classification accuracy is between 95% and 100% as presented in Fig. 9. With a further reduced oversampling factor to ρ=2, the Type-I signal classification accuracy drops to 75% while the Type-II accuracy drops to 63%. This is due to the reduced SEFDM signal resolutions and therefore inaccurate ICI representations.

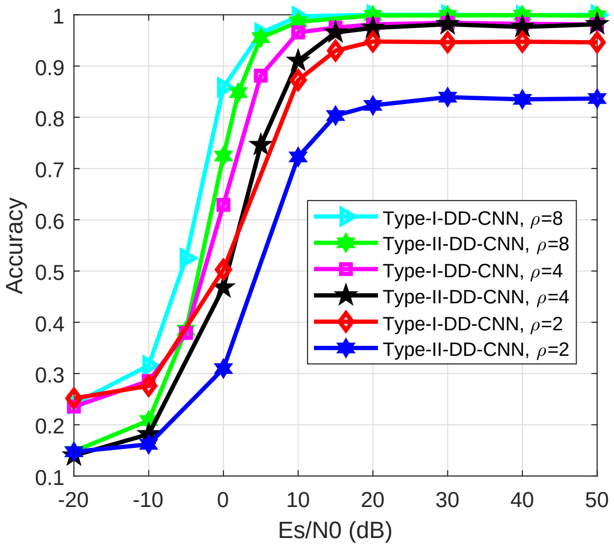


Fig. 11. CNN classification accuracy comparisons with various oversampling factors on the DD based training dataset.

The DD based wavelet classifier is tested with results showing in Fig. 10. A similar trend is observed for the cases of ρ=8, 4, where the accuracy is between 95% and 100%. However, data diversity can efficiently improve the classification accuracy for the case of using a small oversampling factor ρ=2. Results show that the Type-I signals can be identified with 95% accuracy and the Type-II signals with 82% accuracy. Comparing with the same oversampled signals in Fig. 9, the accuracy rates for the Type-I and Type-II signals are improved approximately by 27% and 30%, respectively. The results indicate that both the DD and DA training methodologies achieve similar classification performance when the oversampling factor ρ is large sufficient. However, when the oversampling factor ρ is small, the DD based training is more robust than the DA based training. Therefore, in the following studies, the DD training method will be used for wavelet classifiers training.

The CNN classifiers, trained by signals with different values of ρ, are evaluated in Fig. 11. The signals with large oversampling factors, ρ=8, 4, can achieve high accuracy between 97% and 100%. When the factor is reduced to ρ=2, the Type-I signal maintains a high accuracy at 95% while the Type-II signal accuracy drops to around 84%.

In summary, oversampling determines the number of samples used to represent one symbol and therefore determines the resolution of a signal. The level of oversampling affects accurate feature extractions and robust classifier training especially for non-orthogonal SEFDM signals. A large oversampling factor leads to a better training condition and therefore higher classification accuracy but at the cost of time sample redundancy. A small oversampling factor will save time sample resources, which is more realistic in practical communication systems. It should be noted that the accuracy degradation due to reduced oversampling will be an extra benefit to SEFDM signals in terms of secure communications.

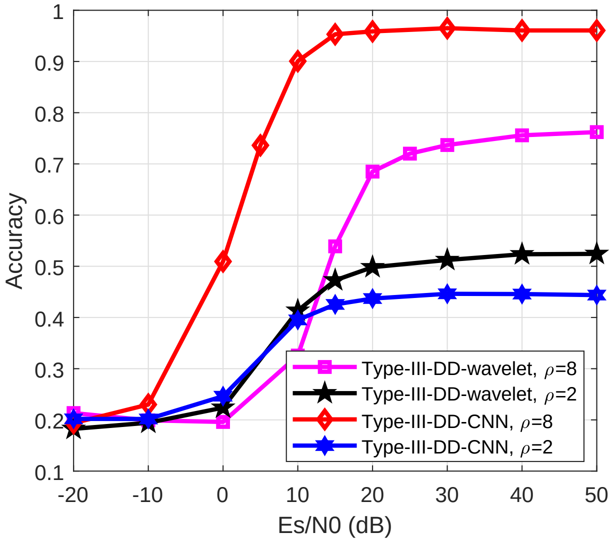


Fig. 12. Classification accuracy for the Type-III signal pattern.

For a comprehensive comparison, an upper-bound case of ρ=8 (following [17], [20]) and a lower-bound case of ρ=2 will be both considered in the following studies.

C. Impact of BCF Offset

Tuning the bandwidth compression factor will modify signal feature similarity and diversity. Previous work studied two types of signal patterns in [17]. As shown in Fig. 3, the Type-I signals with BCF offset $\Delta\alpha$=0.1 have a signal pattern of α=1.0, 0.9, 0.8, 0.7. The Type-I signals are easily identified by either CNN classifiers or wavelet classifiers. A more challenging scenario is the Type-II signal pattern where its BCF offset is $\Delta\alpha$=0.05, which results in a feature-similarity dominant scenario. With proper dataset training and symbol oversampling, the Type-II signals can be classified by both CNN classifiers and wavelet classifiers with results shown in Section IV-A and Section IV-B.

An inspiring enhancement approach for communication security is to narrow the BCF offset further and to have a more challenging feature-similarity dominant scenario. The tuning of BCF offset is flexible and has a number of patterns. This section will choose one pattern for an example demonstration. The optimal tuning pattern is not extensively investigated in this work. A signal pattern with BCF offset $\Delta\alpha$=0.015, termed Type-III, is designed in this section with bandwidth compression factors α=1, 0.985, 0.97, 0.955, 0.94. Fig. 12 will evaluate the Type-III signal pattern classification accuracy using the DD based training method and with ρ=8, 2.

It is clearly seen in Fig. 12 that with the sufficient oversampling ρ=8, the CNN classifier still achieves a high accuracy rate at around 96%. With the same oversampling, the wavelet classifier can only reach 76% accuracy. Reducing the factor to ρ=2, the accuracy rates of both the CNN and wavelet classifiers will drop to 52% and 44%, respectively.

