A Reassessment on Friendly Jamming Efficiency

Rong Jin∗, Kai Zeng†, Kai Zhang‡

∗School of Electronic Information and Communications, Huazhong University of Science and Technology
Email: jinrong@hust.edu.cn
†Department of Electrical and Computer Engineering, George Mason University, VA 22030
Email: kzeng2@gmu.edu
‡Beijing Beike Technology Company
Email: zhangkk@hust.edu.cn

Abstract—With the rapid and continuous growth of various types of wireless devices in IoT, securing the communications among heterogeneous devices becomes an emerging issue. A physical layer security scheme, called “friendly jamming”, has drawn great attention recently owing to its ability to protect the confidentiality of the communication as well as to enable message authentication and access control for those already employed, unencrypted, weakly encrypted or resource constrained devices.

We notice that in a large number of cases in which friendly jamming are preferable, the transmitting signals to be protected have varying spectrum utilization at symbol level. In this paper, we rebuild secrecy capacity models and re-evaluate the jamming efficiency by taking this micro time scale non-stationary characteristic into consideration. Our reassessments reveal that jamming efficiency is greatly overestimated in the existing literature. The second part of our work further proposes a waveform design on jamming signal as a means to enhance the jamming efficiency. The basic idea is to consider both time and frequency domain structure of the transmitting signal when designing the jamming signal, making both time and frequency bandwidth largely match to each other.

We discuss the implementation details for jamming common QAM and PSK modulated signals. Both simulations and proof-of-concept experiments validate the theoretical correctness of our reassessment and practical effectiveness of our method.

Index Terms—friendly jamming; reassessment; time-frequency analysis; symbol level; non-stationary; secrecy capacity; jamming efficiency; waveform design

1 INTRODUCTION

With the revolution of the Internet that is driven by the recent advancements in the fields of sensor networks, mobile devices, wireless communications and cloud technologies, there is a rapid and continuous growth of various types of wireless devices accessing to the Internet. Experts estimate that the IoT (Internet of things) will consist of about 50 billion wireless objects by 2020 [1]. On the other side, the shared nature of the wireless communication channel poses substantial security challenges, from eavesdropping by a nearby passive attacker to illegal access by an active attacker. How to tackle the security challenges among heterogeneous wireless devices becomes an emerging issue.

Encryption has been typically used to provide the confidential communications in wireless networks. However, there are many scenarios where key distribution, resource constraint, deployment or legacy issues prevent the establishment or use of conventional cryptographic mechanisms. One example is the case of medical implants [2], where access to the implant data is safety-critical and must be granted to medical professionals in all circumstances, even in foreign domains to which appropriate credentials or keys cannot be distributed. Other examples are: (a) Sensor networks [3], where sensors are typically low cost devices with limited power and inferior computational capability to carry out complex encryption algorithms. Moreover, the difficulty of managing distributed sensor nodes in a centralized way is another challenge, which is however necessary for many encryption algorithms. (b) NFCs (near-field communication) and RFIDs (radio-frequency identification) [4], [5], where billions of unencrypted or weakly encrypted NFC or RFID tags or facilities have already been widely deployed and will be increasingly distributed; revoking and upgrading these massive amount of devices are nearly infeasible. (c) Smart wearable devices, where the battery capacity is limited and conventional encryption algorithms are not preferable.

Partly due to the encouraging progress on full-duplex radio [2], [6], [7], [8], [9], a physical layer security scheme, called “friendly jamming”, has been considered as a promising technology to enhance the communication security in the above scenarios. Friendly jamming can be used to achieve the following goals [10]: (i) to prevent an attacker from communicating with a protected device, and (ii) to prevent the attacker from eavesdropping on messages sent by protected devices. The first goal is related to access control, authentication and intrusion detection, and is typically achieved by a cooperative jammer who jams all traffic to or
from a protected device. The second goal is confidentiality and is achieved in this setting by exposing the attacker to friendly jamming such that the attacker's channel, unlike the channel of the protected receiver, is degraded to such an extent so that successful decoding of messages becomes infeasible.

Although a number of information theoretical analysis on friendly jamming have been carried out [7], [8], [9], we find that theoretical works are still not comprehensive for guiding practical implementations. Specifically, we notice that in a large number of cases in which friendly jamming are preferable, the transmitting signals (e.g. from sensors, NFC/RFID tags or cards) do not use the frequency spectrum evenly and fully across time domain in order to achieve low power consumption and easy recognition. By taking this micro time scale non-stationary characteristic into consideration, we rebuild secrecy capacity models and re-evaluate the jamming efficiency. Our reassessments reveal that jamming efficiency is greatly overestimated in many cases in the existing literature. We point out that this performance degradation comes from the underestimation of illegitimate decoding. Much higher bit compromising rate could be gained if an eavesdropper can take advantage of the special waveform structure of the signal to decode.

The second part of our work further proposes a waveform design on jamming signal as a means to enhance the jamming efficiency. The basic idea is to consider both time and frequency domain structure of the transmitting signal when designing the jamming signal, making the time and frequency bandwidth of jamming signals largely match those of transmitting signals. To transform the above idea to a practical system, we discuss the implementation details for jamming common quadrature amplitude modulation (QAM) and phase-shift keying (PSK) modulated signals.

We divide the transmitting signal into short segments according to their short term frequency spectrum, and we introduce different jamming signal on each segment separately. A special jamming signal with mixed flat and fluctuated waveform is synthesized. We conduct simulations and real-world experiments to demonstrate the effectiveness of our scheme. With this design, to achieve the same security strength, the power of jamming signal is dramatically reduced compared with the existing unstructured jamming signal schemes, such as Gaussian noise [8] or frequency-profile matched noise [2].

Our main contributions are as follows:

- We rebuild secrecy capacity models and re-evaluate the friendly jamming efficiency by taking micro time scale non-stationary characteristic of transmitting signal into consideration. Our reassessments reveal that jamming efficiency have been greatly overestimated in many cases in the existing literature.
- We propose waveform design on jamming signal as a means to enhance the jamming efficiency for friendly jamming for the first time. We probe into the details of implementation by discussing the waveform design on jamming signal for QAM and PSK modulation schemes.
- We demonstrate the theoretical correctness of our re-assessment and practical effectiveness of our method by extensive simulations as well as proof-of-concept experiments.

2 RELATED WORK

Partly due to the encouraging progress on full-duplex radio [6], [8], friendly jamming schemes have been proposed and drawn great attention recently. Previous works have investigated the scheme in depth from many aspects.

Theoretical works have characterized the impact of friendly jamming on the secrecy outage probability using jamming coverage and jamming efficiency as security metrics [7], [8], [9], evaluating the performance of different jamming strategies that rely on various levels of channel state information.

