Waveform-Defined Security: A Framework for Secure Communications

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

***Abstract*—This work proposes a waveform-defined security (WDS) framework in secure communications via the design of non-orthogonal multi-carrier waveform patterns. The sophisticated detection required by non-orthogonal signal waveforms provides a natural defence mechanism. However, brute-force tactics such as maximum likelihood detection would break the defence by attempting all possible solutions. Thus, a waveform scaling strategy is proposed to scale up the number of non-orthogonally packed sub-carriers, which complicates eavesdropping signal detections. In addition, a waveform tuning strategy is proposed to intentionally tune waveform patterns to enhance feature similarity. Therefore, eavesdroppers would be confused to misclassify signals resulting in subsequent detection failures.**

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

I. Introduction

The open nature of wireless environment makes radio communications vulnerable to eavesdropping data interception [1]. Defence strategies [2], such as millimetre wave, beamforming, artificial noise, secrecy coding and directional modulation are proposed to mitigate eavesdropping. Existing defence solutions are mostly dependent on surrounding channel environment and therefore are not robust in time-variant multipath fading channels when channel state information (CSI) is imperfectly known [3]. Traditionally, theoretical research prefers ideal assumptions such as perfect CSI, which makes theoretically achieved discoveries unrealistic in practical field experiment tests. Secure beamforming is hardly implementable when legitimate users and eavesdroppers are spatially close [4], which is caused by imperfect beam shapes and therefore destructive beam leakages. In addition, the typical non-orthogonal multiple access based solution [5] has risks of information leakages since one user is allowed to decode signals from other users. Traditional ways to extend secure communication coverage would rely on error correction coding [6] at the cost of reduced power and throughput efficiency. Artificial noise enabled security is regarded as an efficient defence solution [7]. However, extra power would be wasted to generate noise and security reliability is compromised. Data encryption [8], widely used at link or transport layers, is also applicable to enhance physical layer security. However, its applications are limited and unrealistic in low-cost and resource-constrained systems.

With the development of artificial intelligence (AI), deep learning based adversarial attacks [9], [10] become more destructive than typical eavesdropping attacks. As defined in [10], adversarial attacks are divided into white-box attack and black-box attack. The white-box attack indicates that the adversary has perfect knowledge of the signal formats while the black-box attack assumes no knowledge about the signal formats. Practically, the signal format is not known by an adversary. Therefore, learning signal features will be the first step in the black-box attack. Work in [11] explains three main types of attack termed inference attack, evasion attack and causative attack. A defence strategy is proposed in [9] where a transmitter can use fake labels to fool an adversary attacker. In this case, the attacker cannot intelligently train a reliable signal classifier at the inference attack stage. This is equivalent to a causative attack to the attacker by falsifying the attacker's training data. However, the throughput would be reduced because of the fake labels transmission.

An alternative solution to enhance communication security is physical layer signal waveform optimization. A non-orthogonal waveform, spectrally efficient frequency division multiplexing (SEFDM) [12], [13], unlikely to be detected by eavesdroppers, could be applied to enhance physical layer security. Unlike the multi-carrier orthogonal frequency division multiplexing (OFDM) signal, SEFDM packs sub-carriers closer by violating the orthogonality leading to either bandwidth saving or data rate increase advantages. Better than the non-built-in security OFDM, the non-orthogonally packed sub-carriers in SEFDM introduce inter carrier interference (ICI), which complicates signal detections but in turn contributes to secure communications since computationally complex signal detectors would increase the cost of eavesdroppers to detect signals. The work in [14] studied the possibility of a similar strategy. The main idea is to generate a non-orthogonal signal via overlapping two OFDM signals. In this case, eavesdroppers cannot intercept signals from the overlapping interference without advanced signal detectors. However, with the advancement in hardware, a brute-force detector becomes realistic in low-cost hardware to break down the method in [14].

In summary, the physical layer security still has the following challenges to be solved:

- The traditional defence solutions are mostly channel dependent and unreliable in conditions such as time-variant multipath fading, imperfect CSI, multiple user access, beamforming leakage and long-range communications.
- The development of artificial intelligence makes the physical layer security vulnerable to deep learning adversarial attacks.

- The advancement of low-cost hardware makes brute-force signal detections practical.

