2018 IEEE 15th International Conference on Mobile Ad-hoc and Sensor Systems

CREAM: Unauthorized Secondary User Detection in Fading Environments

Xiaonan Zhang, Pei Huang, Qi Jia and Linke Guo
Department of Electrical and Computer Engineering, Binghamton University,
State University of New York, Binghamton, NY 13902, USA
Email: {xzhan167, phuang13, qjia1, lguo}@binghamton.edu

***Abstract*—Dynamic Spectrum Access (DSA) has emerged as a major technology in the future wireless system to alleviate the worldwide spectrum scarcity issue. Authorized secondary users can take advantages of underutilized spectrum for communication. However, due to the open nature of the wireless medium, the DSA system suffers spectrum misuse by unauthorized secondary users, and thus fewer users would participate in DSA. Although many existing works have implemented misuse detection schemes into DSA, practical concerns, such as channel fading issues, are not well addressed. Therefore, how to ensure the reliable communication among authorized secondary users in a practical channel model becomes a challenging issue. In this paper, we propose CREAM, a physical-layer based misuse detection scheme specifically in the fading environment, which conceals the unforgeable spectrum permit into the message by superposition modulation for verification. Given the pre-shared secret information, the third-party verifier can perform efficient detection on unauthorized spectrum access. Detailed analysis and simulation results demonstrate the security, accuracy, efficiency, and low intrusion to message transmission in fading environments.**

***Index Terms*—Spectrum Misuse Detection, Fading Environments, Security, Accuracy, Efficiency**

I. Introduction

The exploding growth and popularity of wireless devices and services have exacerbated the depletion of licensed wireless spectrum in recent decades [1], [2]. Dynamic Spectrum Access (DSA) is a viable option to mitigate the above spectrum scarcity issue by allowing the spectrum sharing between primary users (PUs) and secondary users (SUs) [3], [4]. In particular, Federal Communications Commission (FCC) regulates that the spectrum sharing framework in 3.5 GHz allows the Citizens Broadband Service Devices (CBSDs) to opportunistically use the spectrum when it is not occupied by or interfered with the incumbent users (authorized federal and grandfathered fixed satellite service users). To effectively regulate the spectrum access, the spectrum operator in DSA usually issues a unique and unforgeable spectrum permit (denoted as permit hereinafter) to an authorized SU (aSU), which acts as an authorization to allow the aSU to occupy the dedicated frequency channel in the specified area and time duration [5].

Although the DSA is envisioned as a promising approach, quite a few practical concerns prevent it from actually implementing. On the one hand, specifically to the wireless environment, due to the atmospheric ducting, ionospheric reflection/refraction, and the reflection from terrestrial objects, the message transmitted via a wireless multi-path channel suffers dispersion, attenuation, and phase shift, all of which are known as fading effects [6]. On the other hand, the open nature of the wireless medium provides opportunities for unauthorized SUs (uSUs) to occupy the spectrum by faking/replaying the permit, which would cause severe interference to aSUs allocated to the same spectrum. As a result, no user would participate in the DSA system for improving the spectrum usage efficiency. Therefore, it is highly needed to devise an aSU authentication scheme to ensure the security of the DSA system in fading environments to further unleash its great potential for future wireless systems.

In this paper, we propose a spectrum misuse detection scheme in fading environments, **CREAM**, **C**onstellation **R**otation **E**mbedding for **A**uthenticating the authorized SUs based on superposition **M**odulation. CREAM conceals each aSU's permit into its message signal by superposing them into the power domain. To adapt to specific fading environments, interleaving is deployed and an optimization problem is constructed to find the optimal angle for constellation rotation prior to superposition modulation. A third party verifier, close to the aSU transmitter, passively monitors the signal transmission. Having a pre-shared secret on the related parameters with the aSU, e.g., power allocation factor, rotation angles, and the permit root, the verifier detects the permit using maximum likelihood (ML) estimation, followed by the transmitter identification. In general, CREAM has the following **salient features** that make it ideal for uSU detection in fading environments:

- **Security:** Without the complete knowledge of modulation parameters, uSUs cannot fake or replay the current permit of aSUs. When uSUs occupy the spectrum directly, the changes in the received signal's will alert the verifier. In both cases, spectrum misuse can be easily detected.
- **Accuracy:** We deploy the Orthogonal Frequency-Division Multiplexing (OFDM) as the modulation scheme. It is robust against the multi-path fading by separating a wideband signal into many smaller narrowband signals [7], [8]. In addition to that, the optimized constellation rotation produces significant gains by increasing the dimensionality of the signal in fading

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

2155-6814/18/$31.00 ©2018 IEEE
DOI 10.1109/MASS.2018.00064

environments. Therefore, CREAM effectively improves the performance for permit and message transmission and thus achieves low false-positive and false-negative rates for permit detection.