Some other works have discussed different configuration assumptions. For example, the works in [10], [11] have studied multiple jammers for improving information secrecy at the physical layer. The work in [13] has considered multiple users. The works in [10], [14] have addressed MIMO eavesdroppers and given a fundamental limitation of friendly jamming schemes when they are used for confidentiality and refined the conditions under which such schemes can be used. The works in [15], [16] have considered friendly jamming in a relay network. The works in [17], [18], [19] have investigated the power allocation strategies to minimize the overall transmitted power while preserving the source-destination throughput.

Some works studied the practical implementation of friendly jamming in real world applications. For example, the work in [2] has presented a physical-layer solution that delegates the security of an IMD (implanted medical device) to a personal base station called the shield. The shield uses a full duplex radio that can act as a jammer-cum-receiver, so as to jam the IMDS's messages, preventing others from decoding them, and to allow the shield to jam unauthorized commands. The works in [20], [21] have implemented a reactive and frame-selective jammer on a consumer grade IEEE 802.11 access point and reported measurement results from the first real-world study of friendly jamming in an IEEE 802.11 campus network. The work in [22] has investigated the feasibility of using defensive jamming technique to protect enterprise Wi-Fi networks from potential eavesdroppers. The work in [23] has considered the physical-layer security of visible light communication links aided by friendly jamming. The works in [24], [25] have considered the use of multiple available nodes as friendly jammers in order to improve the security performance of multi-hop and ad hoc networks. The work in [3] has proposed an anti-eavesdropping mechanism by introducing friendly jammers to WSNs (wireless sensor networks). The works in [4] and [5] targeted on NFC and RFID and have proposed practical solutions to hide the communications by changing the constant transmitting signal to a random one.

We notice that there has been no prior work (theoretical- or practically) paying attention to the varying spectrum utilization of transmitting signals at symbol level. We rebuild secrecy capacity models and re-evaluate the jamming efficiency and our reassessments reveal that jamming efficiency is greatly overestimated in many cases in the existing literature. We further propose a waveform design on jamming
signal as a means to enhance the jamming efficiency and discuss the implementation details for common QAM and PSK modulated signals. To the best of our knowledge, both theoretical work and proposed waveform design method are put forward first time in this paper.

3 PRELIMINARY

In this paper, we deal with a typical scenario where a wireless device, denoted as the transceiver Alice, transmits messages to or receives messages from another legitimate wireless device, denoted as the transceiver Bob. A third party, denoted as Carol, sends jamming signal to interrupt the communication between Alice (Bob) and a malicious wireless device, denoted as Eve, enhancing the security on both passive attacking case (increasing the difficulty that Eve decodes messages transmitted by Alice or Bob) and active attacking case (increasing the difficulty that Alice or Bob decodes messages transmitted by Eve). 1

3.1 Adversary Model

We assume a powerful attacker, who tries to (i) decode the messages transmitted by Alice through eavesdropping or (ii) send malicious commands to Alice actively. The attacker can be located in any location with a moderate distance of several meters from Alice (the attacker cannot be too close to Alice or Bob otherwise she will be physically discovered easily), and she can have a high quality line-of-sight attacking channel. The wireless channels among Alice, Bob, Eve and Carol are assumed stable when the friendly jamming is applied per data frame, and the corresponding statistical channel state information (CSI) can be estimated from the preamble. This assumption can be usually satisfied given that the duration of a data frame is typically short and within the channel coherence time. The attacker can capture baseband and RF signals with high sensitivity and sampling rate. In this case, she can obtain adequate sample points to reconstruct the waveform of the received signal. The attacker is also assumed to have powerful computational capability. She can store all the overheard signals and conduct sophisticated signal processing or data analysis.

3.2 Jammer Model

There are two basic friendly-jamming applications, full-duplex based friendly jamming and half duplex based friendly jamming (denoted as FD-FJ and HD-FJ, respectively).

In FD-FJ, the jamming device, Carol is typically a rich-resource and full-duplex enabled device such as small scale base stations, programmable NFC and RFID readers, so that this jamming device, much like a proxy server, can decrypt the messages from Alice, re-encrypt with strong password and relay to Bob to maintain the legitimate communications using a secure channel.

Some of the realistic applications could be implanted medical device (IMD) [2], near field communication (NFC) [4], and radio frequency identification (RFID) [5].

In HD-FJ, the jamming device, Carol is a normal half-duplex device (or multiple cooperative devices), and the presence of which would disrupt illegitimate decoding while the legitimate decoding is preserved. 2

Some of the realistic applications could be wireless sensor networks (WSN) [3] and wearable devices.

General model

For the convenience of description and without loss of generality, a general model is established using the term Transmitter to denote the legitimate message sender, the term Receiver to denote the legitimate message receiver, the term Eavesdropper to denote the illegitimate message receiver (or legitimate message receiver but subject to illegitimate messages) and the term Jammer to denote the jamming device 3 as demonstrated in Fig. 3.2.

To exemplify our reassessment and method, the following paper deals with FD-FJ and the passive attacking case in case study, simulations and experiments.

Frame-selective jamming

We assume that Jammer uses reactive and frame-selective jamming strategy as proposed in [20], [26], [27], which is the most attractive jamming technique for friendly jamming and would bring minimum interference to legitimate wireless applications. In reactive jamming, the interfering signal is emitted only when a transmission is detected. This can be done selectively by analyzing signals and interfering only with certain ones.

As exemplified in Fig. 2 where the frame header is defined by IEEE 802.15.4 ZigBee standard [28], reactive jamming starts with the task of channel sensing in order to detect a target frame. After having detected the signal, the jammer starts the decoding and analysis in order to make a jamming decision. In a realistic scenario, the jammer needs

1. We shall mention that friendly jamming can enhance the security of wireless communication at physical layer when high layer data encryption is not available. However, it does not necessarily exclude the cases involving data encryption in discussion. Even if there is data encryption at higher layers, secret keys could be compromised or need to be updated frequently. In these scenarios, friendly jamming is still very useful to secure the communication at physical layer to hide the real signals from the attacker, reject fake signals, or reduce the key recovery risk.

2. In these applications, legitimate decodings are often assumed to have certain advantages over illegitimate decoding, e.g. Alice and Bob are physically close; Carol is closer to Eve; Alice, Bob or(and) Carol has more antennas than Eve. As a typical example, if Alice and Bob are physically close (within a meter), Bob will receive a stronger signal from Alice than Eve does. So a jamming signal of appropriate power can just degrade the SNR at Eve’s antenna below the SNR threshold required for decoding the signal.

3. In FD-FJ, both Receiver and Jammer are referred to the same party, Carol.
Fig. 2. Reactive and frame-selective jamming involves three steps: detecting the signal by means of preamble, analyzing the signal to decide whether or not to jam, and, if so, emitting the jamming signal.

to identify the target frames based on the MAC header (e.g., the source and destination MAC address) within a very short time. For the example of ZigBee, the total time length of MAC header is about 11 to 23 Bytes, i.e. about 88µs to 184µs. In the remaining time, the jammer’s decision code has to be executed. The hardware needs to switch from receiving to transmitting mode, and the jamming signal has to be emitted before the payload data of the frame is transmitted. (It has been reported in [20], [29] that the reaction time is well achievable.)

