Waveform-Defined Security Enhancement via Signal Generation Optimization

Tongyang Xu
Department of Electronic and Electrical Engineering, University College London, London, UK
Email: tongyang.xu.11@ucl.ac.uk

***Abstract*—Traditional defence strategies of physical layer security (PLS) are highly dependent on channel environments. This work investigates a waveform-defined security (WDS) framework, which can fundamentally prevent signal interception. In the traditional WDS framework, by intentionally tuning waveform parameters to weaken feature diversity and enhance feature similarity, eavesdroppers cannot correctly identify feature-similarity dominant signals using deep learning (DL) classifiers. The imperfect signal classification would result in subsequent detection errors. This work aims to optimize the framework by further complicating signal classification using a newly proposed signal generation architecture. Results show that the new signal generator can cut distinguishable signal features. In this case, classification accuracy at eavesdroppers is reduced by up to 53% leading to an enhanced WDS framework. Meanwhile, legitimate users maintain performance reliability regardless of signal generation architectures.**

***Index Terms*—Waveform-defined security (WDS), waveform, non-orthogonal, secure communications, physical layer security, deep learning, signal classification.**

I. Introduction

Radio signals are broadcasted over the air making physical layer security (PLS) vulnerable to eavesdropping. Beamforming [1] is the commonly used PLS defense technique, which will produce a narrow and directional beam towards a legitimate user. This solution is theoretically robust but practically has some challenges [2]. Firstly, beamforming based PLS requires channel state information (CSI) from both legitimate users and eavesdroppers. Since most eavesdroppers are passive, their CSI are not easily known by a transmitter. Secondly, beamforming requires multiple antennas or even multiple radio frequency (RF) chains, which might be realistic to proprietary systems but would not be realistic to resource-constrained internet of things (IoT) applications [3]. Thirdly, beamforming will be challenged when a legitimate user and an eavesdropper are spatially close or the worst case when they are aligned with the beam direction. Artificial noise [4] can avoid the CSI from eavesdroppers via broadcasting noise to eavesdroppers. However, extra power will be wasted for the noise generation. Directional modulation [5] is another PLS technique, which generates directional beams via specially designed antennas with limitations similar to beamforming. With the advancement of artificial intelligence (AI), adversarial attack [6] is becoming a threat that can use deep learning to intentionally interfere with legitimate user communications. An efficient defence solution is to use fake data to fool eavesdroppers but at the cost of reduced data rate.

Non-orthogonal signal waveforms, which are independent on CSI, are becoming potential candidate solutions for PLS. Existing waveform based PLS techniques are filter hopping [7], [8] and waveform-defined security (WDS) framework. In filter hopping schemes, filterbank based multicarrier (FBMC) and faster than Nyquist (FTN) waveforms will use flexible filter shaping to complicate eavesdropping signal detection. However, the signal generation for those filtering based signals is more complex than orthogonal frequency division multiplexing (OFDM), which makes integration to available communication systems unrealistic. In addition, the signal structure difference between the filtering waveforms and non-filtering OFDM will let eavesdroppers easily identify different signal features. The WDS framework was originally proposed in [9], which shows that interception can be prevented by intentionally confusing eavesdroppers via specially tuned waveform patterns. The benefit of WDS is that the employed spectrally efficient frequency division multiplexing (SEFDM) waveform [10] can bring either higher data rate or compressed spectral bandwidth. In addition, the signal generation is very similar to OFDM. In this case, the WDS framework can be easily integrated in available communication systems.

In this work, we will optimize the WDS framework from a signal generation perspective. This work evaluates two signal generation methods for the WDS framework. Results show that signal generation has impacts on signal classification and the proposed signal generation architecture can greatly reduce classification accuracy at eavesdroppers while maintaining performance reliability at legitimate users.

II. Non-Orthogonal Waveform Fundamentals

The initial motivation of SEFDM waveform is to save spectral bandwidth resources via packing sub-carriers closer as shown in Fig. 1. Such an advantage of spectral efficiency improvement meets the requirements of 5G and beyond. Meanwhile, the non-orthogonality characteristic of the waveform introduces self-created inter carrier interference (ICI), which is regarded as a natural defence mechanism.