In summary, a large value of BCF offset, such that in the Type-I and Type-II signal patterns, would simplify signal classification. However, a small value of BCF offset would challenge accurate signal identification. It is inferred that with a further reduction of BCF offset, an accurate signal classification would be impossible. In addition, oversampling has a greater effect on the Type-III signal pattern than the other two signal types.

V. WLAN Coexistence

WLAN is a ubiquitous technique being used in our daily life. Emerging data-hungry IoT applications are increasingly dependent on WLAN networks, such as remote monitoring, in which a large amount of video/voice data is generated and might be uploaded to the cloud. Typical narrowband IoT techniques such as ZigBee, LoRa, SigFox and NB-IoT would not be possible to achieve this. In addition, most narrowband IoT applications would require WLAN gateways to connect to the Internet. Therefore, the importance of WLAN in IoT applications is significant.

To show the coexistence capability of the WDS framework with existing communication systems, the Type-III signal pattern is integrated in the WLAN standard following IEEE 802.11a signal specifications [29]. By simply upgrading the IFFT signal generation methodology, the proposed WDS framework can be deployed straightforwardly in existing WLAN systems. It should be noted that this work considers coexistence of WDS frames and existing WLAN frames in a time-division multiplexing mode. Therefore, inter-band coexistence interference is not introduced in this work. For complex scenarios when WDS frames and WLAN frames are working in a frequency-division multiplexing mode, inter-band coexistence interference will appear. Previous work in [30] has studied its impact and research results verified that the inter-band interference can be mitigated by using coding schemes. Due to limited space, this work will merely consider the basic scenario when WDS frames and WLAN frames are working in a time-division multiplexing mode, which has no coexistence interference.

A. WDS Framework in IEEE 802.11a

IEEE 802.11a has a unique signal structure, which consists of 48 data symbols and 4 pilot symbols. With a fractional oversampling factor of ρ=16/13, the IFFT size is 64. It is clear that the IFFT size in 802.11a is smaller than that of the previous simulations in Section IV. The smaller oversampling factor will additionally enhance communication security as proved by Section IV-B.

As clarified in (4), the typical SEFDM signal is implementable by IFFT. Therefore, the SEFDM signal generation is highly coexistent with the 802.11a standard via merely modifying the length of IFFT. At the receiver, an FFT is also applicable to match the transmitter side architecture. All other signal processing and system architectures maintain the same with 802.11a. In this case, SEFDM signal generation and reception are highly compatible with the standard WLAN framework.

The 802.11a frame structure is presented in Fig. 13(a). The entire frame is termed physical layer conformance procedure

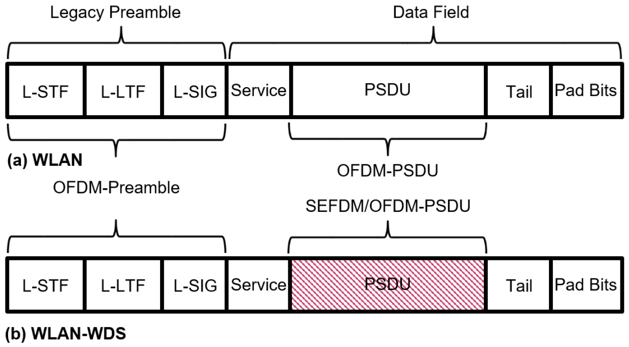


Fig. 13. The design of WDS signal frame coexisting with the standard WLAN 802.11a. (a) Typical WLAN 802.11a frame. (b) Proposed WLAN-WDS frame.

(PLCP) protocol data unit (PPDU) [29], which includes legacy preamble and data field. The legacy preamble, consisting of legacy short training field (L-STF), legacy long training field (L-LTF) and legacy signal (L-SIG) field, is used for frequency compensation, phase correction, timing synchronization, channel estimation, automatic gain control (AGC) adjustment, modulation and coding scheme (MCS) notification, etc. The PLCP service data unit (PSDU) in the data field is responsible for carrying data symbols.

To have a high compatibility with 802.11a, only the PSDU field will be replaced by the Type-III pattern signals and any other fields will be maintained as the 802.11a standard. In this case, the modification to the existing 802.11a standard is minor. Unlike the conventional WLAN frame including OFDM-preamble and OFDM-PSDU, the newly designed WLAN-WDS frame will consist of OFDM-preamble and Type-III pattern based SEFDM/OFDM-PSDU.

Once a WLAN-WDS frame is received, an eavesdropper will have two possible actions to recover signals. In Scenario-I, Eve will mistakenly assume that all captured frames are defined by the traditional WLAN 802.11a standard as shown in Fig. 13(a). This makes sense because a WLAN-WDS frame reuses the WLAN legacy preamble as shown in Fig. 13(b), which would give a wrong indication that the following PSDU is also specified by 802.11a. Therefore, the mismatch between the information extracted from the legacy preamble and the PSDU data will confuse Eve to mistakenly use the typical 802.11a standard to recover the WLAN-WDS PSDU field even the data field PSDU is actually modulated by mixed SEFDM/OFDM symbols. The incorrect PSDU demodulation will significantly affect signal detection. In Scenario-II, the eavesdropper is assumed to realize the unique PSDU pattern in WLAN-WDS frames. However, the eavesdropper cannot easily recognize the difference between SEFDM-PSDU and OFDM-PSDU since an efficient signal classifier is not available. Therefore, the subsequent signal detection will not be reliable.

A list of terms are defined below and will be used in the following simulation and experiment.

- WLAN-OFDM: OFDM symbols are generated for PSDU following the 802.11a standard, which has 48 data symbols, 4 pilot symbols, 64 time samples and ρ=16/13.
- WLAN-SEFDM: SEFDM symbols are generated for PSDU following the 802.11a standard, which has 48 data symbols, 4 pilot symbols, 64 time samples and ρ=16/13.
- WLAN-WDS: the WDS framework is integrated in the standard WLAN frame, as shown in Fig. 13(b).
- WLAN-Type-III: the Type-III signal pattern, consisting of WLAN-OFDM and WLAN-SEFDM, is applied to the PSDU field in an WLAN-WDS frame.