3.3 Mathematical Model
According to the above system configuration assumptions, we model the signal received by Eavesdropper’s antenna as $y(t)$.

$$y(t) = h_{T→E}x(t) + h_{J→E}r(t) + n(t)$$  \hspace{1cm} (1)$$

where $x(t)$ and $r(t)$ represent the transmitting signal and jamming signal, respectively; $h_{T→E}$ and $h_{J→E}$ are the channel coefficients of the wireless channels from Transmitter to Eavesdropper and Jammer to Eavesdropper, respectively. $n(t)$ is the channel noise.

Similarly, we model the signal received by Receiver’s antenna as $y’(t)$.

$$y’(t) = h_{T→R}x(t) + h_{J→R}r(t) + n(t)$$  \hspace{1cm} (2)$$

where $h_{T→R}$ and $h_{J→R}$ are the channel coefficients of the wireless channels from Transmitter to Receiver and Jammer to Receiver, respectively.

4 Reassessment of Jamming Efficiency
In this section, we introduce the motivation and the derivation of our reassessment of jamming efficiency. We then provide some examples to demonstrate that the jamming efficiency is greatly overestimated in the existing literature. We further discuss the reasons behind and propose the idea to improve the jamming efficiency.

4.1 Motivation
As introduced earlier in Section 1, sensor networks, NFCs, and RFIDs are typical applications in which friendly jamming is needed for communication secrecy protection. We notice that in these cases, the transmitting signals do not use the frequency spectrum evenly and fully across time domain and often have varying spectrum utilization at symbol level. The reason is two-fold as follows.

First, the size of the data (e.g. measured/monitored data from sensors) or secret information (e.g. ID/password/secret-key) is small in these applications; it is unnecessary for the transmitting signals to be designed spectrum efficient and low data rates are often applied. For example, a large amount of sensors and embedded devices adopting IEEE 802.15.4 standard have 4 optional bit rates 20/40/100/250kbps. NFC and RFID devices adopting ISO/IEC 18092 and ISO/IEC 14443 standard have 3 optional bit rates 106/212/424kbps. They have much lower bit rates compared with Wi-Fi devices adopting IEEE 802.11 standard with tens or hundreds of Mbps.

Second, sensors and NFC/RFID tags or cards are resource-constrained devices; in these cases, certain waveform structures are often applied to achieve low cost and easy detection of the signal.

Fig. 3(a) shows an example of the in-phase baseband waveform $x(t)$, where the modulation parameters are drawn from IEEE 802.15.4 standard with 250Kbps and OQPSK modulation whose constellation diagram is illustrated in Fig. 7, where Transmitter uses a raised-cosine filter [30] in the filter-amplifier front-end circuit $h_f$ to filter out the out-of-band signal as well as to minimize the inter symbol interference (ISI) [31].

It can be seen that the modulated bit stream presents a common structural characteristics: they have step-shaped waveform structure with relatively stable voltage level in the middle of the symbol. We apply short-time-Fourier-transform (STFT) [32] to conduct time-frequency analysis to provide insight on how the signal frequency changes over time. Fig. 3(a) shows the transmitting signal $x(t)$ and Fig. 3(b) shows the output of the Gabor transform, where the dark color part is the frequency band occupied and the light color part is not fully used. This illustrates that the transmitting signal is not stationary at symbol level scale, which disagrees with the premise in previous works [7], [9].

4.2 Rebuild Secrecy Capacity Model
We refer to the stationary channel model introduced in [7], [9] to derive the secrecy capacity for non-stationary signals. We assume that Transmitter is subject to the short term average-power constraint $P_t$, whereas Jammer is subject to a short-term average power constraint $P_J$. We consider that channels between all pair of nodes are modeled as independent quasistatic Rayleigh fading channels. Specifically, for each channel, fading coefficients remain constant during the transmission of an entire frame but they change randomly and independently from one frame to another according to a complex Gaussian distribution with variance $c/d^\alpha$, where $d$ is the distance between the two nodes, $\alpha$ is the path-loss exponent, and $c$ is a normalization constant. We let $d_{je}$ and $d_{te}$ denote the distances from Jammer to Eavesdropper and from Transmitter to Eavesdropper, respectively. Then the instantaneous signal-to-interference-plus-noise ratio (SINR) at Eavesdropper derived from (1) is the random variable

$$\Gamma_E = \frac{P_t c_{te} G_{te}}{1 + P_J c_{je} G_{je}}$$  \hspace{1cm} (3)$$

where $G_{te}$ and $G_{je}$ are independent exponential random variables with unit mean. $c_{te}$ and $c_{je}$ are dimensionless.
constants with $c_{te} = \frac{c}{N_0 d_e}$ and $c_{je} = \frac{c}{N_0 d_e}$. $N_0$ is the power of channel noise.

Similarly, we use $d_{jr}$ and $d_{tr}$ to denote the distance from Jammer to Receiver and from Transmitter to Receiver. The instantaneous SINR at Receiver derived from (2) is the random variable

$$ \Gamma_R = \frac{P_t c_{tr} G_{tr}}{1 + P_j c_{jr} G_{jr}} $$

where $G_{tr}$ and $G_{jr}$ are also independent exponential random variables with unit mean. $c_{tr}$ and $c_{jr}$ are dimensionless constants with $c_{tr} = \frac{c}{N_0 d_{tr}}$ and $c_{jr} = \frac{c}{N_0 d_{jr}}$.

For stationary channels, in the presence of fading, the secrecy capacity $C_s$ of the channel between Transmitter and Jammer can be treated as a random variable varying among frames, while within a frame, the instantaneous secrecy capacity [9], [33] can be treated as being prescribed for a given realization $(\gamma_E, \gamma_R)$ of $(\Gamma_E, \Gamma_R)$.

$$ C_s = \max(C_R - C_E, 0) $$

where $C_E = W \log(1 + \gamma_E)$ is the capacity of Eavesdropper’s channel, and $C_R = W \log(1 + \gamma_R)$ is the capacity of Receiver’s channel. $W$ is the bandwidth.

Let us further consider a non-stationary channel where effective transmission bandwidth changes with time such as the one illustrated in Fig. 3(b).

We extend the expressions of instantaneous SINR at Eavesdropper and Receiver in (3) and (4) as

$$ \Gamma_E(f, t) = \frac{P_t(f, t)c_{te}G_{te}}{1 + P_j(f, t)c_{jr}G_{jr}} $$

$$ \Gamma_R(f, t) = \frac{P_t(f, t)c_{tr}G_{tr}}{1 + P_j(f, t)c_{jr}G_{jr}} $$

where $P_t(f, t)$ and $P_j(f, t)$ are the instantaneous power spectrums of transmitting signal $x(t)$ and jamming signal $r(t)$ at the time instant $t$, respectively, which describe the distributions of power into frequency components composing the two signals.