- **Efficiency:** Superposition modulation benefits the DSA system from achieving a high authentication rate [9]. Spectrum misuse can be detected in an extremely short time period. Meanwhile, the high authentication rate leaves little time for uSUs to fake or replay the permit.
- **Low-intrusion:** The closeness between the verifier and the aSU transmitter results in less path loss, which requires less power to achieve the reliable communication for the permit. Thus, the permit embedding exerts less intrusion to message transmission. Beyond that, the constellation rotation and interleaving for the message signals contribute to their transmission performance improvement in fading environments.

The rest of this paper is organized as follows: In Section II, we review the existing uSU detection schemes, along with a brief description of the fading environments and the techniques to defend against fading. Section III describes the system model and the proposed framework. The CREAM scheme is elaborated in Section IV from the following three components: permit pre-processing, permit embedding, permit post-processing. Particularly, Section V optimizes the constellation rotation in permit embedding process. In Section VI, we analyze the theoretical performance for CREAM, followed by a thorough evaluation of the permit and message performance using MATLAB simulations in Section VII. Finally, Section VIII concludes the paper.

II. Related Work

A. Unauthorized SU Detection

Methods for authenticating SUs can be classified into three categories. One is to utilize cryptographic schemes [10]–[13] at the higher layers. However, involving higher-layer processing lowers the authentication efficiency due to high time consumption. Meanwhile, incompatible systems may not be able to decode each others' higher layer signals [9]. The transmitter-unique "intrinsic" characteristics of the waveform, such as RF fingerprinting and electromagnetic signature identification [14]–[16], can also be deployed to identify transmitters. However, according to [9], those methods are sensitive to environmental factors, e.g., temperature changes, interference, etc, which limit their efficacy in real-world scenarios.

Recent methods focus on "extrinsically" physical-layer authentication scheme, in which a unique unforgeable signal is embedded in the message signal and then extracted at the receiver [5], [9], [17]–[19]. Yang *et al.* [17] embed the permit by duplicating sub-carriers in OFDM to achieve the desired and detectable cyclo-stationary feature. Such operations not only decrease the message throughput but also introduce high computational overhead. In [18], P-DSA is proposed to conceal permit via controlled inter-symbol interference, which negatively impacts normal message transmission. FEAT scheme in [9] enables the verifier to perform blind parameter estimation on multiple parameters of the OFDM signal, giving rise to a high computation complexity. Jin *et al.* [19] conceal at most two permit bits by changing the cyclic prefix length in each symbol of a physical-layer frame, resulting in low authentication rate. By controlling the power of the transmitted signals in [5], the permit is embedded given power constraint imposed on the transmitter. However, the first two schemes in [5] are mainly designed for AWGN environments and are not robustness to fading effects. Although another scheme is proposed to adapt to fading environments by changing the message constellation, it has a low authentication rate together with the first two schemes. Hence, CREAM rotates and superposes the permit and message to achieve a secure and reliable aSU transmission in fading environments with a high authentication rate and a low-complexity implementation.

B. Fading Environments

The phenomenon of fading is the time variation of the channel strengths due to the small-scale fading resulted from multi-path and moving, as well as larger-scale effects such as path loss via distance attenuation and shadowing by obstacles, which causes the attenuation of the signal at the receiver [20]. Multi-path fading causes the magnitude attenuation and the phase shift of the signal due to the atmospheric ducting, ionospheric reflection and refraction, and reflection from terrestrial objects such as mountains and buildings [21]. Rayleigh fading [22] is a stochastic model to show the effect brought by multi-path fading in which the envelope of the channel response is Rayleigh distributed and the phase of the channel response is randomly distributed between 0 and 2π. It is quite reasonable for scattering mechanisms where there are many small reflectors.

Constellation rotation is considered as a practical implementation of signal space diversity (SSD) [23]. By increasing the diversity order [20], the rotated signal transmitted over the fading channel has exactly the same performance of the nonrotated one transmitted over an additive white Gaussian noise (AWGN) channel [24]. By combining OFDM modulation scheme and constellation rotation, CREAM achieves the permit and message reliable transmission in fading environments.

III. System Model

A. System Model

As shown in Fig.1, our system model contains three entities. **Spectrum Operator**: Being an administrator and pivot in DSA system, it obtains the current channel estimation from dispersed sensors. For example, in 3.5GHz, Environmental Sensing Capability (ESC) is deployed to sense and then report the channel conditions. Receiving the spectrum request from each aSU, it chooses a proper allocation factor and constellation rotation angles based on the channel condition together with a permit root. These parameters are transmitted to the aSU and its nearby verifiers via an authenticated and encrypted channel respectively. When an aSU reports abnormal interference or when a pre-determined random schedule is required, it mandates the verifiers to begin uSU detection.