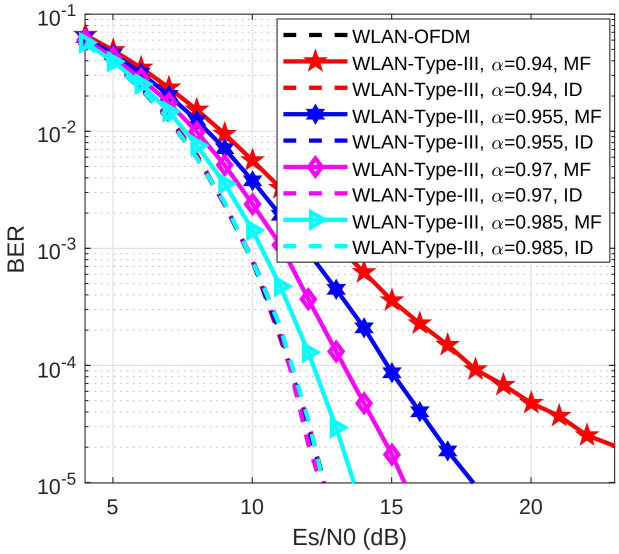


Fig. 14. BER performance of detecting WLAN-Type-III signals at the legitimate user.

B. Reliability and Security

According to the available physical layer security experiment research in [4], [31], [32], [33], the commonly used security metrics are signal power difference and bit error rate (BER). It is well noticing that the security enhancement of the proposed WDS framework is not dependent on the signal power advantage of legitimate communication links over eavesdropper communication links. The aim of the framework is to confuse eavesdroppers. Therefore, an eavesdropper will not break the communication security even its received signal power is higher than the legitimate user. In this case, instead of considering the signal power difference between legitimate users and eavesdroppers, this work will use BER as one metric to evaluate the communication security. Additionally, a specific metric, termed confusion matrix, is also applied in this work. Unlike the average accuracy results on entire signal classes in Section IV, a confusion matrix can tell the details of classification for each signal class.

This section focuses on the feature-similarity dominant Type-III signal pattern. As explained in Fig. 2 that the legitimate user Bob knows accurate signal formats based on pre-shared information. Therefore, Bob can decode signals without the first-step signal classification. Based on the descriptions in Section III-B, the simple ID signal detector is sufficient to recover non-orthogonal signals when the self-created ICI is not

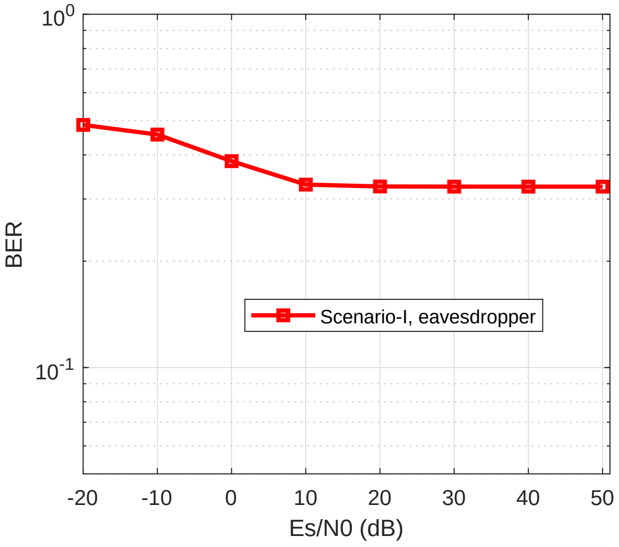


Fig. 15. Scenario-I: BER performance of detecting WLAN-Type-III signals at the eavesdropper when received symbols are incorrectly demodulated and detected following the WLAN-OFDM specification.

Table I: CNN classifier neural network layer architecture

Layers	Dimension
Input layer	2 × 64
Convolutional layer-1	2 × 64 × 64
Convolutional layer-2	2 × 32 × 64
Convolutional layer-3	2 × 16 × 64
Convolutional layer-4	2 × 4 × 64
Convolutional layer-5	2 × 2 × 64
Full-connection layer	2 × 1 × 64
SoftMax output layer	1 × 1 × 5

strong. Since the minimum bandwidth compression factor in the Type-III signal pattern is α=0.94, therefore the ID detector is sufficient. The BER performance for the signals at legitimate user Bob is presented in Fig. 14. It is clearly seen that using the typical matched filter (MF) detector, performance loss will exist and the signal with α=0.94 has the worst performance. On the other hand, all the signals can be recovered perfectly by ID detectors leading to identical performance with the WLAN-OFDM signal. This indicates the WDS framework reliability at a legitimate user when the ID detector is applied.

In terms of BER performance at Eve, there are two possible eavesdropping scenarios considering the use of the proposed WLAN-WDS frame in Fig. 13(b). To test the BER performance, a total of 5,000 OFDM/SEFDM symbols are generated and each signal class has 1,000 symbols.

In Scenario-I, all the symbols will be incorrectly demodulated based on WLAN-OFDM specifications. The improper operation from Eve results in extremely degraded BER in Fig. 15. It is seen that the result of Scenario-I converges to a flat BER curve when Es/N0 is increased, which indicates a failure of eavesdropping.

In Scenario-II, it is assumed that Eve will notice the tricks of the WLAN-WDS PSDU and will apply signal classifiers to identify each signal format. Following the same training methodology in Fig. 5, a CNN classifier is re-trained for the WLAN-Type-III signals with the neural network architecture presented in Table I where five convolutional layers are stacked. A wavelet classifier is re-trained following Fig. 4 based on the manually extracted variance-interquartile-range features and the ECOC model with SVM learners.