The instantaneous secrecy capacity is now a time varying function within a frame

$$ C_s(t) = \max(C_R(t) - C_E(t), 0) $$

where $C_E(t)$ and $C_R(t)$ are the overall capacities of Eavesdropper and Receiver’s channel at the time instant $t$, respectively.

$$ C_E(t) = \int_{f \in W_E(t)} \log[1 + \gamma_E(f, t)] df $$

$$ C_R(t) = \int_{f \in W_R(t)} \log[1 + \gamma_R(f, t)] df $$

where $W_E(t)$ denotes the used frequency spectrum of the transmitting signal at the time instant $t$.

The average secrecy capacity is

$$ \mathcal{C}_s = \frac{1}{T} \int_{t_0}^{t_0 + T} C_s(t) dt $$

where $T$ is the symbol duration.

### 4.3 Modified Secrecy Outage Probability and Jamming Efficiency

The concept, definition and calculation of secrecy outage probability and jamming efficiency have been proposed in [7], [9]. To demonstrate the impact of non-stationary signal on jamming effect, we use the same metrics to compare their calculations with ours.

We denote $R_s$ as the bit rate of the transmitting signal $x(t)$. Communication is secure if the average secrecy capacity $\mathcal{C}_s$ is higher than the target secrecy rate $R_s$. If $\mathcal{C}_s < R_s$, the security is compromised and we can say that a secrecy outage occurs. The secrecy outage probability (SOP) was introduced in [9], [33] to evaluate the security of wireless communication systems and is defined as

$$ P_{\text{out}}(R_s) = Pr[\mathcal{C}_s - R_s < 0] $$

To distinguish the cases with jamming ($P_j > 0$) and without jamming ($P_j = 0$), we add the superscripts $j$ and $n_j$, respectively. The SOP with and without jamming are denoted as $P_{\text{out}}^j$ and $P_{\text{out}}^{n_j}$ respectively.

To analyze the effect of jamming on security, we focus on the performance metric, jamming efficiency, which was
defined in [9] as the ratio between the SOP without and with jamming.

\[ \Delta P_{\text{out}} = \frac{P_{\text{out}}^j}{P_{\text{out}}^0} \quad (13) \]

This measure of security captures the reduction in the SOP introduced by Jammer for a given system setup (e.g., the location and power of Transmitter, Receiver and Jammer, the bit rate of transmitting signal), and higher value of this measure indicates higher jamming efficiency.

4.4 Case Study

In order to demonstrate the value of the reassessment, we draw a typical example to compare the proposed new jamming efficiency calculation formula \(^5\) with the existing one. \(^6\)

Exemplified scenario

We assume that the secrecy capacity of friendly jamming relies on a full duplex jammer located in an effective location. We target on a single transmitter, receiver and jammer system. We assume that they are all subject to single antenna restriction. \(^7\) The target secrecy rate and path-loss are set to \( R_s = 0.25 \text{Mbps} \), and \( \alpha = 2 \) based on [9]. The residue self interference is set to \( g_{jj} = -20 \text{dB} \) (It is stated in [6] that the receive antenna’s signal can be decoded if self-interference can be removed 20dB below the transmitting signal). The target secrecy rate is normalized with respect to the capacity of the AWGN channel with the same average SNR. The relative location relationship (relative positions and distances) among Transmitter, Eavesdropper and Receiver (Jammer) are denoted by (0,0), (0,1), (0,0,1) respectively.

For the transmitting signal \( x(t) \), the bit rate is 250Kbps; the modulation is OQPSK based on ZigBee protocol [34]; the frequency spectrum \( W_r(t) \) is shown in Fig. 3(b).

The following two types of popular jamming signals are evaluated:

1) Band-limited Gaussian white noise (denoted by Gaussian Noise): Jammer simply generates additive Gaussian noise with the same bandwidth as the transmitting signal as discussed in [7], [35], [36]. From a practical perspective, this case is important since it addresses a common active jammer that can be easily realized with off-the-shelf equipment.

2) Frequency profile matched noise (denoted by Fre-Match Noise): Jammer considers the frequency structure of the transmitting signal when crafting the jamming signal, shaping the amount of energy it puts in each frequency according to the frequency profile of the transmitting signal as proposed in [2].

Jamming efficiency calculation

We calculate the jamming efficiency analytically \(^8\), and draw the jamming efficiency to jamming power curves in Fig. 4(a), where the solid line denotes the existing jamming efficiency calculation without considering frequency-band mismatch; cross marked line and circle marked line denote the modified jamming efficiency calculation, where the jamming signals are Gaussian Noise and Fre-Match Noise, respectively. It can be seen that solid line is located above cross marked line and circle marked line in this case. The result reveals that jamming efficiency is greatly overestimated for the given scenario in the existing literature.

Next, we investigate weather the overestimation of jamming efficiency is a general situation.

Different modulation methods

We first calculate the jamming efficiency under different modulation order. Fig. 4(b) and Fig. 4(e) illustrate the cases of 8PSK and 16QAM, respectively, where the system configurations have remained unchanged. It can be seen that the curves of 8PSK and 16QAM have similar shapes and trends with that of QPSK, despite that their efficiency values are not identical. This is reasonable because constellation based modulation methods have similar waveform structure where center parts are relative flat and marginal parts are changing rapidly. More importantly, solid lines are located above cross marked lines and circle marked lines for different constellation point distributions. The results mean that jamming efficiency could be commonly overestimated for different modulation order.

We then apply the jamming efficiency calculation on common multi-carrier modulation method, i.e. OFDM. The jamming efficiency to jamming power curve is illustrated in Fig. 4(d), where the bit duration, the bandwidth, the modulation and the number of subcarriers are set according to IEEE 802.11a standard [17]. It can be seen that solid line is still located above cross marked line and circle marked line apparently. This is reasonable because for each subcarrier, the symbols are still modulated by QPSK, and thus present the discussed structural waveform. As a result, the overall spectrum utilization is not stationary at symbol level.

All the subfigures in Fig. 4 show that it is not an individual case but common situation of the overestimation of jamming efficiency in today’s communication systems.

Different system configurations

8. by numerical calculation method since jamming efficiency cannot be obtained in closed form in general [9].
Fig. 4. Examples of the impact of jamming power on jamming efficiency (a) QPSK (b) 8PSK (c) 16QAM (d) OFDM.

Note from Fig. 4 that each curve shows an inverse-U shape and there is normally a maximum value indicating the optimal jamming efficiency [9], [17], [18], [19]. That is, in the early stage when the jamming signal power is not significant, jamming is beneficial as the SOP becomes lower when jamming signal becomes stronger; while at the later stage when the jamming signal becomes much stronger, the harmful effect of jamming signal to legitimate decoding becomes dominant.