This work will deal with physical layer security from a fundamentally different perspective by proposing a waveform-defined security (WDS) framework, which is independent from channel conditions. Firstly, a waveform scaling strategy, aiming to increase the number of non-orthogonally packed sub-carriers, can significantly increase the computational complexity of signal detections but in turn prevent eavesdropping and enhance information confidentiality. Secondly, a waveform tuning strategy, related to a waveform bandwidth compression factor adjustment, is proposed to confuse eavesdroppers by misidentifying signals. Deep learning has seen great success in various applications and is believed to be a potential approach to assist eavesdropping. Therefore, a deep learning based eavesdropping model is trained to evaluate the robustness of the proposed WDS defence framework. Results indicate that by intentionally tuning waveform parameters (i.e. bandwidth compression factor), signal features cannot be correctly identified by eavesdroppers, which leads to subsequent eavesdropping detection failures.

II. Waveform-Defined Security Framework

A. Waveform Fundamentals

The secure waveform has self-created ICI, which is the essential mechanism of preventing eavesdroppers to accurately identify and detect signals. The principle of the waveform is expressed as

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

where X_k is the k^{th} time sample with $k = 0, 1, ..., N-1$, s_n indicates the n^{th} single-carrier symbol within one SEFDM symbol, N is the number of sub-carriers and $\alpha = \Delta f \cdot T$ is the bandwidth compression factor where T is the time period of one SEFDM symbol and $\Delta f \leq 1/T$ is the sub-carrier spacing. The instantaneous power at time sample index k for one SEFDM symbol is computed as

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

The self-created ICI within the SEFDM waveform complicates signal detections and therefore increases the cost of eavesdropping. To mathematically separate the constructive signal from its self-created destructive interference, variables m and n are introduced in (2). The signal part is defined when $m = n$ while the interference part is the term when $m \neq n$. It should be noted that the value of α determines the interference term, which is zero when $\alpha = 1$ (i.e. OFDM) while non-zero when $\alpha \neq 1$ (i.e. SEFDM). An illustration of the non-orthogonal sub-carrier overlapping interference is shown in Fig. 1, where it clearly shows the ICI at each sub-carrier location in SEFDM.

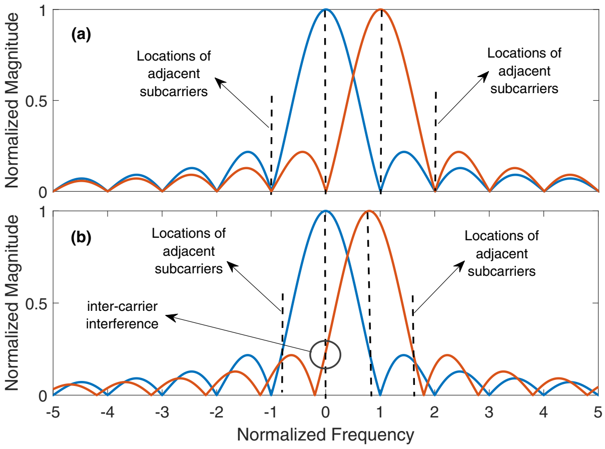

Fig. 1. Illustration of self-created inter carrier interference within SEFDM waveform. (a) OFDM sub-carrier packing. (b) SEFDM sub-carrier packing.

The generation of SEFDM signals can be simply performed via inverse discrete Fourier transform (IDFT). To remove the parameter α in (1), a new parameter $M = N/\alpha$ is defined. By padding $M-N$ zeros at the end of each input vector (i.e. a vector consists of N single-carrier symbols), a new vector of input symbols is obtained as

$$s_i^{'} = \begin{cases} s_i & 0 \leq i < N \\ 0 & N \leq i < M \end{cases}, \tag{3}$$

where the value of $M = N/\alpha$ is rounded to its closest integer and the SEFDM signal in a new format is

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

where $n, k = [0, 1, ..., M-1]$. The output is cut with only N samples reserved and the rest $M-N$ samples are discarded. Due to the discard of the last $M-N$ samples, ICI is therefore introduced and is regarded as a new enhancement solution for physical layer security.

B. Waveform Scaling

The detection of traditional OFDM signals depends on the matched filter (MF), which is essentially a fast Fourier transform (FFT) operation at the receiver. The complexity of FFT is acceptable in widely used communication systems, which requires $(N/2)log2(N)$ multiplications and $Nlog2(N)$ additions. For the proposed WDS framework, the detection of non-orthogonal signals relies on the brute-force maximum likelihood (ML) detector, which has exponentially increased computational complexity.