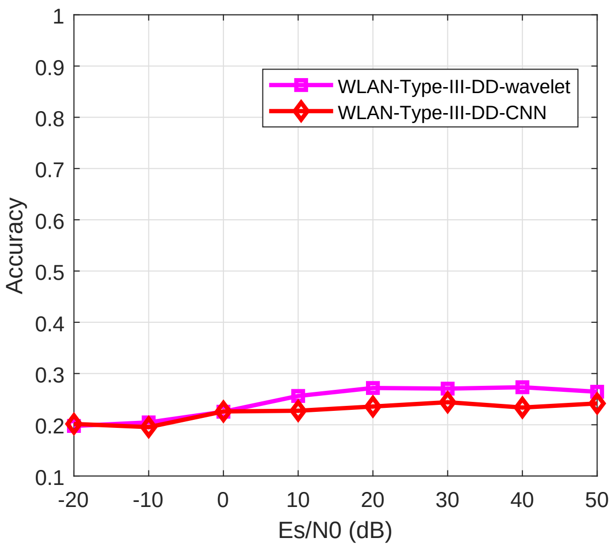


Fig. 16. WLAN-Type-III signal classification at the eavesdropper.

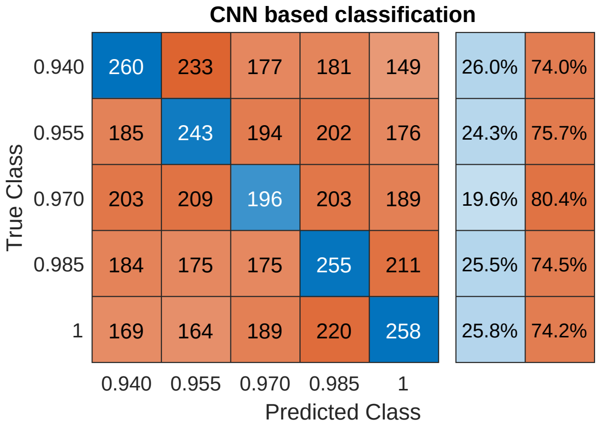
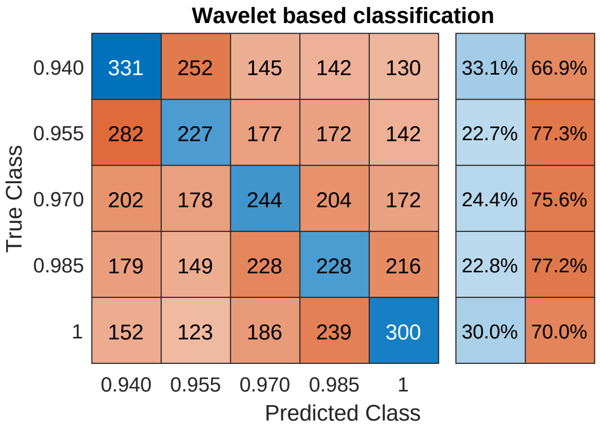


Fig. 17. Confusion matrix of WLAN-Type-III signals CNN classification at Es/N0=20 dB. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

The classification accuracy for the WLAN-Type-III signal pattern is shown in Fig. 16. It is clearly seen that when applying WLAN-Type-III structured signals with an oversampling factor ρ=16/13, both the CNN and wavelet classifiers cannot identify signals properly with only 24% and 27% accuracy, respectively. The reduced accuracy is expected since Fig. 12 has verified that a small oversampling factor will degrade classification accuracy.

The detailed results of classification can be expressed in the format of confusion matrix, in which diagonal elements indicate perfect classification while any non-diagonal elements indicate misclassification. A confusion matrix commonly uses



True Class \ Predicted Class	0.940	0.955	0.970	0.985	1		
0.940	331	252	145	142	130	33.1%	66.9%
0.955	282	227	177	172	142	22.7%	77.3%
0.970	202	178	244	204	172	24.4%	75.6%
0.985	179	149	228	228	216	22.8%	77.2%
1	152	123	186	239	300	30.0%	70.0%

Fig. 18. Confusion matrix of WLAN-Type-III signals wavelet classification at Es/N0=20 dB. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

different coloured grids to give, at first glance, a general idea of correct classification and incorrect classification. However, a more scientific approach is to examine the values in each coloured grid. The values in each diagonal grid indicate the number of correctly identified symbols while other values indicate incorrectly identified symbols. In addition, a separate percentage table is jointly presented, in which the first column represents correct classification accuracy rates and the second column represents incorrect classification accuracy rates. The CNN based confusion matrix is presented in Fig. 17. The values on the vertical axis indicate BCF for true signal classes while the horizontal axis shows predicted signal classes. The average accuracy for each signal class is between 19.6% and 26%. It is clearly seen that only 25.8% of transmitted WLAN-OFDM signals are properly classified. A similar result for wavelet classification is illustrated in Fig. 18 where the average accuracy is ranged from 22.7% to 33.1%. In terms of the WLAN-OFDM signal, its correct classification is at 30%. Most of the misclassified WLAN-OFDM signals are concentrated in its adjacent signal class, α=0.985. This is due to the fact that the WLAN-SEFDM signal of α=0.985 is more similar to the WLAN-OFDM signal than any other WLAN-SEFDM signals. In this case, misclassification is unavoidable and communication security is beneficially enhanced.

The performance evaluation of Scenario-II is more complex than that of Scenario-I. As shown in Fig. 17 and Fig. 18, each confusion matrix has 25 possible classification mapping schemes. Each mapping, either correct or incorrect, will indicate one signal recovery scheme. Therefore, there are overall 25 signal recovery schemes per confusion matrix. One signal recovery scheme includes signal demodulation and signal detection. The function of one complete recovery process is to demodulate and detect true class labelled signals using predicted class labels. To get a general idea of the performance, a single BER result is obtained by averaging the 25 possible results per confusion matrix. Therefore, for either the CNN classifier or the wavelet classifier, a total of eight BER results will be obtained when considering Es/N0 from -20 dB to 50 dB with a 10 dB increment step.