We vary the residue self-interference from $-30dB$ to $-10dB$ (with other parameters remaining unchanged) to study the impact of residue self-interference on the optimal jamming efficiency in Fig. 5. Note that each curve shows a monotone decrease with the increase of residue self-interference. This is intuitive since generally better full duplex radios with higher self-interference cancellation capabilities lead to better security enhancement. However, as can be seen from Fig. 5 that under the same residue self-interference, existing jamming efficiency calculation always presents the highest optimal jamming efficiency over the proposed new ones.

We further study the distribution of the optimal jamming efficiency for Jammer at different locations in Fig. 6 (where the residue self-interference is set to $-20dB$ with other parameters remaining unchanged), where the locations of Transmitter and Eavesdropper are fixed to (0,0) and (2,0). Note that the optimal locations of the jammer achieving the highest efficiencies appear in the intermediary areas between Transmitter and Jammer. This is reasonable since Jammer has a greater distance advantage over Eavesdropper in these areas. As can be seen from Fig. 6 that the existing jamming efficiency calculation gives the largest efficiency values; the scope of the optimal jamming efficiency by the existing jamming efficiency calculation formula ranges from 3.1 to 4.1 within the area of study, while that of Gaussian Noise and Fre-Match Noise by the proposed new jamming efficiency calculation formula range from 1.5 to 1.9 and 2.2 to 2.6, respectively.

The conclusion is that applying the existing jamming efficiency calculation formula on spectrum utilization varying signals leads to overestimated jamming efficiency for all the tested cases.

4.5 Need for Frequency-Time Domain Consideration on Jamming Signal

Gaussian Noise Case

At first, it is easy to think of using Gaussian noise as jamming signal $r(t)$ to cover the transmitting signal $x(t)$ because Gaussian signal presents good randomness.

However, it lacks frequency domain consideration. To understand this issue, we take the waveform in Fig. 3(a) as an example. Fig. 3(c) shows the frequency spectrum of transmitting signal. Transmitter operates over a channel bandwidth of about 2MHz. Jammer might create a jamming signal over the entire 2MHz. However, since the frequency domain representation of transmitting signal has most of its energy concentrated around carrier frequency $f_c$, Eavesdropper can eliminate most of the jamming signal by applying a band-pass filter centered on carrier frequency $f_c$ with a good chance to decode the signal.
have narrow bandwidth (denoted as center parts) and the other is located on the borders between two consecutive symbols which have wide bandwidth (denoted as marginal parts). For marginal parts, the jamming signal fails to cover the entire bandwidth of the transmitting signal.

It can be seen from (6) accordingly that the SINR at Eavesdropper could be still high in this case since jamming signal is not applied on certain transmitting signal: \( \Gamma_r(f, t) \approx P_r(f, t)c_rG_{tr}, f \in W_{t-j}(t), \) where \( W_{t-j}(t) = W_i(t) - W_j(t) \) denotes the uncovered bandwidth.

**Summary**

It can be seen that for both cases, the illegitimate decodings are greatly underestimated. Much higher bit compromising rate would be gained if an eavesdropper can exploit the special time and frequency structure of its received signal to decode. As a result, the jamming efficiency is overestimated in the existing literature if the transmitting signal is not stationary.

**5 JAMMING EFFICIENCY ENHANCEMENT BY WAVEFORM DESIGN ON JAMMING SIGNAL**

It has been pointed out in the previous section that using common Gaussian Noise or Fre-Match Noise as jamming signal presents relative low jamming efficiency in the case that the transmitting signal is not strictly stationary.

In this section, we further study how we can improve the jamming efficiency in practical scenarios. We notice from (6) that theoretically, jamming efficiency could be completely restored if the bandwidth of jamming signal \( r(t) \) matches that of transmitting signal \( x(t) \) all the time \( W_j(t) \approx W_i(t) \). Although perfect time and frequency bandwidth match is usually infeasible in practice due to the random structure of the jamming signal and synchronization offset, this observation still inspires us to study waveform design on jamming signal to replace unstructured jamming signal, making both time and frequency bandwidth of jamming signal largely match that of transmitting signal (denoted by Time-Fre-Match Noise).

To investigate whether the above idea can be transformed into a practical mechanism, we discuss the implementation details for generating Time-Fre-Match Noise to jam common quadrature amplitude modulation (QAM) and phase-shift keying (PSK) modulated signals in the remaining part of this section.

**Basic mathematical model of transmitting bit sequence**

We assume that the communication between Transmitter and Receiver adopts popular QAM or PSK, whose digital modulation schemes are represented by constellation diagrams as exemplified in Fig. 7.

We denote the waveform of the \( k \)th symbol of the transmitting signal \( x(t) \) as

\[
x_k(t) = h_T[I_k \cos(2\pi f_c t) + Q_k \sin(2\pi f_c t)]
\]

where \( I_k \) and \( Q_k \) are the values of the I-axis (in-phase component) and Q-axis (quadrature component) of the \( k \)th symbol as shown in Fig 7. \( h_T \) is the transfer function of the front-end of Transmitter.

![Fig. 6. Examples of the distribution of the optimal jamming efficiency for Jammer at different locations](image)
To explain the advantage of our design, let us consider a fluctuated voltage noise $r'_C$ with the average amplitude equal to $\alpha$ as shown in solid line in Fig. 8(a) (left). At decoding stage, Eavesdropper takes the average of the multiple sample points from its received signal. In this case, the fluctuation over $\alpha$ is cancelled out and $r'_C$ is equivalent to $r_C$ for Eavesdropper, but the flat voltage noise $r_C$ is more energy efficient than the fluctuated voltage noise $r'_C$ for Jammer.

5.3 Generate Gaussian Noise at Marginal Part
For marginal parts, the frequency domain representation is different from center parts as illustrated in Fig. 8(a) (right) and Fig. 8(b) (right). The energy is distributed wider around zero frequency in this case than the center part case.

We match the frequency components to generate common Gaussian noise at the marginal part between the $k$th symbol and the $(k+1)$th symbol $r_M(k, k+1) = [r_M(1), r_M(2), \cdots, r_C(l_M)]$.

$$r_M(j) = n_X, \quad 0 \leq j \leq l_M$$

where $n_X$ denotes a random value drawn from a Gaussian distribution.
In this step, Jammer stitches the flat voltage noise \( r_\text{C}(k) \) and Gaussian noise \( r_\text{M}(k,k+1) \) together to get:

\[
r_0 = [r_\text{C}(1) \ r_\text{M}(1,2) \ r_\text{C}(2) \ r_\text{M}(2,3) \cdots]
\]

To obtain the envelop of jamming signal, Jammer uses a digital-to-analog converter to transform \( r_0 \) to \( r_0(t) \) and then uses the same transfer function \( h_T \) that Transmitter uses to eliminate the energy of out-of-band signal and shape the frequency profile, so as to further increase the energy efficiency.

\[
r_X(t) = h_T r_0(t)
\]

where we use \( r_X(t) \) to denote the baseband waveform (the envelop) of random jamming signal as illustrated in Fig. 8(c): the waveform of the I (in-phase) component is mixed with flat lines and fluctuated curves.

