Secure and Optimized Unauthorized Secondary User Detection in Dynamic Spectrum Access

Xiaonan Zhang, Qi Jia and Linke Guo
Department of Electrical and Computer Engineering, Binghamton University,
State University of New York, Binghamton, NY 13902, USA
Email: {xzhan167, qjia1, lguo}@binghamton.edu

***Abstract*—Dynamic spectrum access (DSA) has been envisioned to become the key to solving worldwide spectrum shortage. However, the open nature of wireless medium brings severe threats to the DSA system resulting from unauthorized access. Specifically, unauthorized secondary user (SU) utilizes the licensed spectrum by faking/replaying the spectrum permit, which will not only introduce severe interference to authorized SU but also disable the DSA system due to the lack of stability and incentives. In this paper, we propose a secure and optimized unauthorized SU detection scheme. By optimizing permit modulation and embedding based on the current channel condition, we shorten the unauthorized SU's detection period and further improve the accuracy with low-complexity implementation. The proposed scheme ensures the security of DSA system and will further unleash its great potential. Extensive experimental results using both MATLAB and Universal Software Radio Peripheral (USRP) demonstrate the effectiveness, efficiency, and accuracy of our proposed scheme.**

***Index Terms*—Dynamic Spectrum Access, Unauthorized SU Detection, Security, Accuracy, Efficiency**

I. Introduction

The proliferation of mobile and interconnected devices has exacerbated the depletion of licensed wireless spectrum bands in the recent decades. Dynamic System Access (DSA) has received considerable attention recently due to its ability to alleviate the spectrum scarcity issue. In a DSA system, a spectrum operator, who regulates the licensed spectrum, authorizes the secondary user (SU) to opportunistically use the spectrum when it is not occupied by primary users. However, the open nature of the wireless medium makes the DSA system a potential target for unauthorized access. Specifically, by faking/replaying the spectrum permit (denoted as permit hereinafter), unauthorized SU can use any available spectrum bands and introduce severe interference to authorized SU who is currently using the designated spectrum bands. As a result, the authorized SU will lose interests on participating in DSA and thus the benefits brought by the DSA system are largely deteriorated. Therefore, it is highly needed to devise an efficient and accurate unauthorized SU detection scheme to ensure the DSA system and further unleash its great potential for future wireless systems with cognitive capabilities.

Physical-layer authentication is an effective way to distinguish unauthorized SU from authorized SU without having to complete higher-layer processing [1]–[5]. Specifically, the authorized SU embeds an unforgeable permit into its data traffic using techniques related to the physical layer. A third party named as the verifier passively eavesdrops on the SU's transmission and tries to detect and verify the permit. Yang *et al.* [2] add cryptographic permit into OFDM symbols for detection. Permit is concealed via inter-symbol interference in [4]. These two schemes negatively impact normal data transmission. Jin *et al.* [3] embed the permit by using dynamic power control on transmitted signals. FEAT scheme in [1] embeds the authentication information into the transmitted waveform by inserting an intentional frequency offset. It takes a long time to detect the unauthorized SU in these two schemes, which gives the unauthorized SU opportunity to transmit its information without being detected. By concealing the permit into the cyclic prefix in [5], the fake/replayed permit can be detected, which is impractical due to the modification of the existing physical layer protocols. These identified weaknesses motivate us to design an accurate, efficient and implementable unauthorized SU detection scheme, which not only ensures the current DSA system but also becomes a crucial component adapted to future wireless systems [6].

In this paper, we propose a novel unauthorized SU detection scheme based on hierarchical modulation [7], where permit symbols generated using a hash function and data symbols are synchronously aggregated before transmission. To overcome the intrusion to data transmission, the operator picks up a proper power allocation scalar between the permit and data transmission power, which allows the reliable transmission of both permit and data. Different from the traditional hierarchical modulation, the operator modulates the permit using rotation multiple layer modulation (RMLM), in which permit bits are first grouped, modulated, rotated and finally added together. By choosing proper rotation angles based on the current channel condition, which sensors in DSA obtain by performing channel estimation and then return to the operator, RMLM not only helps permit information to resist the noise but also prevents unauthorized SU faking/preventing the permit. The parameters related to the hash function, the power allocation scalar, the rotation angles in RMLM together with permit rotation angles are sent to the verifier through an authenticated and encrypted channel at the beginning of the spectrum authentication by the operator.

This work is supported by National Science Foundation under grants ECCS-1710996 and CNS-1744261.

978-1-5386-0683-4/17/$31.00

At the verifier, MMSE-SIC (Minimum mean square error-Successive interference cancellation) is deployed to detect the permit information. Together with RMLM, our scheme can achieve permit reliable transmission with high transmission rate [8]. Since no extra knowledge is needed at the authorized SU receiver, our scheme does not change the existing physical-layer protocols. We highlight and list our **contributions** as follows:

- We propose a novel unauthorized SU detection scheme, which prevents unauthorized users from capturing the authorized SU's spectrum bands.
- We deploy an improved hierarchical modulation to embed permit information into data transmission. A proper power allocation scalar is chosen to reduce the permit's intrusiveness to normal data transmission.
- Based on the current channel condition, we optimize the permit RMLM and achieve high efficiency and accuracy in unauthorized SU detection.
- By combining the permit embedding at the SU transmitter and MMSE-SIC at the verifier, a satisfactory permit error performance is achieved.

The rest of this paper is organized as follows: In Section II, we briefly review the existing unauthorized SU detection schemes and study the literature of RMLM and MMSE-SIC. Then, we give a description of our system model and the proposed framework in Section III. In Section IV, we elaborate the scheme from the following four parts: permit generation and encoding, permit modulation, permit embedding, and permit detection and verification. To show the security effectiveness of our proposed scheme, we analyze the resilience to emulation and replay attacks, as well as the comprising attack in Section V. Both permit and data detection performance are thoroughly evaluated in Section VI, followed by the conclusion in Section VII.