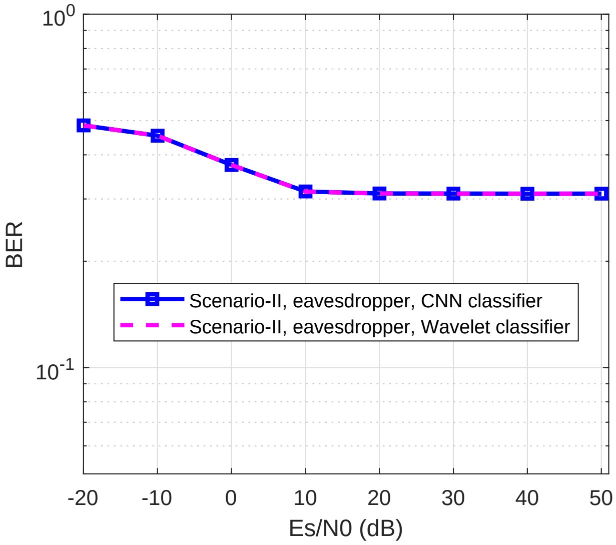


Fig. 19. Scenario-II: BER performance of WLAN-Type-III signals at the eavesdropper when received symbols are incorrectly demodulated and detected following the confusion matrix classification mapping scheme.

Prior to the BER calculation, multiple confusion matrices should be obtained at Es/N0=-20 dB:50 dB. Due to the limited space, this work merely presents the confusion matrices at Es/N0=20 dB in Fig. 17 and Fig. 18. The final BER of Scenario-II will consider all the confusion matrices Es/N0=-20 dB:50 dB leading to Fig. 19. The results show clearly that without an accurate classifier, which is currently unachievable, the eavesdropper cannot properly recover signals.

It reveals that the WDS framework in WLAN maintains the legitimate user side reliability using a specially designed signal detector. In addition, the joint study of confusion matrix and BER verifies that the framework enhances security by confusing an eavesdropper in two possible scenarios.

C. Complexity Analysis

The complexity of WDS framework should be evaluated comprehensively. It can be divided into signal processing complexity and hardware architecture complexity.

WDS signal processing includes signal generation, signal classification and signal detection. Taking Fig. 2 as an example. Alice is responsible for signal generation. Bob will use the ID detector to recover signals. Eve will need signal classification and signal detection. Since the purpose of Eve is to exhaustively recover signals without considering power/resource consumption, therefore the complexity at Eve is ignored in this work. In principle, the higher eavesdropping computational complexity the better security level for the proposed WDS framework.

Unlike typical WLAN communications where more traffic happens at downlink, IoT based applications would generate more traffic at uplink. In this case, the signal generation at Alice who is functioned as an IoT user, will be more concerned in this work. The signal detection at Bob, which would be at a WLAN router, is not considered. The reason is that WLAN routers are powered via wires and power consumption or computational complexity is not very crucial to the implementation of WDS. Therefore, the computational complexity in this section focuses merely at an IoT user side. In terms of the downlink channel from a WLAN router to an IoT device, the original 802.11a standard will be used in order to maintain simple signal processing at an IoT device. Since an IoT downlink channel is responsible for crucial control instructions that will determine the working principle for each IoT device, the WDS framework is also applicable but at the cost of extra signal processing power consumption from the non-orthogonal ID signal detector. Therefore, the deployment of WDS is flexible and its computational complexity is related to applications and downlink/uplink channels.

In terms of hardware architectures, unlike MIMO beamforming requiring multiple RF chains; millimeter wave requiring high frequency modulators; directional modulation requiring unique antennas; artificial noise requiring beamforming and power allocation, the proposed waveform-defined security framework can use available hardware and will not require additional hardware resources. Therefore, the hardware complexity of WDS is identical to the typical WLAN configurations. In this case, hardware complexity is not considered in this section.

The WDS computational complexity is thus analyzed merely on the digital signal generation. As explained in [34], by using the framework of Fastest Fourier Transform in the West (FFTW), the asymptotic computational complexity of IDFT is $\mathcal{O}(\xi \times log_2\xi)$ when the transform size is ξ. It is well noticing that FFTW works well when the value of ξ is either a power of two or a prime number. Therefore, considering the IDFT-based signal generation with Q samples, the complexity of OFDM signal generation is

$$\mathcal{O}(Q \times log_2 Q). \tag{16}$$

In terms of SEFDM signal processing at the transmitter, as explained in Section II, an IDFT architecture is applicable even when α is introduced. Therefore, the SEFDM signal generation complexity, computed based on (4) considering Q/α signal length, is given by

$$\mathcal{O}(Q/\alpha \times log_2 Q/\alpha). \tag{17}$$

As explained in (3), zeros are padded at the end of each input symbol vector. Therefore, a pruned operation [16] can be applied to simplify further the SEFDM signal generation complexity to

$$\mathcal{O}(Q/\alpha \times log_2 Q). \tag{18}$$

A bar chart is designed in Fig. 20 to compare each signal generation method as a function of the number of operations. Computational complexity for each signal is computed following (16), (17) and (18). It is clearly seen in Fig. 20 that the OFDM signal generation complexity is independent and will not be affected by the value of α. The complexity of SEFDM signal generation is correlated to the value of α. With the reduction of α, more operations are required. This is reasonable since the value of Q/α is increased when α is reduced. Therefore, a larger IDFT is needed for an SEFDM signal with smaller α. In addition, the pruned version of SEFDM signal generation has limited computational complexity reduction advantage. Another discovery in Fig. 20 is that the number of required operations for SEFDM signal generation at different α is on the same order of magnitude relative to the OFDM signal generation.

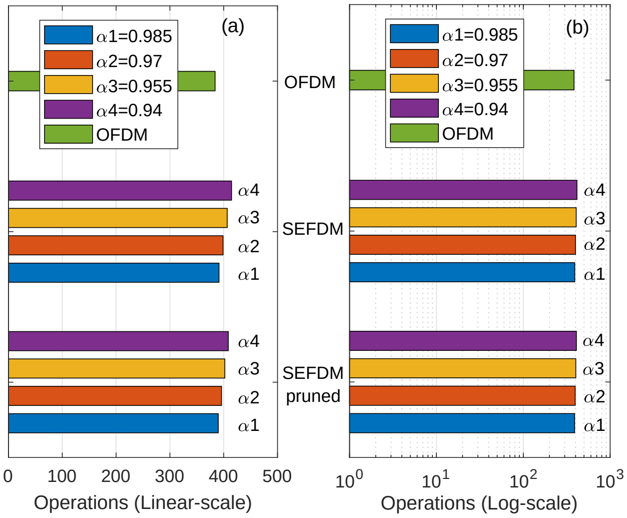


Fig. 20. Asymptotic complexity of WLAN-Type-III framework in terms of the number of complex operations in (a) linear-scale and (b) log-scale.