In practice, an optimal performance achievable but simpler sphere decoding (SD) detector is used instead of ML due to the reduced signal processing complexity in SD by searching a partial number of solutions. However, the complexity of SD is random since the search for an optimal solution is related to noise power. Therefore, to get

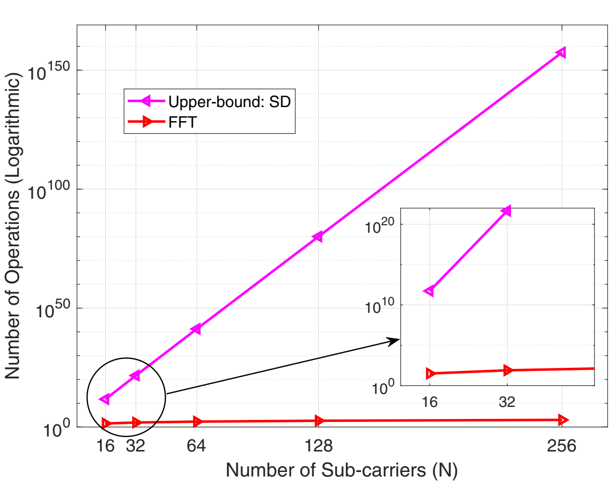

Fig. 2. The upper-bound number (logarithmic-scale) of multiplication operations versus the number of sub-carriers for SEFDM detector (i.e. SD) and OFDM detector (i.e. FFT).

a convincing comparison, the upper-bound complexity is considered leading to the search of all possible solutions in SD, which is the case when a signal is contaminated by high power noise. This section evaluates complexity in real-valued operations and only considers the detection complexity for one OFDM/SEFDM symbol. The computational complexity [15] of multiplication and addition operations is mathematically defined as

$$C_{SD} = \underbrace{(\sum_{n=1}^{2N} 2^n[2n+1])}_{multiplication} + \underbrace{(\sum_{n=1}^{2N} 2^n[2n-1])}_{addition}. \qquad (5)$$

With the breakthrough of low-cost hardware, a complex but powerful detector is no longer a barrier for eavesdroppers to intercept small size signals such as a signal with N=12 sub-carriers, which is the size of one resource block in 5G-NR [16]. Therefore, a straightforward solution to prevent the interception is to make the signal detection harder by scaling up the size of the non-orthogonal signal. The scaling-up methodology also meets the practical requirement in 5G-NR where a large number of sub-carriers are used to cope with multipath fading. The complexity of SD is random but it is proportional to the number of sub-carriers. A larger number of sub-carriers can enhance communication security by complicating signal detections. Numerical comparisons are presented in Fig. 2 where only multiplication is considered since its complexity is more concerned in practical systems. For the purpose of illustration, the number of operations in Fig. 2 is expressed on a logarithmic scale. Therefore, it is clearly shown that the FFT operation maintains at a low complexity level while the SD complexity increases exponentially. Such a large number of mathematical operations would take a significant processing time for the SD detector, which is unrealistic in commercially available hardware. Thus, the waveform scaling will increase the cost of eavesdroppers to intercept the signals and therefore ensures information confidentiality.

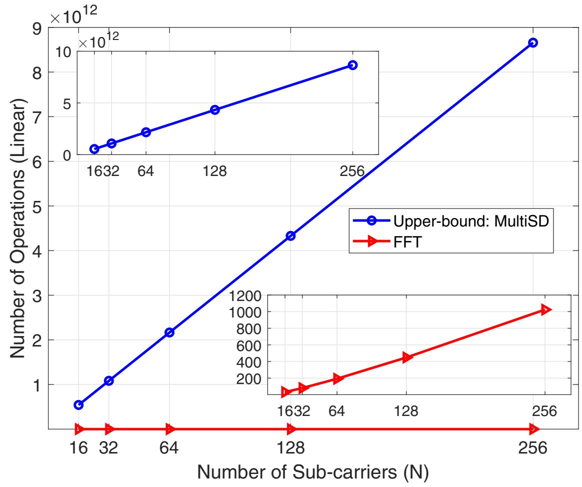

Fig. 3. The upper-bound number (linear-scale) of multiplication operations versus the number of sub-carriers for SEFDM detector (i.e. MultiSD) and OFDM detector (i.e. FFT).