II. Related Work

In this section, we review the prior works closely related to our proposed scheme.

A. Unauthorized SU Detection

Previous methods on safeguarding the DSA system is to deploy cryptographic schemes [9]–[12] at the higher layers where messages carried by the waveform are detected for authentication. Different with those mechanisms, the physical layer-based authentication approaches enable a receiver to distinguish the authorized SU and the unauthorized SU without involving higher-layer processing. This fact brings obvious advantages on efficiency improvement. More importantly, the physical layer-based detection is indispensable in some cases. For example, in the heterogeneous coexistence environment, e.g., IEEE 802.22 and 802.11af systems coexisting in TV white space, incompatible system may not be able to decode each others' higher layer signals. Thus, the research on the physical layer-based detection approaches, such as RF fingerprinting in [13]–[15] and authentication signal embedding in [1]–[5], [16], [17], attract a lot of attentions.

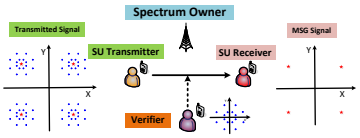


Fig. 1: System Model of the Optimized Detection Scheme

B. Superposition coding (SC) and MMSE-SIC

Hierarchical modulation is considered as a practical implementation of SC [18] while RMLM is the extension of SC. Tse *et al.* [8], [19]–[22] assume SC to be an alternative scheme for high throughput transmission. An interesting feature of SC is that the transmitted signal exhibits an approximately Gaussian distribution, which provides a more straightforward approach for achieving the so-called shaping gain [23]–[25] as demonstrated in [21]. Successive interference cancellation (SIC) is a physical-layer detection strategy at the receiver. As is described in [8], in SIC, one of the users, say user 1, is decoded treating user 2 as interference, but user 2 is decoded with the benefit of the signal of user 1 already removed. It has been proven that the transmission rate of users in the capacity region can be achieved by deploying SC at the transmitter and SIC at the receiver in [8]. Therefore, we apply SC and SIC to improve the accuracy and efficiency of both permit and data transmission.

III. System Model and Framework Overview

A. System Model

As shown in Fig.1, our system model contains three entities.

- Spectrum Operator: It refers to a licensed spectrum owner or a spectrum-service provider that regulates spectrum sharing. A typical example is the SAS in 3.5GHz band [26]. When a SU requests an unoccupied spectrum, the spectrum operator allows the SU transmission by sending it the spectrum authorized information. To prevent unauthorized access, the spectrum operator recruits multiple verifiers in the specific area. Besides, the spectrum operator optimizes the permit embedding by picking up a proper allocation scalar and rotation angles in RMLM according to the known current channel condition (In 3.5GHz, it is sensed by Environmental Sensing Capability sensors (ESC) and reported to SAS), which are sent to the SU and its nearby verifier. Either according to a pre-determined random schedule or when the authorized SU in a particular area reports abnormal interference, the spectrum operator authorizes the SU and the verifier to begin permit detection process.
- Secondary Users (SU): A SU requests and pays for a given licensed spectrum at the desired location and time. As soon as receiving permit detection indication from the spectrum operator, the SU transmitter embeds the permit into its data and transmits the aggregated symbols. The SU receiver has no idea about the permit embedding and detects data information without any changes on the physical layer.

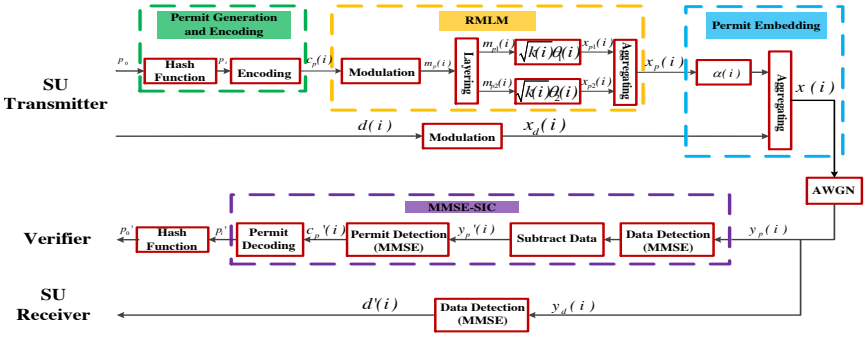


Fig. 2: Framework of the Secure and Optimized Detection Scheme

- Verifier: It extracts the permit information from the received signal and does not participate in normal data transmission. Even if the verifier detects data symbols, it cannot know the data information due to the lack of higher layer protocols. After authentication, the verifier reports its results to the spectrum operator who will then physically locate and further punish the illegitimate transmitters.

B. Attack Model

We define the attacker as the unauthorized SU who transmits without authentication either by accident or misconfiguration, or who illegally accesses the spectrum to avoid costs of spectrum occupation. Given the flexibility of today's cognitive radios, above operations can be done by controlling its transceiver to manipulate its physical-layer symbols. Without a valid permit, the attacker tries to compromise the spectrum by faking/replaying one. Meanwhile, we assume that the unauthorized SU is computationally bounded and cannot break the cryptographic primitives used to generate the permit. Finally, the unauthorized SU can compromise the verifier to report incorrect results to the spectrum operator.

C. Framework Overview

The framework of the proposed detection scheme is shown in Fig.2. The permit sequence p_i in time slot i is encoded as the coded bit sequence $c_p(i)$, which is then mapped into permit symbol sequence $x_p(i)$ using RMLM:

$$x_p(i) = \sqrt{k(i)}(m_{p1}(i)e^{j\theta_1(i)} + m_{p2}(i)e^{j\theta_2(i)}) \quad (1)$$

which is then added to the modulated data symbol sequence $x_d(i)$. Given the AWGN noise $n_d(i)$ with mean 0 and variance σ^2, the received signal $y(i)$ at the SU receiver is:

$$y_d(i) = x_d(i) + x_p(i)e^{j\alpha(i)} + n_d(i) \quad (2)$$

MMSE is used to detect the data bit sequence $d'(i)$ from $y_d(i)$.