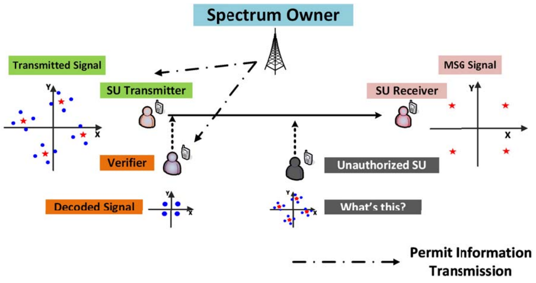


Fig. 1: System Model

Secondary Users: They request and pay for a given licensed spectrum by submitting their locations and time periods. Meanwhile, they embed the unique spectrum permits into the message signals to demonstrate their legal identities using the received parameters from the spectrum operator.

Verifiers: They are employed by the spectrum operator to help identify their nearby SU transmitters. The authentication results are sent to the spectrum operator. They do not participate in the message transmission.

B. Adversary Model

We define the attacker as a uSU who accesses the spectrum either by accident or misconfiguration, or to avoid costs of spectrum occupation. The above operations can be done by controlling its transceiver to manipulate its physical-layer symbols. By occupying the channels allocated to aSUs directly or with a faked/replayed permit, the uSU brings severe interference to aSUs. Meanwhile, we assume that the uSU is computationally bounded and cannot break the cryptographic primitives used to generate the permit. Finally, it can compromise verifiers to report incorrect results to the spectrum operator.

C. Framework Overview

The CREAM framework is shown in Fig.2, in which the superposed signal in time slot i is:

$$x(i) = \sqrt{P_p(i)}x_p(i)e^{j\theta_p(i)} + \sqrt{P_d(i)}x_d(i)e^{j\theta_d(i)} \quad (1)$$

where $x_p(i)$ and $x_d(i)$ are the permit and message symbols after encoding and modulation respectively. Their corresponding constellation rotation angles are $\theta_p(i)$ and $\theta_d(i)$ whereas $P_p(i)$ and $P_d(i)$ are their transmitted powers. Denote $x(i)$'s real and imaginary components as $x_R(i)$ and $x_I(i)$. After interleaving [25], it becomes:

$$x^{'}(i) = x_R(i) + jx_I(i-k) \quad (2)$$

which is remapped to OFDM symbols to be transmitted.

Denote $h(i)$ as the channel multi-path fading coefficient with expectation $E\{|h(i)|^2\} = 1$. At the verifier and the aSU receiver, the received signal is:

$$r(i) = h(i)x^{'}(i) + n(i) \quad (3)$$

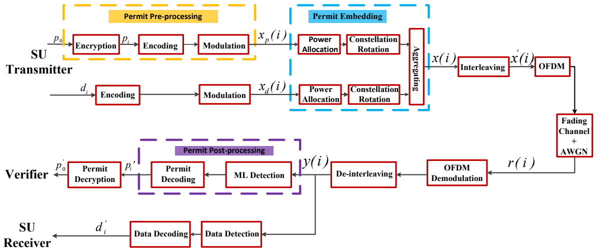


Fig. 2: Framework

where $n(i)$ is the equivalent AWGN noise with large-scale path loss absorbed into it. It has noise variances σ_p^2 and σ_d^2 at the verifier and the aSU receiver respectively. Assume perfect channel estimation, the received signal after OFDM demodulation and de-interleaving is:

$$y(i) = h(i)^*/|h(i)|r(i) = |h(i)|x(i) + \eta(i) \quad (4)$$

where $|h(i)|$ is the channel gain and the equivalent noise becomes $\eta(i) = h(i)^*/|h(i)|n(i)$. It has the same variance as the original noise $n(i)$. ML detection is deployed at both the verifier and the aSU receiver. Without loss of generality, we ignore index i in what follows.

IV. CREAM Scheme

According shown in Fig. 2, CREAM is divided into three sequential parts *permit pre-processing*, *permit embedding*, and *permit post-embedding*, each of which will be discussed respectively as follows.

A. Permit Pre-processing

Similar to [5], the spectrum and the geographic region are divided into non-overlapping parts respectively. The time period is split into slots of equal length. All entities are assumed to be loosely synchronized to a global time server.

- Generation: An efficient one-way hash chain is used to generate the unforgeable spectrum permits. Let $f(x)$ denote a cryptographic hash function on x, and $f^{\eta}(x)$ means η successive operations on $f(\cdot)$ to x. Assuming an aSU requests a spectrum in a time period γ. The spectrum operator sends a random number p_γ to the aSU. The aSU recursively computes $p_i = f(p_{i+1})$, $i \in [1, \gamma - 1]$ as its permit in time slot i. Meanwhile, the spectrum operator transmits $p_0 = f^{\gamma}(p_\gamma)$ to the verifier.
- Encoding: For simplicity, the permit is encoded using repetition code $\mathcal{C}_m$ to tolerate transmission errors resulted from the noise, in which each permit bit is repeated m times.
- Modulation: Quadrature Phase Shift Keying (QPSK), which has been widely applied in many applications and standards such as IEEE 802.11b and IEEE 802.11g, is chosen as the basic modulation scheme for both permit and message. General quadrature amplitude modulation is also supported.