VI. Low-Cost SDR Experiment

Proof-of-concept experiments of traditional physical layer security techniques have been designed and tested in millimeter wave [4], artificial noise generation [32], directional modulation [31] and secrecy coding [33]. However, those experiments might not be practical to low-cost and resource-constrained communication scenarios.

This section aims to verify the WDS framework in low-cost hardware with the following objectives:

- The WDS framework is applicable to low-cost hardware, which will be beneficial to resource-constrained IoT communications.
- The WDS framework is highly coexistent with existing WLAN communication standards. It will be flexibly extended to other standards.
- The WDS framework is robust and will not be compromised even when eavesdroppers have signal power and channel environment advantages.
- CSIT is not required by the framework in experiments.

A. Experiment Design

The low-cost Analog Devices SDR PLUTO [35] is applied in the experiment to demonstrate that the proposed WDS framework is practical to resource-constrained IoT scenarios. The framework does not require complex hardware such as MIMO antennas, directional modulation driven antennas,

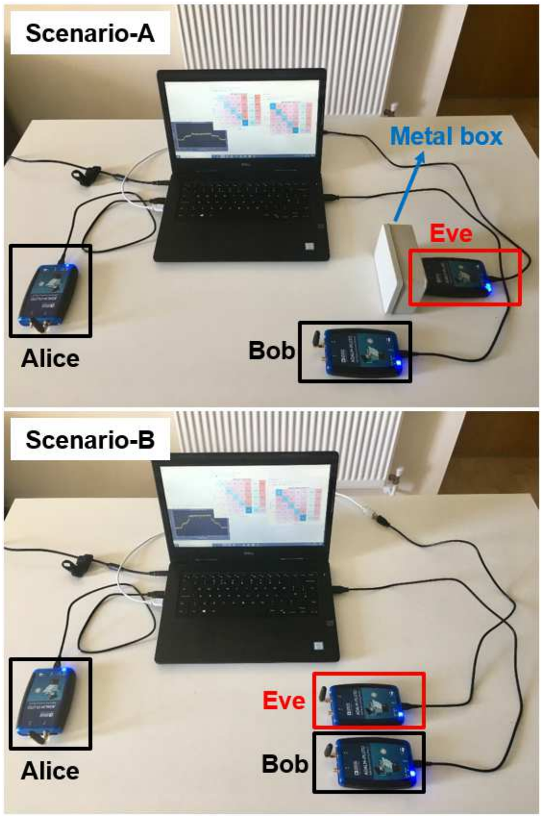


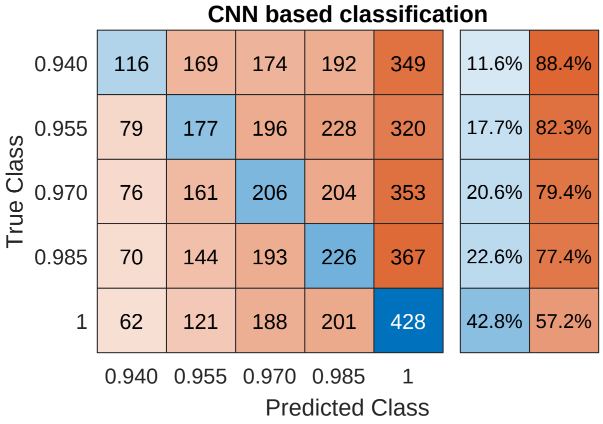
Fig. 21. Experiment setup for the WDS framework considering a non-line-of-sight eavesdropping link in Scenario-A and a line-of-sight eavesdropping link in Scenario-B.

phase shifters, high-frequency modulators and artificial noise generators. In this experiment, the SDR devices are equipped with single omni-directional antennas and therefore beamforming is not implemented.

The SDR device at Alice will generate all the signals based on the WLAN-Type-III signal pattern and deliver the signals over the air. Eve and Bob will receive them on their own SDR devices. Bob will demodulate and detect the signals with pre-shared signal format information while Eve will need to intelligently identify different signals before subsequent signal demodulation and detection.

To maintain a stable legitimate channel environment, the locations of Alice and Bob are fixed throughout the experiment. To have different eavesdropping channel scenarios, the position of Eve can be flexibly re-located. Two experiment scenarios are designed and tested using three SDR devices as shown in Fig. 21.

In the first experiment, Scenario-A, a line-of-sight legitimate link exists between Alice and Bob while the eavesdropping link between Alice and Eve is blocked by a metal box to emulate a non-line-of-sight communication. This scenario is challenging to Eve since the eavesdropping link signal power is lower than that of legitimate link. This scenario is designed based on the assumption that Eve in this work is passive and will merely listen to confidential information in a disadvantageous location. Otherwise, the existence of Eve will be detected.



True Class \ Predicted Class	0.940	0.955	0.970	0.985	1		
0.940	116	169	174	192	349	11.6%	88.4%
0.955	79	177	196	228	320	17.7%	82.3%
0.970	76	161	206	204	353	20.6%	79.4%
0.985	70	144	193	226	367	22.6%	77.4%
1	62	121	188	201	428	42.8%	57.2%

Fig. 22. Confusion matrix of Eve employing CNN classification in Scenario-A. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

In the second experiment, Scenario-B, Eve is placed next to Bob without the metal box blockage. In this case, a line-of-sight eavesdropping link is created, which has a similar signal power condition with the legitimate link. Scenario-B is challenging to communication security since the eavesdropper has a better condition than that in Scenario-A. Typical beamforming and artificial noise based physical layer security solutions are not efficient any more since Eve and Bob are placed closely next to each other.

This experiment will follow the 802.11a signal specifications and use the maximum bandwidth option, 20 MHz. The employed SDR PLUTO is supported by the WLAN toolbox [36] in Matlab. Therefore, the implementations of 802.11a and WLAN-WDS are straightforward. Over-the-air carrier frequency is tuned to 2.412 GHz, which is the Channel-1 frequency defined by [29]. To have a high coexistence with WLAN, this experiment maintains the 802.11a standard defined legacy preamble while merely changing the PSDU data field to the WLAN-Type-III signal pattern.