A. Signal Principle

The fundamental OFDM signal is defined with the sub-carrier spacing of $\Delta f = 1/T$ where T is the time period of one OFDM symbol. To get SEFDM signals, the sub-carrier spacing is compressed to $\Delta f = \alpha/T$ where α is termed bandwidth compression factor (BCF), which determines the ratio of bandwidth compression.

The definition of an SEFDM signal is straightforward by adding α in a traditional OFDM signal expression as

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

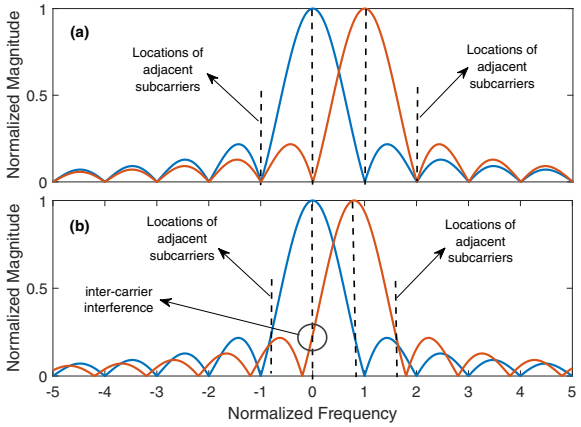

Fig. 1. Illustration of bandwidth compression in SEFDM. (a) OFDM sub-carrier packing. (b) SEFDM sub-carrier packing.

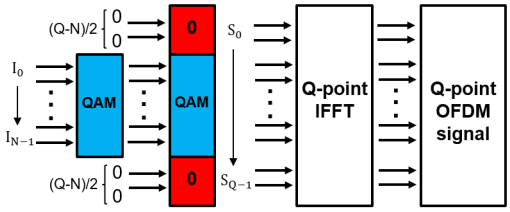

Fig. 2. Signal generation architecture for OFDM.

where $Q = \rho N$ indicates the number of samples with the oversampling factor ρ and the number of sub-carriers N. X_k is the k^{th} time sample with the index $k = 0, 1, ..., Q-1$, S_n is the n^{th} single-carrier symbol with the index $n = 0, 1, ..., Q-1$. It should be noted that since oversampling is applied, some elements in the vector S are zeros.

B. Signal Generation

OFDM signal generation is straightforward using inverse fast Fourier transform (IFFT) when $\alpha = 1$ in (1). Its signal generation block diagram is illustrated in Fig. 2. Typically, a signal requires protection guard bands on both sides of a raw input vector. Therefore, in Fig. 2, the original input symbol vector $[I_0, I_1, ..., I_{N-1}]$ is expanded to a Q-dimensional vector as

$$[S_0, S_1, ..., S_{Q-1}] = [\underbrace{0, ..., 0}_{(Q-N)/2}, I_0, I_1, ..., I_{N-1}, \underbrace{0, ..., 0}_{(Q-N)/2}], \quad (2)$$

where a Q-point IFFT is applied on the zero padded vector S leading to an oversampled Q-dimensional OFDM signal.

As expressed in (1), the direct operation for SEFDM signal generation will cause high computational complexity due to the parameter α. The effect of α can be removed via introducing a new parameter $M = Q/\alpha$ where M should be rounded to its closest integer. Traditionally, following previous work [11], the original vector S will be further expanded to a longer vector $S^{'}$ with the following stage-II zero padding operation

$$S_n^{'} = \begin{cases} S_n & 0 \leq n < Q \\ 0 & Q \leq n < M \end{cases}. \quad (3)$$