B. Permit Embedding

As shown Fig.2, CREAM allocates the power to permit and message, followed by rotating their constellations with the optimized angles. Finally, the rotated permit and message are superposed with the Gray-mapping rule [8], in which constellation points with the minimum Euclidean distance have one-bit difference. A Grey-mapping constellation example after permit embedding is shown in Fig.3 with $\theta_d = \theta_p = \pi/6$ and $P_p = 0.1$, $P_d = 0.9$, where the first two bits represent message and the second bits in the bracket denote the permit.

In order to achieve low intrusion to the message, the permit and message power should satisfy:

$$P_p + P_d = 1, P_d > P_p > 0. \tag{5}$$

Fractional Transmit Power Allocation (FTPA) [26], as an effective power allocation method, is chosen in CREAM. In FTPA, the power of the permit is allocated as:

$$P_p = \frac{1}{(|h|/{\sigma_p}^2)^{-\alpha} + (|h|/{\sigma_d}^2)^{-\alpha}} (|h|/{\sigma_p}^2)^{-\alpha} \tag{6}$$

where $\alpha \in [0, 1]$ is the decay factor. The case of $\alpha = 0$ corresponds to equal transmit power allocation between the permit and message. When α is increased, the more power is allocated to the message. In CREAM, the spectrum operator thoroughly investigates the value of the decay factor via experiments such that the reliable transmission of both permit and message is ensured.

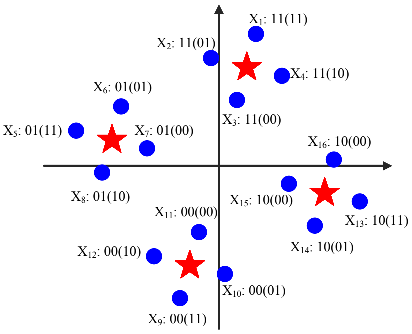


Fig. 3: An Example of Superposed Constellation

C. Permit Post-processing

According to Eq (2), interleaving the real and imaginary components of the superposed symbol x makes them being transmitted in different time. Hence, when the duration between the transmission of real and imaginary components is larger than the coherent time of the fading channel [20], their transmissions suffer independent fading effect. Therefore, different to Eq (4), the received signal after de-interleaving can be rewritten as:

$$y_R = |h_R| x_R + \eta_R, \quad y_I = |h_I| x_I + \eta_I \tag{7}$$

where $|h_R|$ and $|h_I|$ are the channel gains of the signal x's real and imaginary components, respectively. To ease the description, we rewrite $|h_R|$ and $|h_I|$ as h_R and h_I. In the Rayleigh fading model, they are *i.i.d.* Rayleigh random variables with distribution as follows:

$$p(x) = 2x/\beta \times e^{-\frac{x^2}{\beta}}, \quad x = h_R, h_I \tag{8}$$

where $\beta = E(h_R^2) = E(h_I^2) = \frac{1}{2}$.

At the verifier, ML is deployed. According to Eq (7), the ML metric for detecting x_p is:

$$M(x) = \exp\left(-\frac{(y_R - h_R x_R)^2 + (y_I - h_I x_I)^2}{\sigma_p^2}\right) \tag{9}$$

The bit Likelihood ratio (LLR) for the permit is written as:

$$L(i) = \text{In} \sum\nolimits_{x \in A_i^0} M(x) - \text{In} \sum\nolimits_{x \in A_i^0} M(x), i = 3, 4 \tag{10}$$

where A_i^l is a set of x whose i bit is l, $l = 0, 1$. If $L(i) > 0$, the i bit in x is detected as 0. Otherwise, it is detected as 1. The majority rule is applied to decode each permit bit. Permit transmission and detection are totally transparent to the aSU receiver as if it does not know the permit existence. QPSK together with ML detection is utilized at the aSU receiver.

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 f on p_i', $p_0' = f^i(p_i')$. If $p_0' \neq p_0$, the verifier suggests the transmitter as a uSU. The detection results are finally reported to the spectrum operator who will physically locate and further punish the transmitter.

V. Optimized Constellation Rotation in CREAM

In this section, we thoroughly investigate the how to optimize constellation rotation for permit and message in a specific fading environment.

A. Motivation

Consider the case without constellation rotation, $\theta_p = \theta_d = 0$ in Eq (1). the superposed symbol becomes:

$$x = \sqrt{P_p}(x_{p,R} + x_{d,R}) + j\sqrt{P_d}(x_{p,I} + x_{p,I}). \tag{11}$$

in which the real/imaginary component of x is only composed of the corresponding real/imaginary component of the permit and message respectively. Suppose that a deep fade hits only one of the components of the superposed signal, e.g., real component. Then, only the imaginary components of the permit and message survive. The integrity of the permit and message symbol is negatively affected.