In order to cover the transmitting signal of both in-phase and quadrature, we employ the above procedures to generate \( r_X(t) \) twice independently to get \( r_X^1(t) \) and \( r_X^2(t) \). Jammer modulates \( r_X^1(t) \) and \( r_X^2(t) \) with \( \cos(2\pi f_s t) \) and \( \sin(2\pi f_s t) \) respectively to get the jamming signal \( r(t) \).

\[
r(t) = r_X^1(t) \cos(2\pi f_s t) + r_X^2(t) \sin(2\pi f_s t)
\]

Finally, Jammer synchronizes the jamming signal with the transmitting signal and sends it.

### 5.5 Synchronization Consideration

It is worth pointing out that the tolerance to synchronization offset should be considered in jamming signal design since strict time synchronization is not achievable in practice [37]. Note that if jamming signal does not match the transmitting signal, some of marginal parts are not well covered; the jamming efficiency decreases consequently.

In Fig. 9, circle marked line shows the optimal jamming efficiency with respect to synchronization offset, where the parameters are the same as that used in Fig. 4 (a). As expected, the optimal jamming efficiency decreases as synchronization offset increases, with the jamming efficiency somewhat below that of Fre-Match Noise (as shown in solid line) if synchronization offset is larger than about 10\% of a symbol duration.

To mitigate the jamming efficiency drop caused by inevitable synchronization offset, Jammer should try its best to synchronize its jamming signal with the transmitted signal. Other than that, Jammer can slightly increase the signal width of Gaussian noise to add redundancy to make sure that all of the frequency spectrum of the marginal parts are still covered by jamming signal in the presence of a small synchronization offset, making a trade-off between the robustness against synchronization offset and the jamming efficiency performance.

In Fig. 9, cross marked line shows the case in which the signal width of Gaussian noise is extended by 10\% of a symbol duration. As can be seen that after adding this redundancy, the optimal jamming efficiency of Time-Fre-Match Noise is above that of Fre-Match Noise by about 40\%, as long as the random synchronization offset is less than 5\% of a symbol duration in either direction. Recall 10. the transfer function \( h_T \) can be estimated by the frequency profile of the transmitting signal if it is not directly available.
that the transmitting signal which presents non-stationary characteristic at symbol level often has very low symbol rate, so the required synchronization accuracy is normally achievable. 11

6 Performance Evaluation

In this section, we conduct numerical simulations in MATLAB to evaluate our design. We draw the simulation parameters from IEEE 802.15.4 standard. We set the bit rate to 250kbps, the center frequency to 2.4GHz and bandwidth to 2MHz. We assume that Alice encodes the digital signal using OQPSK method and uses a raised-cosine filter to shape the baseband waveforms of in-phase and quadrature components. It multiplies the baseband signals of I and Q components by a cosine and a sine carrier wave, respectively.

At Jammer and Receiver’s sides, they down convert RF signal by the same carrier waves and use a low pass filter to get the baseband signal. We set their sampling rates to 10Mbits/s. 12 We set their SNR to 20dB. We assume that the residue self interference of the full duplex radio possessed by Jammer is small (−30dB).

To decode the bit flow from the baseband signal, Eavesdropper may use one of the following strategies.

1) Constellation diagram decoder:

It is the most popular maximum likelihood detection [39] almost universally employed in practice. Upon reception of the signal, the demodulator examines the received symbol, which has been corrupted by the channel and the jamming signal. It selects, as its estimate of what was actually transmitted, that point on the constellation diagram which is closest (in a Euclidean distance sense) to that of the received symbol. Thus it will demodulate incorrectly if the corruption has caused the received symbol to move closer to another constellation point than the one transmitted.

2) Voltage slope decoder:

It exploits the voltage slope between two consecutive symbols to decode indirectly as introduced in Section 5.3. Voltage slope decoder pays attention to the sample points of marginal parts and ignores all sample points of center parts. It estimates the angle of the slope θk(Ik) between the kth symbol and the (k + 1)th symbol according to (20), and then decode the kth and the (k + 1)th symbols accordingly. Voltage slope decoder is an effective way to make use of the residue information to compromise the bit flow.

To quantify the impact of jamming signal on security enhancement, we introduce Eavesdropper’s bit recovery rate as security metric to compare with the secrecy outage probability (SOP) defined in (12). We draw energy efficiency curve to demonstrate the variation in bit recovery rate with jamming power.

• Bit Recovery Rate:

Bit recovery rate (BRR) stands for the Eavesdropper’s success rate of the decoding of a transmitted random bit sequence, calculated as the percentage of correct bit decoding over a random guess normalized to the interval of [0, 100%].

\[ P_{rec} = \frac{|50\% - P_{err}|}{50\%} \]  (24)

where \( P_{err} \) is the bit error rate (BER), measured by the number of bit errors divided by the total number of transmitted bits during a studied time interval. Especially, when \( P_{rec} = 0\% \), the BER is equal to 50\%, meaning that Eavesdropper’s decoding is equivalent to a random guess. When \( P_{rec} = 100\% \), the BER is equal to 0\%, meaning that Eavesdropper can deterministically decide the transmitting bit.

• Energy Efficiency Curve:

We normalize the average power of transmitting signal to unit \( \bar{P} = 1 \) and draw the energy efficiency curve \( P_{rec} = \eta(\bar{P}) \) to demonstrate the jamming effectiveness with respective to the average power of jamming signal. An energy efficient jammer is expected to lead to the lowest possible bit recovery rate at Eavesdropper for a given energy budget of jamming signal. Therefore, a lower curve indicates better performance.

Notation: It should be pointed out that, the statistical average BRR is not numerically equal to SOP. As an information theoretic metric, SOP is calculated based on the amount of leaked information that can be used by Eavesdropper, while BRR is a practical metric measuring the amount of bits being compromised by a specific decoding method. In this way, SOP is the upper bound of BRR. For example, even though the BER is 50\%, Eavesdropper may obtain some information that has not been used properly by the decoding method. In this case, BRR= 0 but SOP> 0. Nevertheless, for a reasonable decoding scheme, BRR can largely reflect SOP and the jamming effect. The smaller the Eavesdropper’s BRR, the higher the security strength provided by Jammer.