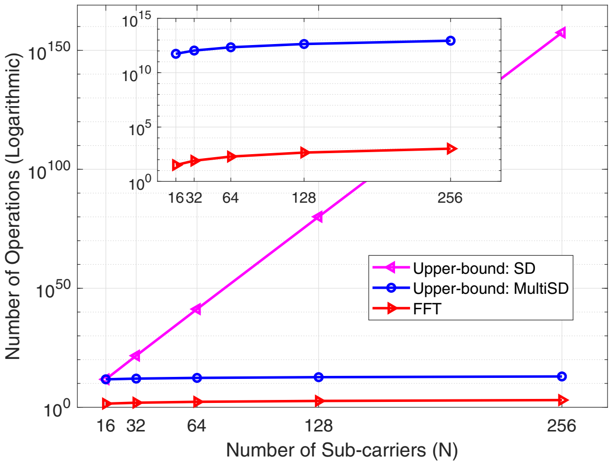

Fig. 4. The upper-bound number (logarithmic-scale) of multiplication operations versus the number of sub-carriers for SEFDM detectors (i.e. SD and MultiSD) and OFDM detector (i.e. FFT).

Waveform scaling is an efficient secure communication method to prevent eavesdropping but it also prevents communications between legitimate users. To deal with the detection of such a large size signal, a MultiSD detector was specially designed in [15], which can recover large size non-orthogonal signals with linear computational complexity as shown in Fig. 3. The newly designed detector still has higher computational complexity than FFT. However, its multiple-SD architecture enables parallel processing for multiple small size signals of N_B sub-carriers in commercially available hardware. Its complexity [15] is computed as

$$C_{MSD} = \underbrace{\frac{N}{N_B}(\sum_{n=1}^{2N_B} 2^n[2n+1])}_{multiplication} + \underbrace{\frac{N}{N_B}(\sum_{n=1}^{2N_B} 2^n[2n-1])}_{addition}. \qquad (6)$$

In Fig. 4, it clearly shows that the complexity of MultiSD is significantly reduced relative to the traditional SD detector

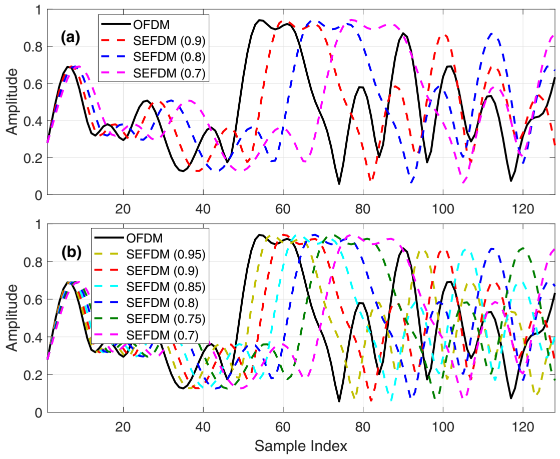

Fig. 5. Signal feature diversity and similarity visualization by modulating the same QPSK data. (a) Type-I signal pattern. (b) Type-II signal pattern. Values in the bracket indicate the bandwidth compression factor α.

considering the same signal scale. This discovery however endangers the waveform scaling security since eavesdroppers can detect signals using the MultiSD detector as well. Therefore, a more clever and robust defence method is needed to prevent the eavesdropping signal detection.

C. Waveform Tuning

In practice, an eavesdropper has to learn a signal classifier, which can identify different signal formats before any intentional attacks. Existing defence actions for such AI dependent eavesdropping would falsify data or labels to prevent accurate classifier training. Without accurate signal identifications, eavesdroppers cannot effectively carry out subsequent attacks. However, these traditional defence mechanisms rely on additional transmissions of fake data and labels, which reduces the data throughput between legitimate users. An efficient approach to address the deep learning adversarial attack is to design a waveform tuning defence method, which can mislead eavesdroppers into misclassifying the signals. The inaccurate classification of signal formats would result in subsequent detection errors. This solution is to prevent potential interceptions when the MultiSD detector is known by eavesdroppers.