While we rotate the constellation of the permit and message with θ_p and θ_d respectively, the real component of x in Eq (1) becomes $\sqrt{P_p}(x_{p,R}\cos\theta_p - x_{p,I}\sin\theta_p) + \sqrt{P_d}(x_{d,R}\cos\theta_d - x_{d,I}\sin\theta_d)$, whereas the imaginary component changes to $\sqrt{P_p}(x_{p,R}\cos\theta_p - x_{p,I}\sin\theta_p) + \sqrt{P_d}(x_{d,R}\cos\theta_d - x_{d,I}\sin\theta_d)$. Each component now contains all the components of the permit and message after rotation. Thus, even if one component suffers from deep fading, the integrity of the permit and message is still retained. The information involved in real and imaginary components of the symbol can be reconstructed. Fig. 4 shows a simple example to further illustrate the advantages of the rotation. With constellation rotation, any two points achieve the maximum number of distinct components.

In the case that one component is deep faded, e.g., imaginary component, the 'compressed' constellation in Fig.4b (empty circles) offers more protection against fading effect, since no components for any two points collapse together as would happen with Fig.4a.

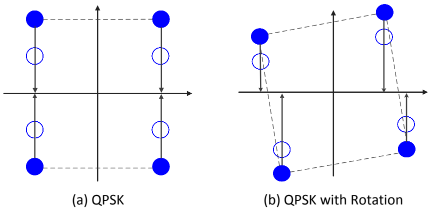


Fig. 4: Comparison between QPSK and QPSK with Rotation

B. Constellation Rotation Optimization

To effectively defend against fading effects, the constellation rotation is usually optimized by maximizing the minimum product distance or minimizing error probabilities when ML detection is deployed. However, it is difficult to obtain an explicit expression for the exact error probabilities [20]. Therefore, CREAM employs a suboptimal method, which is to minimize the permit symbol error rate (PSER) upper bound.

$$P_e \leq \frac{1}{N}\sum\nolimits_{i=1}^{N}\sum\nolimits_{k=1,k\notin\Gamma_{(i)}}^{N} P(x_i \to x_k) \tag{12}$$

where N is the size of the superposed constellation. $P(x_i \to x_k)$ is the pairwise error probability (PER) of confusing x_i with x_k when x_i is transmitted. $\Gamma_{(i)}$ is the set involving symbols that do not constitute a valid PER for x_i after permit detection. For example, when x_1 is transmitted, the detected permit bits are always 11 if the detected signal belongs to the set $[x_1, x_5, x_9, x_{13}]$ as shown in Fig.3.

PER in Eq (12) is refined as $P(x_i \to x_k) = \int_0^\infty \int_0^\infty P(x_i \to x_k|h_R, h_I)p(h_R)p(h_I)dh_R dh_I$ given the probability density function of channel gain $p(h_R)$ and $p(h_I)$, where $P(x_i \to x_k|h_R, h_I)$ is calculated based on Eq (9) as:

$$\begin{aligned}
&P(x_i \to x_k|h_R, h_I) = \\
&= P\left((y_R - h_R x_{k,R})^2 + (y_I - h_I x_{k,I})^2 \leq \right.\\
&\left.(y_R - h_R x_{k,R})^2 + (y_I - h_I x_{k,I})^2 | x_i \text{ is sent}\right)\\
&= P\left(h_R(x_{i,R} - x_{x,R})\eta_R + h_I(x_{i,I} - x_{k,I})\eta_I \leq \right.\\
&\left.-\frac{1}{2}h_R^2(x_{i,R} - x_{k,R})^2 - \frac{1}{2}h_I^2(x_{i,I} - x_{k,I})^2\right)\\
&= \frac{1}{2}\text{erfc}\left(\frac{1}{2}\sqrt{\frac{1}{\sigma_p^2}}\sqrt{h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2}\right)\\
&\leq \frac{1}{2}\text{exp}\left(-\frac{1}{4\sigma_p^2}\left(h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2\right)\right)
\end{aligned} \tag{13}$$

in which the third equation is derived because $h_R(x_{i,R} - x_{k,R})\eta_R + h_I(x_{i,I} - x_{k,I})\eta_I$ is a Gaussian random variable with zero mean and the variance $\Omega^2 = h_R^2(x_{i,R} - x_{k,R})^2 + h_I^2(x_{i,I} - x_{k,I})^2$. The inequality is based on the rule $P(X \leq x) = \frac{1}{2}\text{erfc}(\sqrt{x^2/2\Omega^2})$ [27].