The received signal $y_p(i)$ at the verifier is:

$$y_p(i) = x_d(i) + x_p(i)e^{j\alpha(i)} + n_p(i) \quad (3)$$

where $n_p(i)$ is the AWGN noise with the same mean and variance with $n_d(i)$. We apply MMSE-SIC to detect the permit p_i'. The verifier detects data symbols while treating permit symbols as interference at first. After subtracting detected data symbols, the remaining part is decoded as the permit p_i' using MMSE.

IV. Optimized Unauthorized SU Detection Scheme

In this section, we elaborate the proposed unauthorized SU detection scheme. Mutual information (MI) between the transmitter and receiver is a measure of transmission rate on the premise of reliable communication [8]. Therefore, we choose the rotation angle in permit RMLM by maximizing MI to achieve the accurate and efficient permit detection. As for permit embedding, the power allocation scalar and the rotated angle for permit symbols are discussed step by step. Due to the same detection scheme optimization in each time slot, we ignore the time slot expression i in the following.

A. Permit Generation and Encoding

Before elaborating the scheme in detail, we make three assumptions to ensure the entire process, which is the same as those in [3]. First, the geographic region is divided into non-overlapping cells of equal size to avoid the inter-cell interference. In each cell, we assume that the idle spectrum is divided into non-overlapping channels to prevent the intra-cell interference. Finally, time is divided into slots of equal length. To ensure the correct detection for permit and data, all entities are assumed to be loosely synchronized to a global time server.

An efficient one-way hash chain is deployed by the operator to generate the unforgeable spectrum permits. Denote $h(x)$ as a cryptographic hash function on x and $h^\eta(x)$ as η successive operations on $h(\cdot)$ to x. An SU transmitter requests a spectrum usage by specifying a band index, an area index, and a time duration γ. Receiving the request, the spectrum operator transmits a random number p_γ to the SU transmitter securely. The SU transmitter recursively computes $p_i = h(p_{i+1})$, $i \in [1, \gamma - 1]$ as its permit in time slot i. The spectrum operator also generates $p_0 = h^\gamma(p_\gamma)$ and sends it to the verifier.

To tolerate transmission errors resulted from the noise and reduce the hardware cost, the permit is encoded using repetition code $\mathcal{C}_m$ with system parameter m. Other encoding techniques, such as convolutional code and turbo code, can also be applied, which further improves the permit detection efficiency by paying the complexity cost.

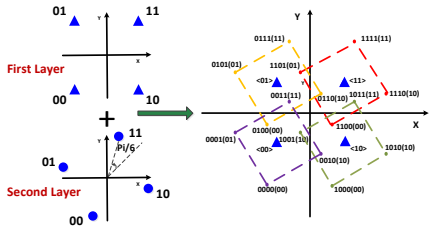


Fig. 3: An Example for Permit Symbol Constellation

B. Permit RMLM

Given the permit RMLM process in Fig.2, we first show an example of permit constellation assuming $\theta_1 = 0$ and $\theta_2 = \pi/6$ in Fig.3 after RMLM. We employ Quadrature Phase Shift Keying (QPSK) to modulate the permit bits. It is widely applied in many applications and standards such as IEEE 802.11b and IEEE 802.11g. General quadrature amplitude modulation is also supported. In Fig.3, the two bits in angle brackets represent permit bits in the first layer while those in parenthesis indicate permit bits in the rotated second layer. Every four bits correspond to one permit symbol.

1) Rotation Angle Effect: As shown in Fig.3, the choice of rotation angle affects the permit transmission reliability due to its effect on the minimum distance between permit symbols. In AWGN channel, increasing the minimum distance is an effective method to enhance the noise-resilient capability [27]. A worst case is $\theta_1 = 0$ and $\theta_2 = \pi/2$ under which the minimum distance becomes 0. The verifier cannot distinguish permit bits from the detected permit symbols. Therefore, how to choose a proper rotation angle becomes the key part in permit RMLM. Since the repition code $\mathcal{C}_m$ encoding the permit has an strong error correcting capacity of $(m-1)/2$, we consider the permit transmission quality instead of its recoverability at the verifier in our scheme. According to [28], the input−output MI is an indicator of how much coded information can be pumped through a channel reliably given a certain input signaling. Therefore, we pick up the rotation angle by maximizing MI.

Assuming we have subtracted the data symbols at the verifier. Since choosing the proper rotation angle is the same in each time slot, we rewrite the permit at the SU transmitter and the verifier as $U = U_1 + U_2 e^{j\theta}$ and $V = U + N$, where U_1, $U_2 e^{j\theta}$, U represent $\sqrt{k(i)} m_{p1}(i)$, $\sqrt{k(i)} m_{p2}(i) e^{j\theta_2(i)}$ and $x_p(i)$ respectively. The noise $n_p(i)$ in (3) is denoted as N with zero mean and variance σ^2. Our goal is to find a proper θ by maximizing MI between V and U:

$$\begin{aligned} \max_{\theta} \quad & I(U;V) \\ \text{s.t.} \quad & 0 \le \theta \le 2\pi \end{aligned} \tag{4}$$

where $I(U;V) = \sum_{u\in U, v\in V} p(uv) \log_2 \frac{\sum_{u'\in U} p(v|u')p(u')}{p(u)}$ [19]. The joint distribution of the input u and output v, the probability distribution function (PDF) of u, and the PDF of v on the knowledge of u' are $p(uv)$, $p(u)$, and $p(v|u')$, respectively. When the probability of each elements in U is equal, the MI gets the maximum value [19]. It is written as:

$$I(U;V) = \log_2 M - \frac{1}{M} \sum_{\substack{u_m \in U \\ v \in V}} p(v|u_m) \log_2 \frac{\sum_{u_j \in U} p(v|u_j)}{p(v|u_m)} \tag{5}$$

where $p(v|u_j) = \frac{1}{\pi\sigma^2} \exp(\frac{-|v-u_j|^2}{\sigma^2})$. M denotes maximum number of permit symbols after RMLM. Using QPSK modulation, $M = 16$.