6.1 Effectiveness of Waveform Design

We evaluate the effectiveness of our proposed waveform design on jamming signal, Time-Fre-Match Noise, against...
6.2 Impact of Jamming Power on BRR

We then vary the normalized average jamming power $P_j$ from 0dB to 20dB to draw the energy efficiency curve $P_{rec} = \eta(P_j)$. For each point on the curve, we take the average of 1,000 simulations.

In Fig. 11, cross-marked lines show the average BRR as a function of $P_j$. For constellation diagram decoder in Fig. 11(a), Eavesdropper’s average BRR decreases from about 62% to 8% as the jamming power increases. For voltage slope decoder in Fig. 11(b), Eavesdropper’s average BRR decreases from about 38% to 4% as the jamming power increases. We can see that Eavesdropper’s bit recovery possibility converges quickly to 0% as the jamming power increases no matter what decoding method does Eavesdropper use.

For comparison, we also draw the energy efficiency curves in circle-marked lines for Gaussian Noise under constellation diagram decoder and Fre-Match Noise under voltage slope decoder. The circle-marked lines are located above the cross-marked lines as expected. It can be seen from Fig. 11(a) that the BRR of Gaussian Noise is larger than that of Time-Fre-Match Noise by 12% to 30% for all of the tested points. And to gain the same BRR, Gaussian Noise has to be set about 7dB to 8dB stronger than Time-Fre-Match Noise. It can also be seen from Fig. 11(b) that the BRR of Fre-Match Noise is larger than that of Time-Fre-Match Noise by 10% to 44% for all of the tested points. And to gain the same BRR, Fre-Match Noise has to be set about 10dB to 11dB stronger than Time-Fre-Match Noise. The results show that Time-Fre-Match Noise outperforms unstructured jamming signal for all of the tested cases.

Further more, to verify the validity of our reassessment, we draw the old calculations of the theoretical SOP curves in Fig. 11 in solid lines. As can be seen from Fig. 11(a) and Fig. 11(b) that, the BRR curves of Gaussian Noise and Fre-Match Noise are located above the theoretical SOP curves. Recall that as the upper bound of average BRR, SOP is typically higher than the practical BRR. This means that the existing method for calculating the SOP is not appropriate for non-stationary signals. There could be more leaked information that can be used by the Eavesdropper than previously assumed by taking the advantage of the special waveform structure. As a result, the actual SOP curve should be higher, so as to locate above the BRR curves, which is in agreement with our earlier reassessment.

On the other hand, the BRR curves of Time-Fre-Match Noise are located below the theoretical SOP curve. It can be inferred that jamming effect is largely restored by our waveform designed jamming signal. In this particular case, the rule that practical achievable BRRs are bounded by SOP
has been followed.

6.3 Impact of Modulation Order on BRR

We then investigate the performance of Time-Fre-Match Noise on different modulation orders. We keep the bit rate, center frequency and bandwidth unchanged to test 8PSK and 16QAM. We test both constellation diagram decoder and voltage slope decoder and choose the better one (the one that Eavesdropper gets higher average BRR). We vary normalized average jamming power $P_j$ from 0dB to 20dB to draw the energy efficiency curve. For each point on the curve, we calculate the average BRR of 1,000 simulations.

Fig. 12 shows the average BRR with respect to jamming power. The cross-marked lines, circle-marked lines, and triangle-marked lines show the performance of Time-Fre-Match Noise, Gaussian Noise, and Fre-Match Noise, respectively. The solid lines are the old calculations of the theoretical SOP curves.

It can be seen that the cross-marked lines are located far below the circle-marked lines and triangle marked lines. For 8PSK as illustrated in Fig. 12(a), the BRR of Gaussian Noise is larger than that of Time-Fre-Match Noise by 12% to 43%; the BRR of Fre-Match Noise is larger than that of Time-Fre-Match Noise by 10% to 40%. For 16QAM as illustrated in Fig. 12(b), the BRR of Gaussian Noise is larger than that of Time-Fre-Match Noise by 10% to 32%; the BRR of Fre-Match Noise is larger than that of Time-Fre-Match Noise by 8% to 29%. The results show that Time-Fre-Match Noise outperforms unstructured jamming signal for different modulation orders.

Similar to QPSK, for both cases, the solid lines are located below circle-marked lines and triangle marked lines but above cross-marked lines. This indicates that the existing method for calculating the SOP overestimates the jamming effect for non-stationary signals, while our proposed jamming signal largely restores the jamming effect.

6.4 Segmentation Robustness

Finally, we test the robustness of our proposed waveform segmentation method against channel noise.

We vary the receiving SNR at Jammer from 10dB to 30dB and use the segmentation method introduced in Section 5.1 to conduct simulations. To observe the segmentation accuracy, we define the segmentation error as the standard deviation of the distance between the ideal segmentation point and the actual segmentation point divided by the symbol length. Fig. 13 shows the average segmentation errors based on single symbol (solid line), 4 symbols (cross-marked line) and 20 symbols (circle-marked line), respectively, where for each point on the curve, we take the average of 1,000 runs.

It can be seen that the segmentation can be quite accurate. For only single symbol, the mean segmentation errors are less than 6.5% when SNR > 10dB. If more symbols in MAC header could be used, the segmentation error will further reduce. For example, if we average the segmentation results of 20 symbols, the mean segmentation errors could be less than 2% when SNR > 10dB.

**Notation:** It should be pointed out that our current segmentation algorithm is a preliminary one, aiming at validating the feasibility of the waveform design by considering only Gaussian noise environment. In practical implementation, due to the coexistence of various wireless transmission systems in the same spectrum span, there could be other types of interference. For example, the interference in short duration may have the similar magnitude. In this case, our short-term averaging scheme would fail to remove the interference. More complicated algorithms involving edge detection, feature classification discrimination and intersymbol comparison are needed to maintain the segmentation robustness under different noisy environment. This is a challenging and practical research direction and will be our future work.

6.5 Discussion

In previous sections, we take QAM and PSK as examples to demonstrate the correctness of our reassessment and the practical effectiveness of the idea of waveform design.

In theory, as long as the transmitting signal is non-stationary, according to our reassessment, there exist a decoding method for the eavesdropper to make use of the structured signal and compromise some extra bits than previously assumed and a corresponding waveform designed jamming signal to better protect the transmitting signal and prevent the eavesdropper from obtaining these extra bits. However, for more complicated transmitting signal, the actual realization could be difficult.

Let us take OFDM as an example.

First, it is a challenging task to find a proper decoding method for the eavesdropper. Although for each subcarrier, the QPSK modulated signals present the discussed structural waveform. The eavesdropper cannot simply apply the proposed voltage slope decoder, because for marginal parts,
there will be serious inter-carrier interference (ICI) due to the special crossing multi-carrier design.

Second, with the presence of multi-path, the accurate segmentation could be difficult. Same as in wireless communication, channel estimation and equalization are needed in OFDM systems. However, to perform equalization, the jammer needs to observe next few symbols to remove the multi-path impact from the current symbol. The delay may not be acceptable in this case.