Since h_R and h_I are the Rayleigh channel gain, $p(h_R^2)$ and $p(h_I^2)$ submit to the exponential distribution where $p(x^2) = e^{-x^2}$ [28]. $P(x_i \to x_k)$ in Eq (12) is finally expressed as:

$$\begin{aligned}
&P(x_i \to x_k)\\
&\leq \frac{1}{2}\int_0^\infty \text{exp}\left(-h_R^2\left(1 + \frac{1}{4\sigma_p}(x_{i,R} - x_{k,R})^2\right)\right)dh_R^2\\
&\times \int_0^\infty \text{exp}\left(-h_I^2\left(1 + \frac{1}{4\sigma_p}(x_{i,I} - x_{k,I})^2\right)\right)dh_I^2\\
&= \frac{1}{2\left(1 + \frac{(x_{i,R}-x_{k,R})^2}{4\sigma_p^2}\right)\left(1 + \frac{(x_{i,I}-x_{k,I})^2}{4\sigma_p^2}\right)}
\end{aligned} \tag{14}$$

Based on Eq (14), the upper bound for PSER P_{upper} in Eq (12) is:

$$P_e \leq \frac{1}{N}\sum_{i=1}^{N}\sum_{k=1,k\notin\Gamma_{(i)}^{N}} \frac{1}{2\left(1 + \frac{(x_{i,R}-x_{k,R})^2}{4\sigma_p^2}\right)\left(1 + \frac{(x_{i,I}-x_{k,I})^2}{4\sigma_p^2}\right)} \tag{15}$$

Since the constellation rotation angels θ_p and θ_d are concealed in x_i and x_k, the angles can be obtained by minimizing above PSER upper bound. The optimization problem in CREAM is as follows:

$$\begin{aligned}
\min_{\theta_p,\theta_d} \quad & P_{upper}\\
\text{s.t.} \quad & 0 \leq \theta_p, \theta_d \leq 2\pi
\end{aligned} \tag{16}$$

Based on Eq (15), P_{upper} mainly depends on the constellation pattern. In addition, different rotation angles may produce the same constellation pattern. Therefore, the PSER upper bound minimization is a non-convex problem. We deploy a numerical method by performing a global search with one-degree step.

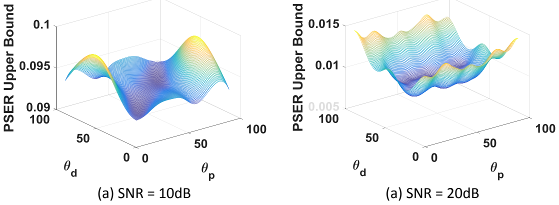


Fig. 5: PSER Upper Bound vs. SNR

TABLE I: PSER Upper Bound when $SNR = 10dB$

Upper Bound	0.0092	0.0092	0.0092	0.0092	0.0092
θ_d	19	20	20	70	71
θ_p	23	24	25	65	67

Two examples are shown in Fig.5 with $P_p = 0.1$ and $P_d = 0.9$. Meanwhile, Table I illustrates the minimized PSER upper bound with corresponding rotation angles θ_p and θ_d when $SNR = 10dB$. From them, we see that 1) the PSER upper bound has different shapes under different channel conditions, which verifies that the constellation rotation angles vary with the current channel condition; 2) the PSER upper bound minimization problem has multiple solutions. Such characteristics make CREAM a powerful scheme to prevent the uSU from replaying the permit.

VI. Scheme Analysis

In this section, we analyze the spectrum misuse detection efficiency, the computational complexity, and the security of CREAM.

A. High Detection Efficiency

Assume the permit is repetition coded with $1/7$ rate ($m = 7$) and the message is convolutional coded using $1/2$ rate. In IEEE 802.11a standard with 24Mbps message bit rate, the transmission rate for the permit bits is close to 7Mbps. FEAT [9] and SafeDSA [19] embed one permit bit into each OFDM frame. The permit bit transmission rate is at most $1/4$Mbps when there is only one OFDM symbol in each frame that includes 96 message bits. Compared with SafeDSA and FEAT, CREAM achieves a high authentication rate. For the uSUs who have not accessed the spectrum, CREAM leaves them little time to prepare the faked/replayed permit. For the uSUs who are occupying the spectrum, CREAM can detect them in a short time.

B. Low Computational Complexity

In CREAM, the transmission and reception of both permit and message use the basic physical-layer techniques. Although interleaving and de-interleaving are the most time-consumption operations, they only require a buffer to store the received signal without complex operations. Whereas in SafeDSA [19], the verifier needs to estimate the cyclic prefix length based on the message dependency test to detect each permit bit. Even worse, in FEAT [9], the verifier has to perform blind parameter estimation on multiple parameters of the OFDM signal. For complete blind estimation, the possible ranges of the parameters to be estimated need to be comprehensive, which covers all possible values and thus results in a high computation complexity.

C. High Resilience to Attack

Emulation Attack. A successful emulation attack is achieved if a uSU provides a proof of an aSU transmitter identity to mislead the verifier to believe that the current spectrum is not misused. Specifically, the uSU launches an emulation attack if it derives a faked permit which is the same as that of the aSU transmitter. Since the one-way hash chain is employed to generate the spectrum permits, the uSU does not have the computational ability to break the cryptographic primitives and therefore it cannot obtain the permit without the root of the hash chain. Unfortunately, the uSU may occasionally create the same permit. However, the probability of such a situation is so small that we can ignore it. Taking SHA-1 with 160-bit length as an example, the probability of generating the same permit is $(1/2)^{160}$. Therefore, our scheme can successfully prevent the emulation attack [29].