The principle of waveform tuning is illustrated in Fig. 5. It is clearly seen that by tuning the bandwidth compression factor, signal waveforms would have trade-offs between diversity and similarity. Type-I shows strong signal diversity since adjacent signals have evident feature differences while Type-II shows increased signal similarity because adjacent signals have similar features. It is expected that the second type of signals are more difficult to separate from each other than the first type of signals. The same QPSK data is modulated on all the waveforms in Fig. 5 merely for the visualizations of signal feature diversity and similarity. For realistic training and testing in the following sections, random QPSK symbols will be used.

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	$1 \times 1 \times 4(7)$

Table II: Signal and channel/hardware specifications

Parameter	Specification
Sampling frequency (kHz)	200
IFFT sample length	2048
Oversampling factor	8
No. of data sub-carriers	256
Bandwidth compression factor α	1,0.95,0.9,0.85,0.8,0.75,0.7
Modulation scheme	QPSK
RF center frequency (MHz)	900
Path delay (s)	[0 9e-6 1.7e-5]
Path relative power (dB)	[0 -2 -10]
Maximum Doppler frequency (Hz)	4
K-factor	4
Frequency offset (PPM)	2
Omni-directional antenna gain (dBi)	2

III. Eavesdropping Signal Classifier

This work assumes that an eavesdropper would automatically learn signal features. Therefore, manual feature extractions are not taken into account in this work. There is no standardized training methodology for signal classifications. This work applies the deep learning convolutional neural network (CNN) model in the eavesdropping signal classifier. The neural network architecture, initially proposed by [17], is presented in Table I where seven convolutional layers are stacked to extract signal features and ReLU activation functions are employed through the network. The first six convolutional layers use MaxPool for downsampling while the last convolutional layer employs AveragePool. For the signal classification, a full-connection layer and SoftMax activation functions are applied. The cross-entropy loss between predicted values and true values is minimized by the stochastic gradient descent with momentum (SGDM) algorithm. After iterative operations, the optimal CNN classifier will be obtained.

Unlike the single-band signal generation in [17], this section employs the multi-band signal architecture [15], which can simultaneously confuse eavesdropping signal identifications and simplify legitimate user signal detections. The signal generation for each class (i.e. each α) follows the specifications in Table II. Since over-the-air signals would experience a variety of wireless environments, therefore the signal dataset can be enlarged similar to [17] via data augmentation. This can emulate a data-limited scenario at the eavesdropper by expanding a limited dataset through the time-variant channel models in Table II. Training is operated offline in a computer equipped with an Intel(R) Xeon(R)

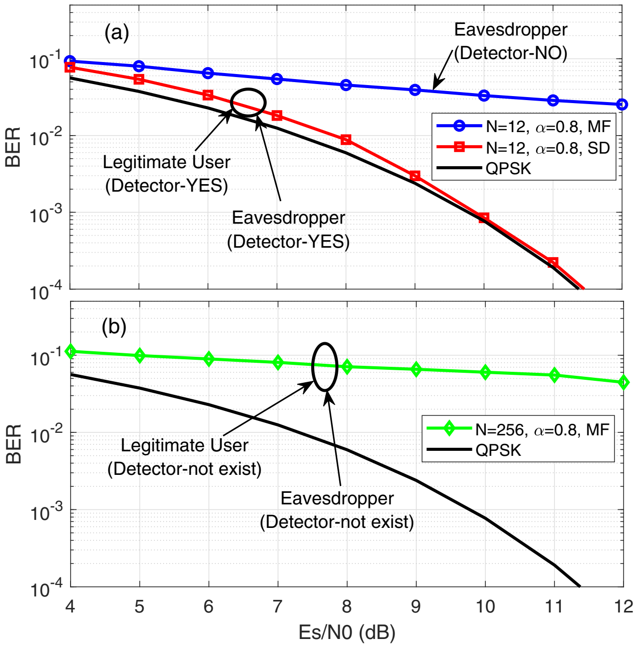

Fig. 6. Defence impact of waveform scaling. (a) N=12. (b) N=256. The ellipse notations indicate that both legitimate user and eavesdropper achieve the same BER performance.