B. Experiment Results

To validate the experimental communication security at the eavesdropper, both confusion matrix and BER are investigated. In the experiment, 1,000 symbols per signal class are generated. There are overall 5,000 OFDM/SEFDM symbols for each test. Unlike simulations, in practical experiments, signal-to-noise ratio (SNR) is commonly measured at the receiver. In this experiment, to show the signal power difference between Eve and Bob, SNR is measured based on their frequency-domain signal spectra.

In Scenario-A, the value of SNR at Bob is around 35 dB, which is power sufficient to provide reliable performance with zero BER. The metal box at Eve can create a non-line-of-sight link but cannot influence SNR greatly. Therefore, by tuning the AGC at Eve, the SNR is reduced to 10 dB. This will emulate the practical eavesdropping condition where interception environment is commonly disadvantageous. With the above experiment setup, the average successful classification

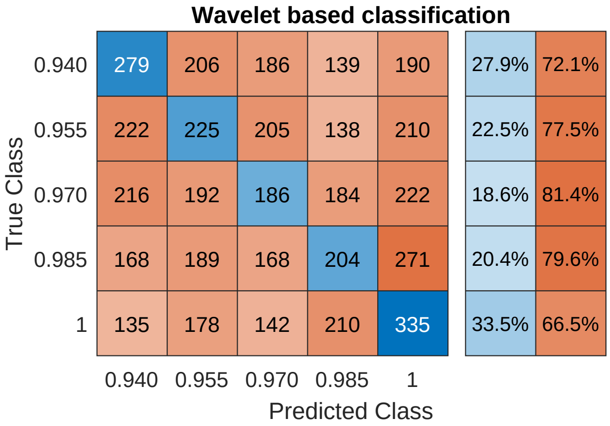


Fig. 23. Confusion matrix of Eve employing wavelet classification in Scenario-A. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

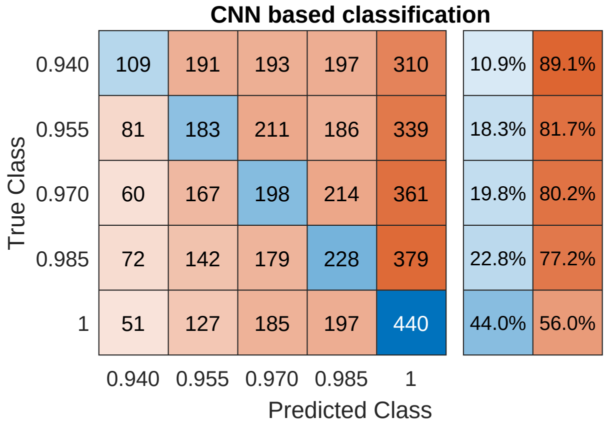


Fig. 24. Confusion matrix of Eve employing CNN classification in Scenario-B. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

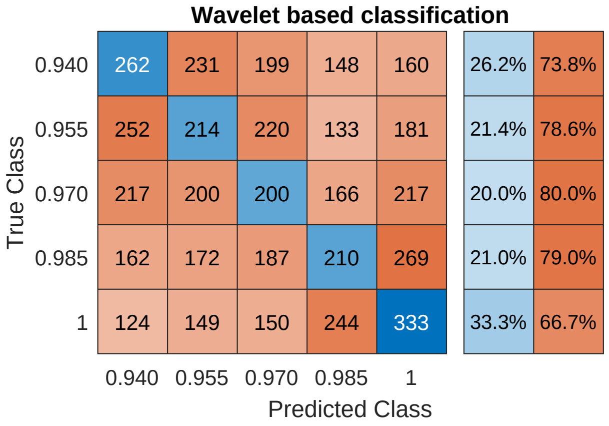


Fig. 25. Confusion matrix of Eve employing wavelet classification in Scenario-B. α=1 indicates WLAN-OFDM while other values of α indicate WLAN-SEFDM.

accuracy at Eve is 23.06% for the CNN classifier in Fig. 22 and 24.58% for the wavelet classifier in Fig. 23.

In Scenario-B, the location of Bob is fixed while Eve is placed next to Bob, which gives Eve a better eavesdropping environment with a line-of-sight link at SNR=35 dB. The confusion matrices for Scenario-B are presented in Fig. 24 and Fig. 25, which show average classification accuracy of 23.16% and 24.38%, respectively. It is practically verified that the proposed waveform-defined security framework is robust and is not related to SNR and communication link conditions at eavesdroppers.

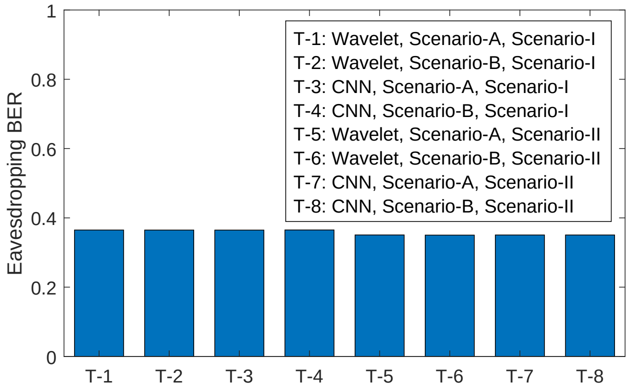


Fig. 26. Eavesdropping BER considering signal classifiers, eavesdropper channel conditions and eavesdropper receiver operations.

An additional experiment discovery is that the CNN classification accuracy is not equal for each signal class in Fig. 22 and Fig. 24. It is apparent that WLAN-OFDM has a higher classification accuracy than other signal types achieving 42.8% and 44.0% in Scenario-A and Scenario-B, respectively. Moreover, all other WLAN-SEFDM signals are mostly classified into WLAN-OFDM. The reason for this is that the offline trained CNN model is not perfectly fit in a new channel environment. Previous work [17] applied transfer learning to deal with the mismatch between offline training environment and practical environment. However, this is not realistic in secure communications since legitimate users will not allow eavesdroppers to adjust signal classifiers via transfer learning. Therefore, the mismatch between offline and practical environments would additionally enhance communication security. In terms of wavelet classification, accuracy is relatively stable for each signal class, which indicates the robustness of wavelet classification since signal features are manually extracted based on domain knowledge rather than data training.