Replay Attack. The uSU may eavesdrop an aSU transmission, extract its permit, and then attempt to use it for its message transmission. CREAM provides several barriers to prevent the replay attack. Since the constellation rotation angles are calculated based on the current channel condition, it is difficult for the uSU to extract the permit from the received signals with wrong channel estimation. In addition, the characteristics of the minimized PSER upper bound allows for using different rotation angles in the same channel condition. Therefore, even if the uSU eavesdrops the angles by monitoring the permit transmission in the current slot, it does not know the rotation angles in the next slot, which confuses it when extracting permit. In addition to that, since it cannot generate the next permit based on the current eavesdropped one without the root of the hash chain, it is impossible for the uSU to replay the future permits to deceive the verifier. Therefore, CREAM is resilient to replay attack.

Free-rider Attack. In free-rider attack, the uSU hides behind the aSU by sending message parallel without permits [17]. Since the messages of the uSU and the aSU are independent, the free-rider attack would increase the number of the constellation points, which can be easily found by the verifier.

Compromising Attack. By compromising the verifier to report the wrong detection results to the spectrum operator, the uSU can access the spectrum "legally". The low computational complexity allows the DSA to employ a number of verifiers to patrol the area near the aSU transmitter. By receiving detection results from various verifiers and combining them using known consensus distributed algorithms [30], the probability of wrong spectrum occupation judgment is greatly lowered.

VII. Performance Evaluation

We evaluate the performance of CREAM in fading environments using MATLAB simulations. Specifically, three indoor environments are considered as listed in Table II and CREAM performance in fading environment 1 is mainly discussed. We show the performance in other two fading environments 2 and 3 by comparing with that in fading environment 1.

A. Simulation Settings

Adapting to indoor environments, we set parameters in CREAM with the help of IEEE802.11a standard, in which message transmission speeds as high as 54Mbps are possible. The main difference is that we consider CREAM performance in 3.5GHz band, particularly for small cell deployments [31] approved by FCC [32]. The system parameters are listed in Table III and Table IV respectively.

As for other default simulation settings, CREAM uses the 160-bit SHA-1 function to construct the permit. Each frame has a constant message payload length of 100 OFDM symbols. Hence, $N_s = \left\lfloor \frac{100*96}{160m} \right\rfloor = \left\lfloor \frac{60}{m} \right\rfloor$ permit is transmitted in each frame. Moreover, we transmit 500 frames to average each point in MATLAB results. As for power settings, we assume the superposed symbols are transmitted using the unit power. The received signal-to-noise radio at the verifier SNR_p and the aSU receiver SNR_d are defined respectively as follows:

$$SNR_p = \frac{1}{\sigma_p^2}, SNR_d = \frac{1}{\sigma_d^2}, \quad SNR_\delta = SNR_p - SNR_d > 0$$

TABLE II: Fading Parameters

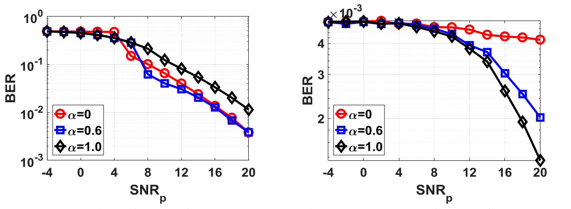
Parameter	Values
Moving speed	2.7km/h
1. Small office/ Home office	
Rms delay spread	50ns
Number of taps	5
2. Large office building	
Rms delay spread	100ns
Number of taps	10
3. Factory	
Rms delay spread	200ns
Number of taps	19

TABLE III: OFDM Parameters

Parameter	Values
Operation Frequence	3.5GHz
Sampling rate	20Mhz
IFFT/FFT sampling point	64
Subcarrier frequency spacing	0.3125MHz
Total Bandwidth	$16.25MHz$
OFDM Symbol Period	4μs
Guard interval	0.8μs
Number of message Subcarriers	48
Number of pilot Subcarriers	4

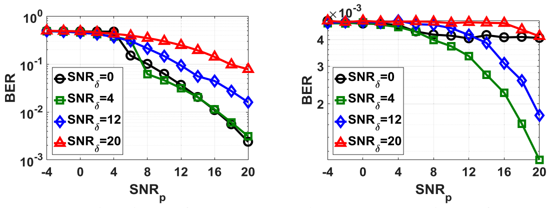
TABLE IV: System Parameters

Parameter	Values
message Encoding	$1/2$ Conv coding
Permit Encoding	$1/m$ repetition coding
Modulation	QPSK
Mapping	Grey mapping
Coded bits	96
message bits	48
Permit bits	$96/m$



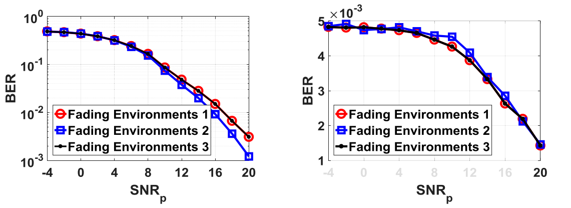
(a) Permit Bit Performance (b) Message Bit Performance