2) MI Optimization: Denote $d_{mj} = \frac{u_m - u_j}{\sigma}$ and $t = \frac{v - u_m}{\sigma}$. Due to the complex and continuity of the received signal V, rewrite $I(U;V)$ in (5) as:

$$\begin{aligned} I(U;V) = & \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \exp\left(-|t|^2\right) \times \\ & \left\{ \log_2 \sum_{j=1}^{M} \exp\left(-2t \cdot d_{mj} - |d_{mj}|^2\right) \right\} dt \end{aligned} \tag{6}$$

Assume $f_m(t) = \log_2 \sum_{j=1}^{M} \exp\left(-2t \cdot d_{mj} - |d_{mj}|^2\right)$, $I(U;V)$ is expressed by Gussian-Hermite numerical integration as:

$$\begin{aligned} I(U;V) &= \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \exp\left(-|t|^2\right) f_m(t)\, dt \\ &= \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \sum_{p_1=1}^{P} W_{p_1} \sum_{p_2=1}^{P} W_{p_2} f(t_1, t_2) \end{aligned} \tag{7}$$

where P, W_{p1}, W_{p2}, t_1 and t_2 are the parameters that can be found in [29].

The $I(U;V)$ in (7) is a function with variable θ concealed in $f_m(t)$. The MI maximization problem becomes:

$$\begin{aligned} \max_{\theta} \quad & \log_2 M - \frac{1}{M\pi} \sum_{m=1}^{M} \sum_{p_1=1}^{P} W_{p_1} \sum_{p_2=1}^{P} W_{p_2} f(t_1, t_2) \\ \text{s.t.} \quad & 0 \le \theta \le 2\pi \end{aligned} \tag{8}$$

We solve the above optimization problem by a numerical global research method [30], which can be implemented using the MATLAB Global Optimization Toolbox. This method is a gradient-based algorithm using multiple randomized starting points to find different local optimal values of a smooth nonlinear optimization problem [31].

3) Rotation Angle Chosen: We figure the relationship between the rotation angle and the MI in Fig.4 assuming the Signal-to-Noise Ratio $SNR = 20$dB and $k = 0.25$. The opmital rotation angle is $\theta^* = \pi/4$ and the figure is about θ symmetric. In Fig.5, the permit constellations are plotted together when $\theta = \pi/6$ (red solid circle) and $\theta = \pi/3$ (blue hollow circle). Combining Fig.4 and Fig.5, we conclude that the permit constellations are totally different under different rotation angles even if their effects on MI are similar, e.g., $\theta = \pi/6, \pi/4, \pi/3$. Motivated by above

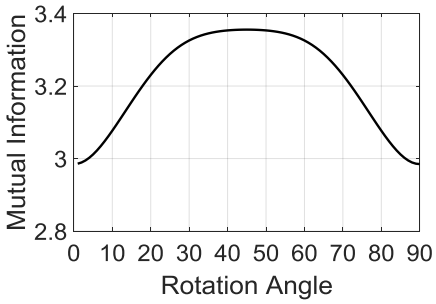


Fig. 4: MI vs Rotation Angle

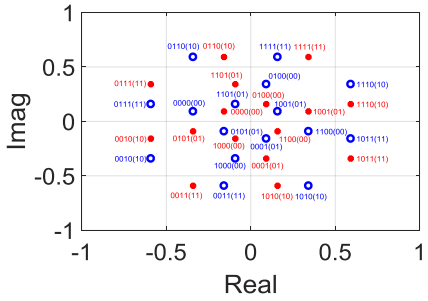


Fig. 5: Permit Contellation after RMLM

observations, the spectrum operator is designed to choose a list of sequential rotation angles randomly based on the current channel condition, e,g., $\boldsymbol{\theta} = \{\pi/6, \pi/4, \pi/3, \pi/3, \pi/4, \cdots\}$ at 20dB, which are sent to the verifier and SU respectively.

C. Permit Embedding

1) Power Allocation: Although the permit symbols and data symbols can be transmitted simultaneously, the embedded permit symbols are actually the interference of data symbols, which brings negative impacts to the data transmission. To alleviate such negative impact, we introduce the power allocation scalar k. Assume the unit total power, the power of the permit and the data is k and $1-k$ respectively. We will thoroughly investigate the power allocation via the experiment in Section V to choose a proper one under which the reliable transmission of both the permit and data is achieved.

2) RMLM Permit Symbol Rotation: The motivation to rotate RMLM symbols when embedded into data is to increase the data detection accuracy and further improve the permit detection performance. Specifically, we rotate RMLM permit symbols with an angle α when they are embedded to the data symbols in the first quadrant, such that the minimum distance between aggregated symbols and the vertical/horizontal axis is maximized. The aggregated symbols are then made symmetric along the vertical axis, the central point, and the horizontal axis to construct the constellation. Since QPSK and MMSE-SIC employed at the SU transmitter and the verifier respectively, the above minimum distance maximization effectively helps resist against the interference to the transmitted symbols brought by the noise. Data symbols are detected with better accuracy and thus an improved permit detection is achieved. Meanwhile, the data detection performance is also improved at the SU receiver.