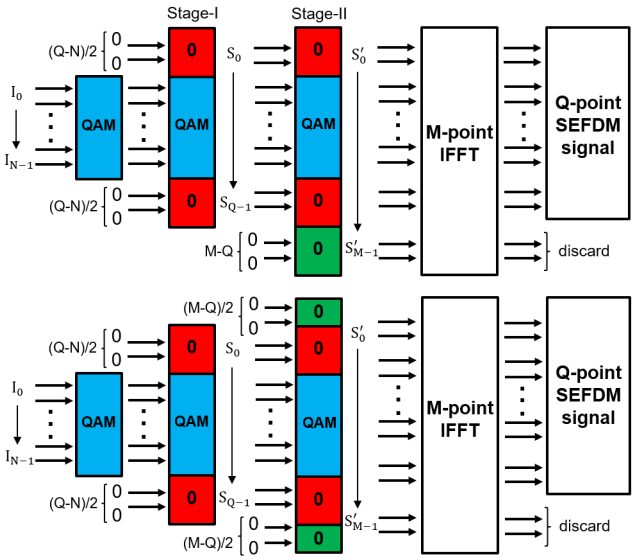

Fig. 3. Signal generation for SEFDM. (a) Typical architecture via padding zeros at the end: SigGen-I. (b) Proposed architecture via padding zeros on both sides: SigGen-II.

The traditional stage-II zero padding is demonstrated in Fig. 3(a) where a vector of $M - Q$ zeros are padded at the end of S as

$$[S_0^{'}, S_1^{'}, ..., S_{M-1}^{'}] = [S_0, S_1, ..., S_{Q-1}, \underbrace{0, ..., 0}_{M-Q}]. \quad (4)$$

The direct signal generation in (1) is thus simplified into an M-point IFFT operation as

$$X_k^{'} = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} S_n^{'} \exp\left(\frac{j2\pi nk}{M}\right), \quad (5)$$

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 leading to a Q-point SEFDM signal.

Due to the stage-II unequal zero padding in Fig. 3(a), the protection guard band created by the stage-I zero padding will be compressed resulting in the shift of an SEFDM spectral band according to the value of α. Therefore, its spectrum will not be centralized in the middle. This will not affect receiver side signal detection but will introduce additional signal features, which might be beneficially used by eavesdroppers.

An alternative way for SEFDM signal generation is to pad zeros on both sides of S as illustrated in Fig. 3(b). This newly proposed architecture will maintain an SEFDM spectral band in the center. The stage-II zero padding is thus modified in the following

$$[S_0^{'}, S_1^{'}, ..., S_{M-1}^{'}] = [\underbrace{0, ..., 0}_{(M-Q)/2}, S_0, S_1, ..., S_{Q-1}, \underbrace{0, ..., 0}_{(M-Q)/2}]. \quad (6)$$

In summary, both SigGen-I and SigGen-II signal generation architectures in Fig. 3 can achieve signal bandwidth compression advantages. However, the traditional generation method in Fig. 3(a) will additionally compress guard bands leading to a spectral band shift proportional to the value of α. Such an additional feature could be used by

eavesdroppers to break communications security. Therefore, the robust SigGen-II architecture in Fig. 3(b) is proposed to limit the spectral compression only to the signal band.

Although Fig. 3 shows two signal generation architectures, they all have the same computational complexity [11] as $M \times log_2 M$. With a pruned operation, the complexity could be reduced to $M \times log_2 Q$. It is apparent that the computational complexity of SEFDM signal generation is similar to that of OFDM, which is $Q \times log_2 Q$.

III. Principle of Waveform-Defined Security

The self-created ICI can be evaluated via computing the instantaneous power of X_k in (1) as the following

$$\begin{aligned} |X_k|^2 &= \frac{1}{Q}\sum_{n=0}^{Q-1}\sum_{m=0}^{Q-1} S_n S_m^* \exp\left(\frac{j2\pi(n-m)k\alpha}{Q}\right) \\ &= \underbrace{\frac{1}{Q}\sum_{n=0}^{Q-1}|S_n|^2}_{Signal} + \\ &\underbrace{\frac{1}{Q}\sum_{n=0}^{Q-1}\sum_{m\neq n, m=0}^{Q-1} S_n S_m^* \exp\left(\frac{j2\pi(n-m)k\alpha}{Q}\right)}_{ICI}. \end{aligned} \tag{7}$$

It is clearly seen that 'Signal' is a common term for both OFDM and SEFDM signals. When $\alpha = 1$, the 'ICI' term is cancelled for OFDM. When $\alpha < 1$, the 'ICI' term will be reserved for SEFDM signals. The variation of ICI is the key factor to enable waveform based communication security.