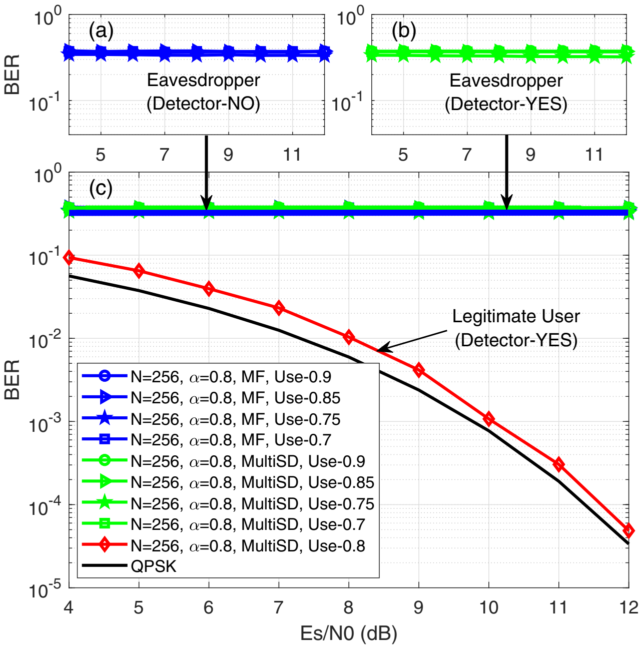

Fig. 7. Defence impact of waveform tuning. (a) BER at the eavesdropper without MultiSD. (b) BER at the eavesdropper with MultiSD. (c) Comparison with the legitimate user side BER.

Silver 4114 CPU (2 processors). Two signal classifiers, CNN-1 and CNN-2, are trained using the Type-I and Type-II data, respectively. Both data types are distorted by the channel/hardware impairments at a fixed Es/N0=20 dB. In each signal class, 2,000 frames (i.e. OFDM/SEFDM symbols) are obtained after the channel/hardware data augmentation. Therefore, there are overall 8,000 training frames for the CNN-1 and 14,000 training frames for the CNN-2.

IV. Security and Reliability Evaluations

The waveform scaling is evaluated in Fig. 6. Firstly, it assumes that the optimal but complex SD detector is technically challenging for eavesdroppers. Therefore, only the simple detector MF is applicable. It is clearly seen in Fig. 6(a) that the non-orthogonal signal, modulated by 12 sub-carriers, is perfectly recovered by legitimate users using the SD detector while it is undetectable by an eavesdropper using MF. However, the risk of knowing and employing SD detection for eavesdropping still exists since the rapid advancement of hardware making SD detection possible in commercially available hardware. A straightforward solution is to make detections harder by enlarging the signal size. Fig. 6(b) shows the performance of a signal modulated by N=256 sub-carriers. The SD detection of such a large size signal is impossible since the computational complexity increases exponentially as shown in Fig. 2. Therefore, it can efficiently prevent eavesdropping but at the cost of complicating legitimate communications.

The proposed waveform tuning can simultaneously deal with eavesdropping security and legitimate user signal reliability. Its performance is shown in Fig. 7. The target signal waveform is defined by α=0.8 while the eavesdropper has no knowledge of the signal format in advance. Fig. 7(a)(b) clearly show that the incorrect use of signal detectors (e.g. α=0.9, 0.85, 0.75, 0.7) results in great BER degradation either with or without the MultiSD detector. Only the legitimate user who knows exactly the signal format is able to apply the correct signal detector (i.e. α=0.8). The BER of the recovered signal therefore approaches the theoretical QPSK result as shown in Fig. 7(c). Thus, the waveform tuning method fundamentally prevents unauthorized interception even the MultiSD detector is leaked to eavesdroppers.

The detailed waveform tuning impacts on Type-I and Type-II signals are shown in Fig. 8 where confusion matrices are illustrated to unveil the accuracy details per signal class. In each sub-figure, vertical labels indicate true signal classes (i.e. α) and horizontal labels indicate predicted signal classes. Perfect signal classification will show only diagonal elements in each confusion matrix. Therefore, it is visually concluded that Type-I signals yield higher classification accuracy than Type-II signals. The Type-I signals, with strong feature diversity, achieve nearly 100% classification accuracy. By tuning the waveform parameter α to enhance feature similarity, only 56.3% of Type-II signals are classified into correct signal classes.

Eavesdropping BER results are compared in Fig. 9. Since the Type-I signal pattern is classified with high accuracy in Fig. 8(a), the BER is therefore zero for the MultiSD detected Type-I signal. However, due to the limited detection capability of MF, the MF detected Type-I signal has a minor BER degradation. The misclassification of Type-II signals in Fig. 8(b) results in significant eavesdropping BER degradation in Fig. 9 with either the MF detector or the MultiSD detector. This effectively verifies the robustness of the Type-II signal pattern and the feasibility of the WDS framework in secure communications.