To have a comprehensive study on eavesdropping BER performance, Fig. 26 jointly considers signal classifier types (i.e. CNN and wavelet), eavesdropper channel conditions (i.e. Scenario-A and Scenario-B) and eavesdropper receiver operations (i.e. Scenario-I and Scenario-II). Therefore, eight tests are designed with results showing in Fig. 26. It is clear that all the BER results maintain at a similar level while the Scenario-II based eavesdropping shows slightly degraded performance. As explained in Section V-B, Scenario-I has no classification mechanism and assumes all the received signals belong to WLAN-OFDM. However, Scenario-II applies classifiers and misclassification would happen. The performance of signal detection is highly dependent on the quality of signal classification. It is inferred from Fig. 26 that signal misclassification might leads to better BER than a system without signal classification.

VII. Conclusion

Traditional physical layer security techniques are highly dependent on channel conditions such as accurate CSI at the transmitter. However, in practical communications, perfect CSI is mostly unachievable due to time-variant channel characteristics. In addition, extra hardware is commonly required by beamforming or artificial noise techniques. Therefore, a waveform-defined security (WDS) framework is proposed to avoid the dependance on CSI and complex hardware. This work firstly studies three impact factors, which can tune waveform patterns undiscoverable at eavesdroppers. Results show that training data diversity has great effects on signal identification accuracy. In addition, a small oversampling factor and a narrow BCF offset can further confuse eavesdropping. A WLAN-WDS frame is designed to show a compatible coexistence with the existing WLAN 802.11a standard. Results show that BER performance is ensured at the legitimate user and security is promised via preventing eavesdropping. In addition, WLAN-WDS has the computational complexity on the same order of magnitude relative to the traditional WLAN. A low-cost experiment is operated to verify the WDS framework in resource-constrained communication systems. The SDR devices applied in this work are equipped with single omni-directional antennas and therefore beamforming is not implementable. Results show that the eavesdropper fails to recover signals even with an advantageous line-of-sight channel condition at SNR=35 dB, which proves that the success of WDS framework is not dependent on channel conditions. This work successfully verified that the proposed WDS framework is applicable in resource-constrained IoT communications while traditional PLS techniques are unachievable due to channel condition dependance and extra hardware complexity.

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] 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.

[3] Y. Zou, J. Zhu, L. Yang, Y. Liang, and Y. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, Sept. 2015.

[4] 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.

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

[6] 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.

[7] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[8] 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.

[9] 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.

[10] 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.

[11] M. Rodrigues and I. Darwazeh, "A spectrally efficient frequency division multiplexing based communications system," in *Proc. 8th Int. OFDM Workshop*, Hamburg, 2003, pp. 48–49.

[12] 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.

[13] 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.

[14] T. Xu, "Waveform-defined security: A framework for secure communications," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 2020, pp. 1–6.

[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[16] P. N. Whatmough, M. R. Perrett, S. Isam, and I. Darwazeh, "VLSI architecture for a reconfigurable spectrally efficient FDM baseband transmitter," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 5, pp. 1107–1118, May 2012.

[17] 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.

[18] 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.

[19] 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.

[20] T. Xu and I. Darwazeh, "Wavelet classification for non-cooperative non-orthogonal signal communications," in *2020 IEEE Globecom Workshop on Advanced Technology for 5G Plus (GC 2020 Workshop - AT5Gp)*, Taipei, Taiwan, Dec. 2020.

[21] 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.

[22] 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.

[23] T. Xu and I. Darwazeh, "Multi-Sphere decoding of block segmented SEFDM signals with large number of sub-carriers and high modulation order," in *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Nov. 2017, pp. 1–6.

[24] I. Kanaras, A. Chorti, M. Rodrigues, and I. Darwazeh, "A fast constrained sphere decoder for ill conditioned communication systems," *Communications Letters, IEEE*, vol. 14, no. 11, pp. 999–1001, Nov. 2010.

[25] T. Xu, R. C. Grammenos, F. Marvasti, and I. Darwazeh, "An improved fixed sphere decoder employing soft decision for the detection of non-orthogonal signals," *IEEE Communications Letters*, vol. 17, no. 10, pp. 1964–1967, Oct. 2013.

[26] T. J. O'Shea and N. West, "Radio machine learning dataset generation with GNU radio," *Proceedings of the 6th GNU Radio Conference*, 2016.

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

[28] ——, *5G NR: The Next Generation Wireless Access Technology*. Academic Press, 2018.

[29] IEEE-802.11, "IEEE standard for information technology-telecommunications and information exchange between systems local and metropolitan area networks-specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer

(PHY) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, 2016.

[30] X. Liu, T. Xu, and I. Darwazeh, "Coexistence of orthogonal and non-orthogonal multicarrier signals in beyond 5G scenarios," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[31] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 5, pp. 1545–1550, 2010.

[32] S. Goekceli, O. Cepheli, S. T. Basaran, G. K. Kurt, G. Dartmann, and G. Ascheid, "How effective is the artificial noise? real-time analysis of a PHY security scenario," in *2017 IEEE Globecom Workshops (GC Wkshps)*, 2017, pp. 1–7.

[33] C. Martins, T. Fernandes, M. Gomes, and J. Vilela, "Testbed implementation and evaluation of interleaved and scrambled coding for physical-layer security," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–6.

[34] M. Frigo and S. G. Johnson, "The design and implementation of FFTW3," *Proceedings of the IEEE*, vol. 93, no. 2, pp. 216–231, 2005.

[35] T. F. Collins, R. Getz, D. Pu, and A. M. Wyglinski, *Software-Defined Radio for Engineers*. Analog Devices, 2018.

[36] MathWorks, "WLAN toolbox," https://uk.mathworks.com/products/wlan.html, Apr. 2020.