To simplify the analysis without considering zero padding, a matrix format of SEFDM signal generation is expressed as

$$X = \mathbf{F}I, \tag{8}$$

where X is a Q-dimensional vector, I is an N-dimensional vector without oversampling and $\mathbf{F}$ is a $Q \times N$ sub-carrier matrix. At the receiver, when additive white Gaussian noise (AWGN) Z is considered, the received signal will be expressed as

$$Y = X + Z. \tag{9}$$

Signal demodulation is realized by multiplying (9) with the complex conjugate sub-carrier matrix $\mathbf{F}^*$ leading to

$$R = \mathbf{F}^* X + \mathbf{F}^* Z = \mathbf{F}^*\mathbf{F}I + \mathbf{F}^* Z = \mathbf{C}I + Z_{\mathbf{F}^*}, \tag{10}$$

where $\mathbf{C}$ is an $N \times N$ correlation matrix, which contains ICI information. It is inferred that to successfully recover SEFDM signals, two steps have to be operated. Firstly, the perfect correlation matrix $\mathbf{C}$ has to be known. Secondly, an optimal signal detector has to be applied to remove the effect of $\mathbf{C}$.

A commonly used secure communication topology is presented in Fig. 4. Alice is the information sender, Bob is the legitimate user and Eve is the eavesdropper. Due to the nature of the waveform-defined security framework, Alice does not need channel state information at transmitter (CSIT) from Bob and Eve. Since signal format information is pre-shared with Bob, therefore only a signal detector is required by Bob. Eve is assumed to be passive and has no

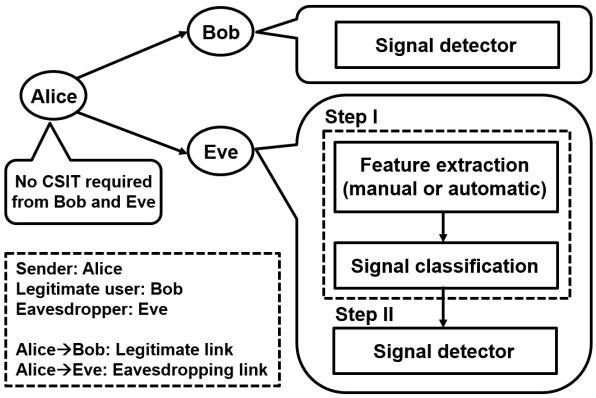

Fig. 4. Waveform based secure communication.

information of the signal format. Therefore, Eve's first step is to learn the signal format to determine the correlation matrix $\mathbf{C}$. With the estimate of $\mathbf{C}$, a signal detector will be applied at the second step. It is anticipated that an imperfect signal classification (i.e. imperfect estimation of $\mathbf{C}$) will cause the failure of subsequent signal detection.

IV. Signal Classification

Signal classification is the first step for a successful signal recovery. The aim of signal classification is to identify signal formats for each received signal. In this work, it will be used to determine the correlation matrix $\mathbf{C}$. With an accurate classification, the subsequent signal demodulation and signal detection will be reliable.

It should be noted that signal classification is different compared with modulation classification [12]. Signal classification aims to separate different multi-carrier signals while modulation classification is normally for signal-carrier signals. Since single-carrier signals are derived from multi-carrier signals, therefore accurate signal classification will determine the success of modulation classification. For modulation classification, constellation patterns are finite and pre-defined. Therefore, maximum likelihood classifiers are possible. However, the value of α in SEFDM is continuous and the infinite variations of α will prevent the use of maximum likelihood classifiers.

To effectively classify SEFDM signals, this work will rely on deep learning. The convolutional neural network (CNN) classifier has been applied in modulation classification [12] with reduced computational complexity. A CNN classifier has also been tested in SEFDM [13] with its potential applications in physical layer security in [9]. Therefore, this work will still use the CNN classifier to evaluate the security impact from different signal generation architectures. A general CNN classifier training framework is presented in Fig. 5 where multiple neural network (NN) modules are packed for automatic signal feature extraction. Each NN module includes four layers, namely Convolution, Normalization, ReLU and MaxPool. The last NN module, termed NN-out, has a unique AveragePool layer, which is used to obtain smooth features at the end. With the extracted features, a fully connected layer and a SoftMax layer are applied to classify signals.