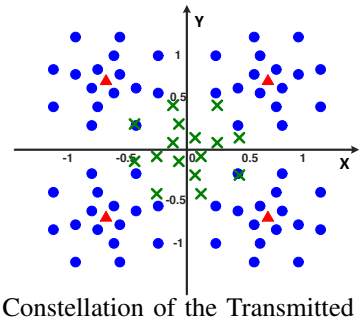


Fig. 6: Constellation of the Transmitted Symbols

An constellation example of the transmitted symbols is shown in Fig.6 with $k = 0.25$, $\theta = \pi/6$, and $\alpha = 0$, in which x marks, red triangles and green blue dots represent the constellations of the original permit symbols, the original data symbols and the final transmitted symbols respectively. In practice, a permit can be transmitted via one or multiple data packets. Permit embedding starts after the preamble and header transmission until either permit bits are all sent or the data symbols all are used up [3]. In our scheme, each data symbol carries four permit bits due to two layers' aggregation in RMLM. More permit bits can be embedded by increasing the number of layers.

D. Permit Detection and Verification

1) Permit and Data Detection: MMSE-SIC is deployed to detect the permit at the receiver. With the received signal, the verifier first detects each QPSK data symbol sequentially by using MMSE. Specifically, the verifier suggests the QPSK constellation point nearest to the received signal as the transmitted data symbol, e.g., red triangular in Fig. 6. The detected data symbol is then subtracted from the received signal. At the same time, the verifier makes a re-symmetry for the remained signal according to the position of the detected data symbol. If it is in the second/three/four quadrant, the verifier finds the point that is symmetric with the remained signal about the vertical/central/horizontal axis as the received permit signal. Similar with the data detection, the verifier detects the permit symbols using MMSE. According to the mapping rules between permit symbols and permit bits, the verifier can easily get the transmitted permit bits, which is then decoded as either 0 or 1 by using the hard-decision strategy. Since each permit bit has been consecutively repeated m times, the majority rule is then applied to determine each permit bit. Note that the verifier reconstructs the permit constellation based on k, α, and θ, e.g., green cross ($\times$) in Fig. 6.

Permit transmission and detection are totally transparent to the SU receiver as if it does not know the existence of permit. The SU receiver still performs QPSK demodulation.

2) Permit Detection in Practice: In practice, the start of the permit detection is similar with that in [3], [5]. The verifier keeps detecting the permit from physical-layer signals on the corresponding band in a specific duration. It first detects the

preamble for synchronization and obtains the packet size from the header, followed by the permit detection. If the verifier misses the preamble of the current packet, it detects the permit from the upcoming packet.

3) Permit Verification: Denote the detected permit in time-slot i as p'_i. To verify the transmitter's identity, the verifier computes p'_0 by i successive operations of the same hash function h on p'_i, $p'_0 = h^i(p'_i)$. If $p'_0 \neq p_0$, verifier suggests this transmitter is an unauthorized SU. Otherwise, the specific band is assumed to be securely used by an authorized SU. All the detection results are finally reported to the spectrum operator who will take further measures according to the receiving results.

V. Security Analysis

By emulating an authorized SU transmitter, replaying an overheard permit, or compromising the verifier to report incorrect results to the spectrum operator, the unauthorized SU may access the spectrum illegally. Our proposed scheme is resilient to above attacks.

A. Emulation Attack

A successful emulation attack is achieved if an unauthorized SU provides a proof of the SU transmitter's identity to mislead the verifier to believe that the current spectrum is occupied. Specifically, the unauthorized SU launches an emulation attack if it derives a fake permit which is the same as that of the SU transmitter. However, such emulation attack is impossible in our scheme. The unauthorized SU does not have the computational ability to break the cryptographic primitives. Therefore, it cannot obtain the permit in the next time slot without the root of the hash chain. However, the unauthorized SU may occasionally create the same permit. Fortunately, the length of the permit generated using hash function is long enough, so we can ignore such case. Taking SHA-1 for example, which is one of the most widely used cryptographic hash functions, it generates 160-bit values. The maximized probability of generating the same permit is $1/(2^{160})$, which is negligible. Therefore, our scheme can successfully prevent the emulation attack.

B. Replay Attack

Although the unauthorized SU cannot derive a fake permit, it may eavesdrop on a SU transmission, extract its permit, and then attempt to use it for its data transmission. To prevent the unanthorized SU from extracting the permit, we provide three barriers. As mentioned in IV-B-3) part, the angles calculated based on the current channel condition are put into the roatation angle list randomly, which is sent to the SU transmitter and the verifier through an authenticated and encrypted channel. Both the SU transmitter and the verifier process the permit using the rotation angles sequentially and consistently. Therefore, the first barrier in our scheme is the channel estimation. With wrong channel estimation, it is difficult for the unauthorized SU to know the rotation angle range. Even though the unauthorized SU guesses the range successfully, the randomness of the chosen rotation angles sets up a new obstacle for the unauthorized SU to know the current rotation angle based on the previous knowledge. Meanwhile, as shown in Fig.5, the constellation patterns of the permit under different rotation angles are totally different. Hence, the unauthorized SU is almost impossible to guess the permit exactly without the rotation angle. Taking a step back, if the unauthorized SU luckily extracts the current permit, it cannot replay the permit in the next slot without the hash root. Therefore, a lion is in the way for the unauthorized SU to extract the current permit and further replay one to deceive the verifier.

C. Compromising Attack

By compromising the verifier to report the wrong detection results to the spectrum operator, the unauthorized SU can access the spectrum "legally". To solve such problem, the spectrum operator deploys a number of verifiers to patrol the potential transmission area. By receiving detection results from various verifiers and combining them using known consensus distributed algorithms [32], the probability of wrong spectrum occupation judgment is greatly lowered.