Third, the spectrum variation of OFDM signals are more complicated. For example, due to ICI, the center parts of the modulated subcarrier signals are no longer flat voltages. Thus, it is necessary to develop more complicated waveform designs.

Fourth, multiple subcarriers mean much higher computational cost. Remember that the waveform designed jamming signal should be emitted within a short period of time. Computing time may not be sufficient.

From the view point of practical implementation, our current work is just the beginning of a new direction. There will still be a lot of works to be done for generalizing and refining the methods for improving the jamming efficiency.

7 Experiments

We conduct concept-proof experiments to demonstrate the effectiveness of our jamming waveform design. The experiment set up is shown in Fig 14(a). We use 3 software defined radios, USRP N210, to simulate Transmitter, Jammer (Receiver) and Eavesdropper, respectively. We use Daughter board SBX-40 as the transmitting and receiving front-end, where the nominal frequency range is 400MHz - 4.4GHz, and the nominal bandwidth is 40 MHz. We use antenna VERT 2450 to send and receive RF signals at 2.4GHz.

At Transmitter side, we refer to ZigBee transmission protocol which applies to IEEE 802.15.4 standard [34] to select the transmission parameters, where the modulation method is set to OQPSK (the constellation diagram is in section 4); the bandwidth is set to 2MHz (a digital low pass filter is used to shape the digital modulation signals before data sending).

At Jammer side, we use the method in Section 4 to generate jamming signal, where a flat voltage noise with random amplitude is generated for center part and Gaussian noise is generated for marginal part. The jamming signal is composed by stitching the two parts together. We set average ratio of jamming power to transmitting power at 10dB and send out the jamming signal synchronously with the transmitting signal.

At Eavesdropper side, we set the sampling rate to 10MHz which is more than double the bandwidth of the transmitting signal according to Nyquist theorem. In the experiment, we investigate a powerful Eavesdropper by letting that (1) She has line-of-sight attacking channel as exemplified in Fig 14(a). (2) She eavesdrops at different locations with respect to Transmitter and Jammer as shown in Fig 14(b). (3) All the overheard data are stored and processed in a desktop, so that Eavesdropper has no time and computational constraint.

Fig. 15 shows the snapshots of the received in-phase base-band signal at Eavesdropper. Fig. 15 (a) shows the original signal sent by Transmitter. Fig. 15 (b) shows the superposed signal sent by both Transmitter and Jammer. It can be seen that the jamming signal covers both the voltage level $I_k$ and the voltage slope $\theta_k$ between two consecutive symbols. In this case, Eavesdropper can no longer recognize the waveforms to decode.

We statistically validate the effectiveness of our proposed waveform design on jamming signal in a real-world configuration. We put Transmitter and Jammer close to each other and put Eavesdropper 1 to 2 meters away from them at 5 different locations labelled as location A to E as demonstrated in Fig 14(b). For each location, Transmitter sends a message of 1,000 random bits. We test both constellation diagram decoder and voltage slope decoder as introduced in Section 6.

Table 1 shows the BRR at Eavesdropper. It can be seen that our proposed jamming signal, Time-Fre-Match Noise randomizes the original waveform and causes low BRR at Eavesdropper for all 5 different locations. The BRRs are from 14% to 29% with the average of 21% for constellation diagram decoder, and the BRRs are from 12% to 28% with the average of 19% for voltage slope decoder. For reference, we also test two unstructured jamming signal, Gaussian Noise and Fre-Match Noise as introduced in Section 6. The results validate that Time-Fre-Match Noise is more secure.
than unstructured jamming signal for all cases. For Gaussian Noise, the BRRs are from 46% to 62% with the average of 54% for constellation diagram decoder; Time-Fre-Match Noise decreases the BRR by 33% on average in this case. For Fre-Match Noise, the BRRs are from 40% to 58% with the average of 46% for voltage slope decoder; Time-Fre-Match Noise decreases the BRR by 27% on average in this case.

We further test the decoding performance at legitimate jammer who cancels out the jamming signal and decodes the message in usual way. It can be seen from the table (4th column) that Jammer’s BRRs are close to 100% at all 5 different locations. The difference of BRR between Eavesdropper and legitimate jammer validates that our proposed Time-Fre-Match Noise presents high jamming efficiency in practical implementations.

**Table 1**
The BRR at Eavesdropper and legitimate jammer at different locations

<table>
<thead>
<tr>
<th>Jamming signal:</th>
<th>Time-Fre-Match Noise</th>
<th>Gaussian Noise</th>
<th>Fre-Match Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decoding method:</td>
<td>Constel-decoder</td>
<td>Slope-decoder</td>
<td>(J) Noise Cancel</td>
</tr>
<tr>
<td>Loc A</td>
<td>17.8%</td>
<td>23.3%</td>
<td>98.6%</td>
</tr>
<tr>
<td>Loc B</td>
<td>29.4%</td>
<td>12.8%</td>
<td>96.8%</td>
</tr>
<tr>
<td>Loc D</td>
<td>25%</td>
<td>15.2%</td>
<td>95.4%</td>
</tr>
<tr>
<td>Loc E</td>
<td>23.6%</td>
<td>11.6%</td>
<td>98.3%</td>
</tr>
</tbody>
</table>

8 Conclusion

In view that in a large number of scenarios the transmitting signals are non-stationary at symbol level scale, this paper rebuilt secrecy capacity model and re-evaluated jamming efficiency. Our reassessments revealed that jamming efficiency is greatly overestimated for many cases in the existing literature. We further proposed a waveform design on jamming signal to enhance the jamming efficiency for the first time. For jamming common PSK and QAM modulated signal, we divide the transmitting signal into short segments of middle parts and marginal parts. We introduce different jamming signal on each parts separately and synthesize a special jamming signal with mixed flat and fluctuated waveform.

Simulation results show that with our design, the power of jamming signal is dramatically reduced comparing with unstructured jamming signal. The BRR of Gaussian Noise is larger than that of our proposed Time-Fre-Match Noise by 12% to 30% for the normalized average jamming power ranging from 0dB to 20dB. And to gain the same BRR, Gaussian Noise has to be set about 7dB to 8dB stronger than Time-Fre-Match Noise. Fre-Match Noise, the weaknesses at marginal parts can be exploited by Eavesdropper. Facing voltage slope decoder, the BRR of Fre-Match Noise is larger than that of Time-Fre-Match Noise by 10% to 44% for the same jamming power range. And to gain the same BRR, Fre-Match Noise has to be set about 10dB to 11dB stronger than Time-Fre-Match Noise.

Concept proof experiments validated that Time-Fre-Match Noise is more secure than unstructured jamming signal under the same jamming power for all 5 tested locations. We conclude that our reassessment to jamming efficiency is valuable and of practical significance and our waveform design on jamming signal is simple, secure, and energy efficient.

**References**