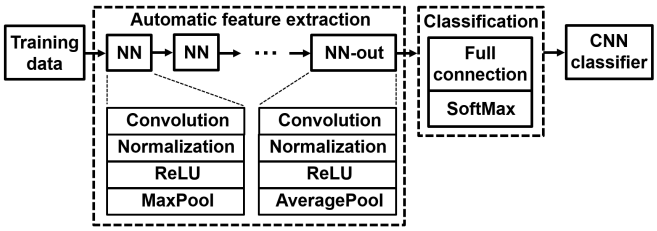

Fig. 5. CNN classifier training framework for the non-orthogonal signal classification.

The signal classification complexity mainly comes from the off-line training stage and a pre-trained model can be directly used for online classification tasks. It should be noted that the CNN classifier is only used by eavesdroppers. The high computational complexity of classifier training complicates eavesdropping and will therefore be beneficial to the WDS framework.

V. Signal Detection

Once the correlation matrix $\mathbf{C}$ is determined via signal classification, signal detection has to be operated to recover original signals from the self-created ICI. The optimal signal detection method is maximum likelihood which will search all possible solutions and find the optimal one. However, its computational complexity is exponentially increased when the number of sub-carriers increases. Its simplified version is sphere decoding (SD), which searches for the optimal solution within a pre-defined space.

The SD search for the optimal estimate I_{SD} is defined as

$$I_{SD} = \arg \min_{I \in O^N} \|R - \mathbf{C}I\|^2 \leq g, \tag{11}$$

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 R and the coarse hard-decision I_{ZF}. It is noted that the hard-decision I_{ZF} is computed based on the zero forcing (ZF) method using a rounding function $\lfloor . \rceil$ as $I_{ZF} = \lfloor \mathbf{C}^{-1}R \rceil$. Therefore, the search radius is defined as

$$g = \|R - \mathbf{C}I_{ZF}\|^2 \tag{12}$$

The final solution I_{SD} is obtained as a N-dimensional vector that meets the condition in (11). Each symbol estimation in I_{SD} is dependent on the symbols 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 in (11)(12) and cause no solution at the end. Therefore, the first step signal classification is crucial to the second step signal detection if an eavesdropper aims to accurately recover SEFDM signals.

The BER performance of different α at legitimate users is demonstrated in Fig. 6. To simplify signal detection, the MultiSD detector [14] is commonly used instead of SD when a signal is equipped with a large number of sub-carriers. Computational complexity will be reduced since multiple small size SD detectors are operated in parallel within the MultiSD. More details on the complexity comparison between SD and MultiSD are referred to [9]. Results in Fig. 6 show that the traditional matched filter (MF) signal

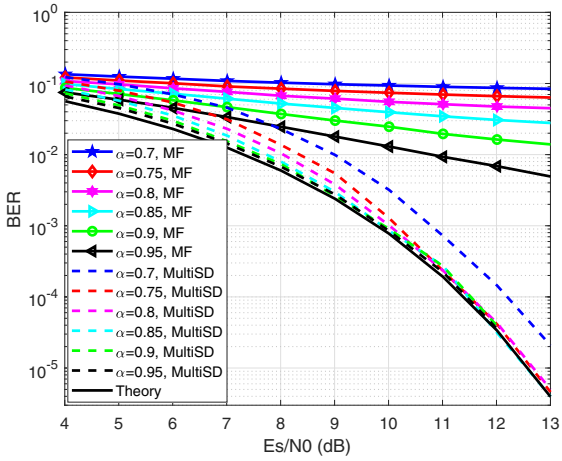

Fig. 6. BER performance at various α with detector (MultiSD) and without detector (MF) when perfect signal classification is assumed. The number of data sub-carriers is N=256.

detector is not powerful to recover non-orthogonal signals properly while the specially designed MultiSD detector can efficiently mitigate ICI and reach theory achievable performance. In addition, Fig. 6 reveals that a strong ICI effect (i.e. small α) will degrade signal recovery while better performance will be achieved with the increase of α.