VI. Performance Evaluation

In this section, we evaluate the performance of our secure and optimized detection scheme using both MATLAB simulations and the USRP experiment.

A. Evaluation Settings

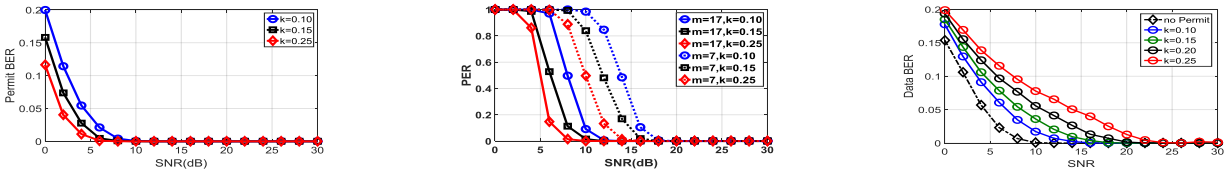
In the evaluation, we use SHA-1 with 160-bit long as the hash function for the permit generation. 100 data packages with payload length of 2000 bytes each are transmitted in each time slot. As shown in Fig. 2, we assume the aggregated symbols are transmitted in an AWGN environment with the noise variance σ^2, the power of which is normalized. SNR is defined as $SNR = \frac{1}{\sigma^2}$. We evaluate the permit detection performance based on permit bit-error-rate (BER) and permit error rate (PER). In particular, PER is approximated by the probability when all the 160 permit bits are correctly extracted. The data detection performance is measured using data bit-error-rate (data BER).

B. Results in MATLAB Simulations

1) Permit BER Performance: In Fig.7a, the permit BER decreases to 0 when SNR is near 15dB with $m = 17$ and $k = 0.10$. By increasing k, the permit BER performance improves. In a very poor wireless channel, e.g., SNR = 5dB, our detection scheme obtains a satisfactory permit BER performance.

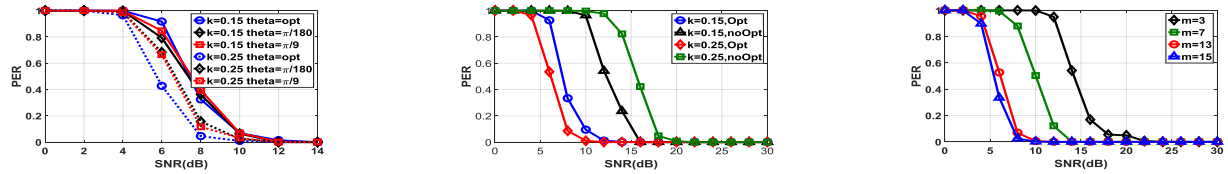
2) PER and Data BER Performance:

PER Performance. Since the one-way hash function is used, we have to ensure the correctness of each permit with



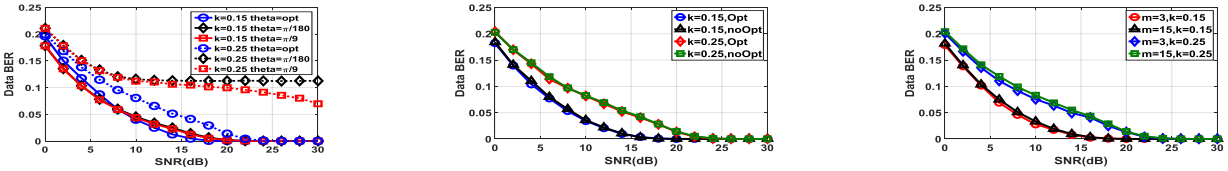
(a) Permit BER vs. SNR with $m = 17$ (b) PER vs. SNR (c) Data BER vs. SNR

Fig. 7: The Impact of Power Allocation Scalar k on Performance



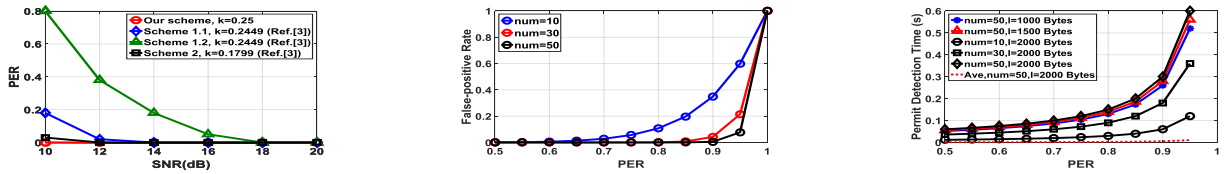
(a) Permit Modulation Optimization (b) Permit Embedding Optimization (c) Permit Detection with $k = 0.25$

Fig. 8: PER vs. SNR



(a) Permit Modulation Optimization (b) Permit Embedding Optimization (c) Permit Detection with $k = 0.25$

Fig. 9: Data BER vs. SNR



(a) Comparison with $m = 17$ (b) Accuracy (c) Efficiency

Fig. 10: Comparison, Accuracy and Efficiency

160 permit bits. The relationship between the permit BER P_b and the PER P_p is calculated theoretically as:

$$P_p = 1 - (\binom{m}{\lceil m/2 \rceil}(1-P_b)^{\lceil m/2 \rceil} P_b^{m-\lceil m/2 \rceil} + \binom{m}{\lceil m/2+1 \rceil}(1-P_b)^{\lceil m/2+1 \rceil} P_b^{m-\lceil m/2+1 \rceil} + \cdots + (1-P_b)^m)^{160} \quad (9)$$

In Fig.7b and Fig.8, we see that our scheme can achieve a very low PER. Taking the case with $m = 17$, $k = 0.25$ as an example, when SNR equals 2|4|6|8|10|12dB, the PER is 1.00|0.86|0.14|0.02|0.0009|0. We compare the PER performance between our proposed scheme and schemes in [3] as illustrated in Fig.10a. With the same repetition parameter $m = 17$ and similar power allocation scalar k, our scheme achieves a lower PER. Note that we evaluate the power allocation scalar in [3] by squaring its system parameter k. When $k = 0.4949$ and 0.4241 in [3], the power allocation scalar equals to 0.2499 and 0.1799.