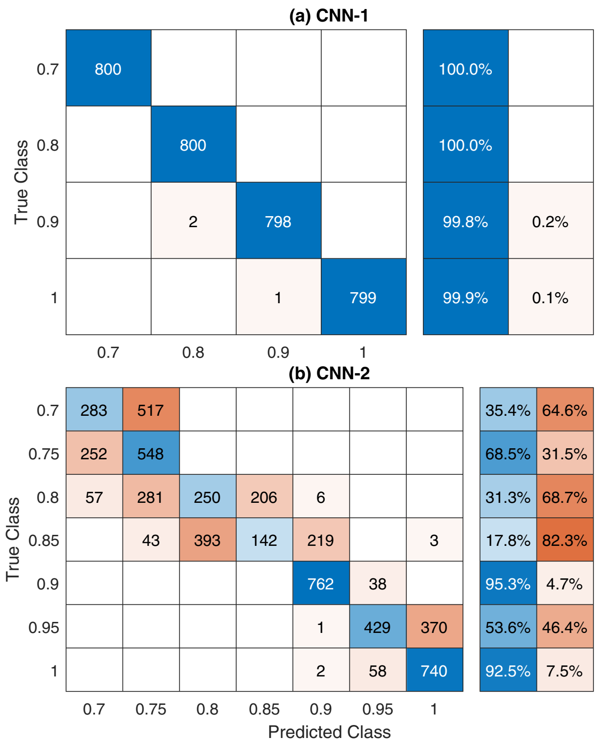

Fig. 8. Confusion matrix visualization for (a) Type-I and (b) Type-II signals at Es/N0=20 dB.

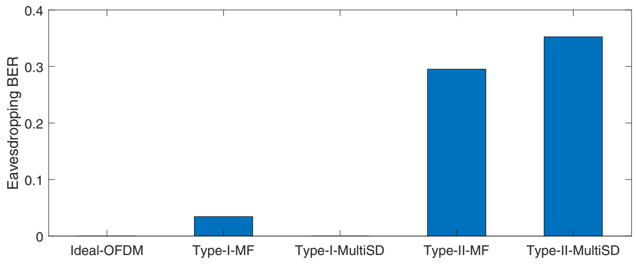

Fig. 9. Defence impact on eavesdropping BER performance for the target waveform α=0.8 at Es/N0=20 dB.

V. Conclusion

A waveform-defined security (WDS) framework is proposed in this work, which investigates the capability of using signal waveform design to defend against eavesdropping. Existing communication security methods are mostly channel dependent and would be unreliable when channel conditions are not perfect. In addition, the development of artificial intelligence makes communications vulnerable to deep learning adversarial attacks. Moreover, the advancement of low-cost hardware makes brute-force eavesdropping signal detections possible. The WDS framework firstly introduces a waveform scaling strategy, which can exponentially complicates eavesdropping signal detections. However, the high computational complexity also prevents communications between legitimate users. A performance-complexity optimized MultiSD detector is crafted to deal with large scale non-orthogonal signal detections but endangers secure communications since eavesdroppers can use the advanced detector as well. Therefore, the WDS framework introduces a waveform tuning strategy to cope with the aforementioned issue by intentionally tuning waveform patterns. In this case, signals would be tuned to have high feature similarity and eavesdroppers cannot easily identify them. Confusion matrices show that the classification accuracy for diversity dominant signals can approach 100% while it reduces to 56.3% when similarity dominates. The low classification accuracy would cause the failure of subsequent signal detections. BER performance reveals the robustness of the waveform tuning strategy, where the misclassification of signals results in eavesdropping detection error floors when the advanced detector is either known or not.

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. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[5] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, “On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming,” *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

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

[8] J. Zhang, A. G. Marshall, R. Woods, and T. Q. Duong, “Design of an OFDM physical layer encryption scheme,” *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 2114–2127, 2017.

[9] 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.

[10] 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.

[11] Y. E. Sagduyu, Y. Shi, and T. Erpek, “Adversarial deep learning for over-the-air spectrum poisoning attacks,” 2019.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] E. Dahlman, S. Parkvall, and J. Sköld, *5G NR: The Next Generation Wireless Access Technology*. Academic Press, 2018.

[17] 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.