VI. Simulation Design and Results

The simulation model is designed following the topology in Fig. 4, in which the eavesdropper requires a classifier and a signal detector while the legitimate user will use pre-shared information to detect signals. One OFDM/SEFDM symbol has N=256 raw QPSK symbols. With a sufficient oversampling factor ρ=8 [12], the time-domain signal has 2048 samples. To test the impact of signal generation architectures, two signal patterns are evaluated in the following with the values of α in the bracket.

- Type-I: OFDM, SEFDM(0.9, 0.8, 0.7)
- Type-II:OFDM, SEFDM(0.95, 0.9, 0.85, 0.8, 0.75, 0.7)

It should be noted that the WDS framework could have infinite signal patterns and the two patterns above are selected as evaluation examples. Type-I has four signal classes and the BCF gap between adjacent signals is $\Delta\alpha$=0.1. Type-II adds more signals leading to a narrower BCF gap of $\Delta\alpha$=0.05. Therefore, the Type-II signal pattern has stronger feature similarity and it is expected that classifying Type-II signals is more challenging than the Type-I signals.

For the CNN classifier training, 2,000 OFDM/SEFDM symbols are generated for each class in either the Type-I pattern or the Type-II pattern based on the data augmentation generation method [9]. Therefore, there are overall 8,000 training symbols for Type-I and 14,000 training symbols for Type-II. At the testing stage, 1,000 OFDM/SEFDM symbols are generated per signal class. In this case, the Type-I pattern will include 4,000 testing symbols and Type-II has 7,000 symbols. The CNN classifier is trained based on Fig. 5 with a detailed neural network architecture presented in Table I. Both training and testing symbols are manually distorted by pre-defined channel/hardware impairments. A three-path

Table I: CNN classifier neural network layer architecture

Layers	Dimension
Input layer	2×1024
Convolutional layer-1	$2 \times 1024 \times 64$
Convolutional layer-2	$2 \times 512 \times 64$
Convolutional layer-3	$2 \times 256 \times 64$
Convolutional layer-4	$2 \times 128 \times 64$
Convolutional layer-5	$2 \times 64 \times 64$
Convolutional layer-6	$2 \times 32 \times 64$
Convolutional layer-7	$2 \times 16 \times 64$
Full-connection layer	$2 \times 1 \times 64$
SoftMax output layer	$1 \times 1 \times 4(7)$

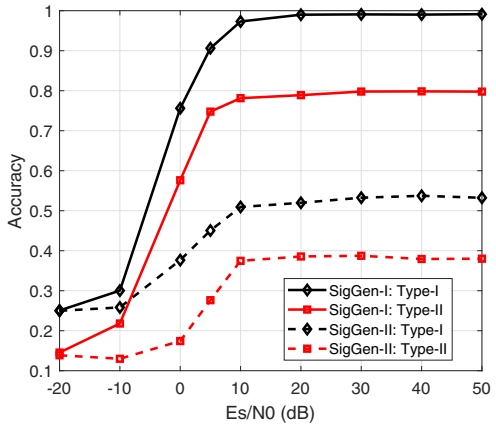

Fig. 7. Classification accuracy for SigGen-I and SigGen-II generated signals.

channel is defined with a path delay (s) of [0 9e-6 1.7e-5] and relative power (dB) of [0 -2 -10]. The maximum Doppler frequency is 4 Hz, the K-factor equals two and the frequency offset is 2 parts per million (PPM).

It is assumed that no signal processing is operated to compensate the channel/hardware impairments before signal classification. Therefore, a received signal will be randomly truncated with only 1024 time samples used by the classifier. Considering both real and imaginary part of a complex signal, the size of the input layer in the CNN classifier is therefore 2×1024 in Table I.

Firstly, a CNN classifier is trained based on the SigGen-I architecture in Fig. 3(a). Unlike the single Es/N0=20 dB training in [13], the training in this work is pre-contaminated by AWGN from Es/N0=-20 dB to 50 dB with a 10 dB increment step. This will ensure a robust CNN classifier that can universally work in a wide range of channel conditions. Classification accuracy is a metric that tells the robustness of classification. The accuracy results for the SigGen-I signal are presented in Fig. 7 where Type-I signals can be accurately classified at nearly 100% while Type-II signals are partially misclassified with a reduced accuracy of 80%.