The impact to Data detection. From Fig.7c and Fig.9, we see that the data can be correctly transmitted with SNR $>$ 15dB. This is consistent with the fact that accurate data transmissions are unlikely to occur in poor wireless channels. In addition, the data BER performance is compared between the case without permit transmission and the case with spectrum permits of different allocating power in Fig.7c, which shows that introducing permit brings 3dB SNR reduction.

To further show the relationship between the permit and the data transmission, we joint consider the performance of PER and data BER as shown in Fig. 11 with $m = 7$. When SNR $=$ 12dB, the power allocation scalar k is equaled to $0.10, 0.15, 0.2, 0.25$ and 0.3, respectively. The setting of k in other SNRs is similar. Obviously, the closer the curves to the origin, the lower decoding errors for the permit as well as the data BER. From Fig. 11, we find that the permit brings a negligible negative impact to the data transmission even in poor wireless channels [33]. When SNR $>$ 15dB and $k >$ 0.20, both PER and data BER approach to the origin.

Additionally, the performance of PER and data BER are affected by parameters and optimization variables related to our scheme. We discuss their influences as follows,

The Impact of Power Allocation Scalar. From Fig.7, we see that the power allocation scalar brings a positive effect on the PER whereas a negative effect on the data BER. It is because permit symbols are considered as the noise when data symbols are detected. Thus, permit symbols with

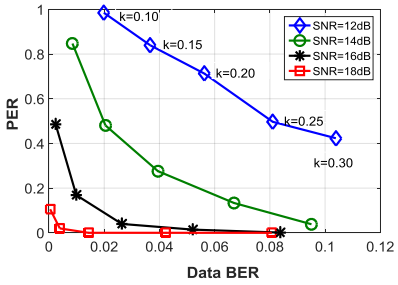


Fig. 11: Trade off between PER and Data BER

higher power make data detection vulnerable to the noise. An interesting observation is that the performance of permit detection mainly depends on k although the detection of permit symbols depends on that of data symbols. It gives a credit to the repetition encoding for permit symbols and the optimization in permit embedding. The optimization in permit embedding ensures that parts of permit symbols can be accurately detected even if data symbols are incorrectly detected. Combing with hard-decision decoding strategy, the PER performance is further improved.

Permit Modulation Optimization. Fig.8a and Fig.9a illustrate the results of permit modulation optimization with $m = 13$. Both PER and data BER decrease with an optimized permit modulation, which satisfies our expectations. By optimizing the rotation angle θ of permit symbols in the second layer, we maximize the MI of permit symbols, which increases their resistance to the environmental noise. The permit symbols with an optimal constellation introduce less noise to data symbols. Therefore, the performance of data BER is improved.

Permit Embedding Optimization. The effect of permit embedding optimization is shown in Fig.8b and Fig.9b with $m = 13$, in which "Opt" means that we rotate permit symbols and make a symmetry for them when they are embedding into data symbols whereas "noOpt" means permit symbols are added on data symbols directly. The data detection mainly depends on k and the permit embedding optimization contributes to permit detection. This can be supported by comparing the "Opt" and "unOpt" cases with $m = 13$ and $k = 0.25$ in Fig.8b. Without optimization, the PER of the permit detection depends on k and data detection simultaneously. When k is large, the incorrect data detection brings negative impacts on permit detection. As illustrated in the impact of power allocation scalar, the permit embedding optimization alleviates the negative impact on permit detection. Thus, "Opt" case outperforms "unOpt" case.

Permit Detection. Fig.8c and Fig.9c describe the impact of parameter m Since repetition encoding is applied to permit symbols, it has nothing to do with data BER. Due to majority rules in the decoding, the detection performance can be easily improved by increasing m. However, it also brings more redundancy to permit transmission. In the simulations, we find that increasing m brings better PER performance by sacrificing efficiency with m lower than 13. However, when $m > 13$, the PER cannot reduce more even if continuing increasing m. This reminds us to choose a proper m which both improves the PER performance and increases the acceptable redundancy.

3) Detection Accuracy and Efficiency:

False-positive and False-negative rates. Based on the PER results, we further analyze the false-positive rate as shown in Fig.10b with $m = 13$ and $k = 0.25$. The num in the figure implies the number of verification attempts for the permit. We can clearly see that the false-positive rate of our schemes is almost negligible even with a high PER. As for the false-negative rate, the probability that a fake permit is identified as authorized one is $(1 - P_p)/2^{160}$, which is too small to mislead the verifier. Hence, our proposed scheme can effectively defend both emulation or replay attack.

Detection Efficiency With the above false-positive rate, we compute permit detection time as follows. Denote l as the byte length of each data packet. Assuming the data is transmitted with a speed of 2 Mbit/s and repetition encoding parameter $m = 13$, Fig. 10c shows the impact of l and num on the permit detection time. Generally, the permit detection time increases with l. In particular, larger data packet means that the time gap between the transmission of two consecutive permits becomes longer, leading to longer permit detection time. With the same length of the data packet, the permit detection time increases with the number of the verification attempts. This is because the increment of the number of verification attempts will potentially increase the number of data packets, which results in longer permit detection time. No matter how many the number of verification attempts and data packet length are, the average detection time for each permit is the same, which is near to 10^{-3}s. Both permit detection time and average permit detection time demonstrate the high efficiency of our scheme.

C. Results in USRP Experiment

An experiment using USRP N210 [34] with GNU Radio is conducted in our lab. During the experiment, there are human activities such as walking. Since the phase ambiguity commonly exists in QPSK modulation in practice, differential QPSK, where the information bits are differentially coded, substitutes QPSK in our experiment [27].