A separate CNN classifier is trained based on the SigGen-II architecture in Fig. 3(b). Classification accuracy rates are therefore reduced to 53% for Type-I and 38% for Type-II in Fig. 7. Compared to the SigGen-I accuracy, the use of SigGen-II can cut eavesdropping classification accuracy by 47% and 53% for Type-I and Type-II, respectively. This is due to the fact that SigGen-I signals have two-

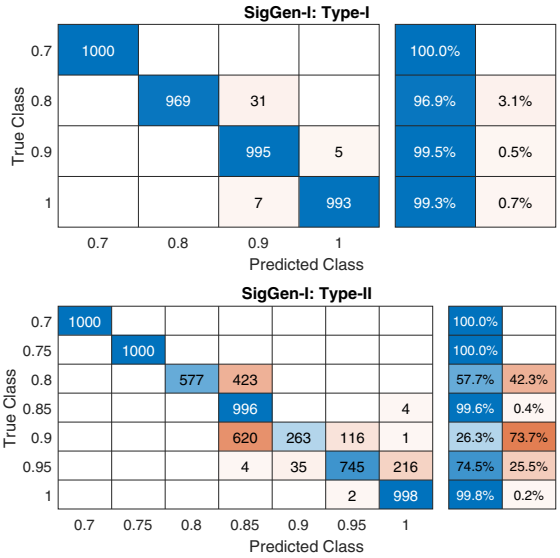

Fig. 8. Confusion matrix for Type-I and Type-II signals using SigGen-I architecture.

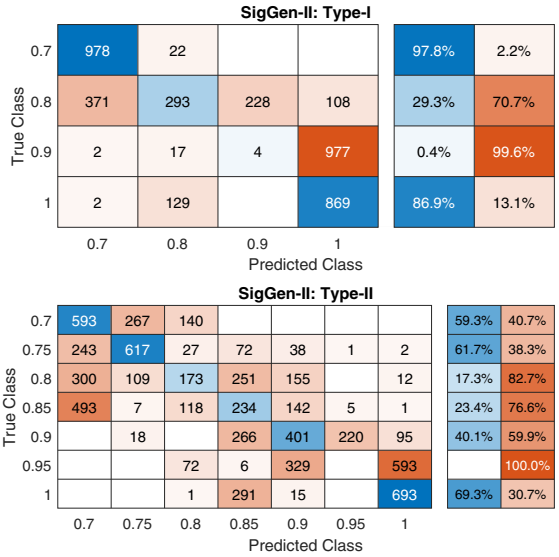

Fig. 9. Confusion matrix for Type-I and Type-II signals using SigGen-II architecture.

dimensional features, namely spectral bandwidth compression and spectral band shift. When the signal is generated via SigGen-II, the feature of spectral band shift will be removed. One-dimensional feature, limited to the spectral bandwidth compression, can not be effectively used by a classifier, resulting in the degraded accuracy.

Confusion matrix is a metric that shows the classification details. Two confusion matrices for SigGen-I signals at the stable Es/N0=30 dB are illustrated in Fig. 8. Perfect classification indicates that all the predicted elements are within the diagonal zone while imperfect classification would cause non-diagonal elements. Based on the principle, it is visually inferred that classifying Type-I signals is easier than Type-II signals. Confusion matrices are also presented for SigGen-II in Fig. 9 where the misclassification for each signal class is more obvious.