The PER performance using USRP is shown in Fig.12. Both the power allocation scalar k and repetition encoding parameter m have a positive impact on the permit detection. However, the PER performance in the USRP experiment is worse than that in MATLAB simulations. Taking the case with $k = 0.25$ and $m = 7$ as an example, the PER is near to 0.3 when the SNR increases to 16dB in the USRP experiment, whereas the PER approaches to 0 when SNR is above 8dB in MATLAB simulations. We infer that it is due to the imperfect time and frequency synchronization together with the phase recovery. Poor phase recovery mechanisms bring a serious impact on the permit detection. Even worse, when k is decreased to 0.15, the verifier cannot detect the permit. This is because the received permit power is further lowered due to the attenuation of transmission signals, which submerges the

permit into the noise. Although the experimental results are not as good as those in MATLAB simulations, our scheme can achieve high detection accuracy in the good environment and outperforms Jin's work in [3] with proper parameters. In the case with $k = 0.3$ and $m = 7$, the PER is about $0.7|0.05|0.02|0.01$ when SNR approaches to $12|14|16|18$dB. This result demonstrates the effectiveness of our scheme.

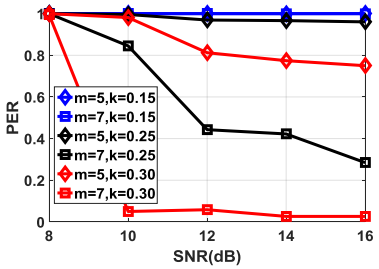


Fig. 12: PER Performance using USRP

VII. Conclusion

In this paper, we present a secure and optimized unauthorized SU detection scheme. Through optimizing both permit modulation and permit embedding, our scheme achieves accurate and efficient permit detection. Meanwhile, unauthorized SU is effectively prevented from faking/replaying the spectrum permit, which improves the security of the DSA system. The detailed MATLAB simulations and USRP experiment results have proven above advantages of our proposed scheme.

References

[1] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 787–798.

[2] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2012, pp. 195–204.

[3] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 172–180.

[4] V. Kumar, J.-M. Park, T. C. Clancy, and K. Bian, "Phy-layer authentication by introducing controlled inter symbol interference," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 10–18.

[5] X. Jin, J. Sun, R. Zhang, and Y. Zhang, "Safedsa: Safeguard dynamic spectrum access against fake secondary users," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 304–315.

[6] "Fcc claims us leadership in 5g with rules for millimeter wave spectrum," http://rethinkresearch.biz/articles/fcc-claims-us-leadership-in-5g-with-rules-for-millimeter-wave-spectrum/, July 2016.

[7] H. Jiang and P. A. Wilford, "A hierarchical modulation for upgrading digital broadcast systems," *IEEE transactions on broadcasting*, vol. 51, no. 2, pp. 223–229, 2005.

[8] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[9] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, May 2014.

[10] C. N. Mathur and K. Subbalakshmi, "Digital signatures for centralized dsa networks," in *First IEEE Workshop on Cognitive Radio Networks*, 2007, pp. 1037–1041.

[11] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 428–445, 2013.

[12] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 286–301.

[13] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 116–127.

[14] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3559–3563.

[15] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.

[16] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[17] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011, pp. 79–90.

[18] H. Méric, J. Lacan, F. Arnal, G. Lesthievent, and M.-L. Boucheret, "Combining adaptive coding and modulation with hierarchical modulation in satcom systems," *IEEE Transactions on Broadcasting*, vol. 59, no. 4, pp. 627–637, 2013.

[19] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[20] X. Ma and L. Ping, "Coded modulation using superimposed binary codes," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3331–3343, 2004.

[21] ——, "Power allocations for multilevel coding with sigma mapping," *Electron. Lett*, vol. 40, no. 10, pp. 609–611, 2004.

[22] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 371–377, 1977.

[23] R. F. Fischer, *Precoding and signal shaping for digital transmission*. John Wiley & Sons, 2005.

[24] U. Wachsmann, R. F. Fischer, and J. B. Huber, "Multilevel codes: theoretical concepts and practical design rules," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1361–1391, 1999.

[25] N. Varnica, X. Ma, and A. Kavcic, "Iteratively decodable codes for bridging the shaping gap in communication channels," in *Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on*, vol. 1. IEEE, 2002, pp. 3–7.

[26] F. C. Commission *et al.*, "Report and order and second further notice of proposed rulemaking," *Amendment of the Commissions Rules with Regard to Commercial Operations in the*, pp. 3550–3650, 2015.

[27] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[28] D. Guo, S. Shamai, and S. Verdú, "Mutual information and minimum mean-square error in gaussian channels," *IEEE Transactions on Information Theory*, vol. 51, no. 4, pp. 1261–1282, 2005.

[29] M. Abramowitz, I. A. Stegun *et al.*, "Handbook of mathematical functions," *Applied mathematics series*, vol. 55, p. 62, 1966.

[30] R. Krishnan, A. G. i Amat, T. Eriksson, and G. Colavolpe, "Constellation optimization in the presence of strong phase noise," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5056–5066, 2013.

[31] V. Brik, V. Shrivastava, A. Mishra, and S. Banerjee, "Towards an architecture for efficient spectrum slicing," in *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*. IEEE, 2007, pp. 64–69.

[32] G. F. Coulouris, J. Dollimore, and T. Kindberg, *Distributed systems: concepts and design*. pearson education, 2005.

[33] J. Geier, "How to: Define minimum snr values for signal coverage," *Viitattu*, vol. 23, p. 2012, 2008.

[34] "Usrp n210," https://www.ettus.com/product/details/UN210-KIT, July 2016.