BER is also an efficient metric to evaluate the security

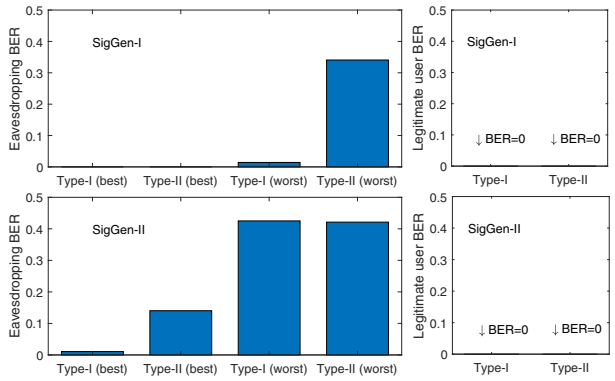

Fig. 10. BER comparison for eavesdropper and legitimate user signals generated by SigGen-I and SigGen-II architectures at Es/N0=30 dB.

robustness and performance reliability. We consider BER measurement based on realistic classification results at Es/N0=30 dB where eavesdropping classification accuracy is stable. Since a received signal can be classified into a random signal class, a weighted eavesdropping BER metric covering all possible prediction results, will be convincing. Considering the confusion matrices in Fig. 8 and Fig. 9, a weighted BER for a given α is computed as

$$BER = \frac{W_1}{W} \cdot BER_1 + ... + \frac{W_i}{W} \cdot BER_i, \qquad (13)$$

where W indicates the number of testing symbols, which is 1,000 for each true signal class in this work. W_i indicates the number of symbols that are predicted to the i^{th} signal class and BER_i is the BER based on the i^{th} predicted class using the MultiSD detector. It is inferred that the higher value of W_i, the higher percentage of its corresponding BER_i will dominate the final BER result.

The eavesdropping BER computation in Fig. 10 will consider the best case and the worst case according to confusion matrices. The best case for SigGen-I based Type-I signal in Fig. 8 is α=0.7 while the worst case is α=0.8. For the Type-II signal, the best case is either α=0.7 or α=0.75 while the worst case is α=0.9. Since the best case in SigGen-I based Type-I signal can be perfectly classified, its BER is thus zero. This is also the case for Type-II signals. However, the worst case will cause increased BER due to the mismatch between true class and predicted class. For SigGen-II generated signals, since the original spectral band shift feature is removed by the SigGen-II generator, its reduced classification accuracy in Fig. 9 results in degraded BER for both Type-I and Type-II patterns in either the best case or the worst case in Fig. 10. In summary, the use of SigGen-I signal generation can not completely ensure physical layer security while SigGen-II can enhance it.

For legitimate users, signal format information is pre-shared and legitimate users can skip the classification step and perfectly recover signals using the optimal MultiSD detector. Fig. 10 reveals that signal generation architecture has no effect on legitimate user BER performance and both Type-I and Type-II signals achieve zero BER.

VII. Conclusion

Instead of focusing on traditional channel dependent PLS techniques, this work aims to enhance communication security from a fundamental perspective using a waveform-defined security (WDS) framework. The traditional WDS framework ensures security by confusing eavesdroppers when signals are characteristically similar. However, the security will be compromised when signal features are diversified. Therefore, this work proposed to use a new signal generation architecture, which can enhance communication security by cutting distinguishable signal features. Both a feature-diversity dominant signal pattern and a feature-similarity dominant signal pattern are tested by deep learning CNN classifiers. Results show that eavesdroppers in the traditional WDS framework can classify the feature-diversity dominant signals at nearly 100% accuracy while the accuracy slightly reduces to 80% for the feature-similarity dominant signals. By using the proposed signal generator, eavesdropping will fail in both signal patterns and the accuracy is decreased by up to 53%. BER performance will not be affected by the new signal generation. Therefore, this work can enhance further WDS framework security and meanwhile maintain legitimate user performance.

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

[3] 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.

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

[5] 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.

[6] 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.

[7] V. Lücken, T. Singh, Ö. Cepheli, G. K. Kurt, G. Ascheid, and G. Dartmann, "Filter hopping: Physical layer secrecy based on FBMC," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, 2015, pp. 568–573.

[8] J. Wang, W. Tang, X. Li, and S. Li, "Filter hopping based faster-than-Nyquist signaling for physical layer security," *IEEE Wireless Communications Letters*, vol. 7, no. 6, pp. 894–897, 2018.

[9] T. Xu, "Waveform-defined security: a framework for secure communications," in *2020 IEEE/IET 12th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP) (CSNDSP2020)*, Porto, Portugal, Jul. 2020, pp. 1–6.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.