Fig. 6: Power Allocation Impact



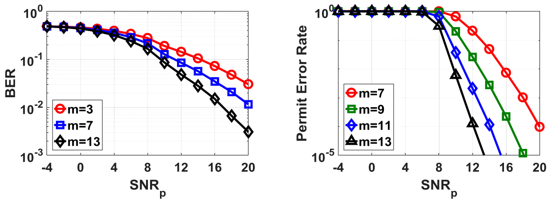
(a) Permit Bit Performance (b) Message Bit Performance

Fig. 7: SNR_δ Impact



(a) Permit Bit Performance (b) Message Bit Performance

Fig. 8: Fading Environments Impact



(a) Permit BER Performance (b) Permit Performance

Fig. 9: Repetition Encoding Impact

Since the aSU transmitter is further to the aSU receiver than the verifier as assumed previously, we denote SNR_δ as the received SNR difference. In the following simulations, $SNR_\delta = 10$dB. The default delay factor α is set to 1. Since ${\sigma_p}^2 < {\sigma_d}^2$, more power is allocated to the message to ensure its reliable communication according to (6). Each permit bit is repeated 7 times, $m = 7$.

B. CREAM Performance

We first evaluate the permit bit-error-rate (BER) and message BER performance. Permit BER is a basic measurement on the permit transmission accuracy, whereas message BER reflects the permit's intrusion to message. Further, we calculate the permit error rate, which describes transmission error for a whole permit composed of 160 bits. False-positive rate is also considered to measure the negative effect CREAM possibly brings to the aSU's transmission. Several key parameters affect the CREAM performance, including the SNR difference between the verifier and the secondary user receiver SNR_δ, the power allocation factor α, the rotation angles θ_p and θ_d, etc, all of which will be discussed in the following.

Note that although the physical-layer authentication work in fading environments is mentioned in [19] and [9], they do not illustrate the detailed factors, e.g., the moving speed, the time delay, and the multi-path. Therefore, we cannot compare the CREAM performance with these works directly.

1) Impact Factor:

The Impact of the Power Allocation. According to Eq (6), the power allocation between the permit and message depends on the decay factor α given SNRs. Fig.6a and Fig.6b show its impact on the permit BER and message BER respectively. By comparing these two figures, it seems that the decay factor puts an opposite effect on the permit and message transmission. When $\alpha = 0$, the power is allocated evenly. The permit is transmitted with the high power. However, it results in the loss of message power and brings serious intrusion to message. When the decay factor is near to 1, most power is allocated to the message transmission. The permit is easily affected by the fading effects and noise. Thus, permit BER has a poor performance. In practice, we have to ensure that the permit embedding brings the slightest negative impact on message transmission. Under this premise, we try to distribute more power to the permit.

The Impact of the Received SNR Difference. SNR difference between the verifier and the aSU receiver plays an important role in both permit and message performance as illustrated in Fig.7a and Fig. 7b. When they are near to each other, the message and permit transmission cannot be easily distinguished in the power domain. Hence, the message transmission is negatively affected by the permit. When they are far from each other and the permit is much closer to the aSU transmitter, a reliable permit transmission can be achieved with less power and thus more power is allocated to the message transmission to help it defend against the pass loss. However, when they are far apart and the aSU receiver is much further to the aSU transmitter, the message transmission would suffer larger pass loss and thus most power has to be allocated to the message, which affects the permit transmission negatively. As shown in Fig.7a and Fig. 7b, the message BER has a poor performance when $SNR_\delta = 0$dB and 20dB. The permit BER also performs poor at $SNR_\delta = 20$dB. When $SNR_\delta = 4$dB, both the permit and message can be transmitted accurately with a low BER.

Fading Environments. We simulate the permit BER and message BER under different fading environments in Fig.8a and Fig.8b, respectively. From them, we see that CREAM has a similar performance and performs well under three different fading environments. The difference is that permit transmission performs slightly better in large office building whereas message transmission has a better performance in small office/home office environments.

The Impact of the Repetition Code Rate. Fig.9a describes the permit BER performance using different repetition encoding rates $1/m$. From it, we see that a low rate helps improve the permit BER performance. According to [21], a repetition code with parameter m has an error correcting capacity $\frac{m-1}{2}$. Hence, when m is large, the permit BER has a good performance. However, a low encoding rate decreases the permit transmission rate and brings a negative impact on the authentication rate. We will discuss it later.

The Impact of the Rotation Angles. By optimizing the rotation angles in Section V, we can get a minimized PSER upper bound. Fig.10 compares the permit BER performance under different rotation angles. From it, we conclude that optimized permit rotation angle indeed improves the permit BER performance. Specifically, when the $SNR_p \in [0\text{dB}, 10\text{dB}]$, it brings almost 3dB gain.

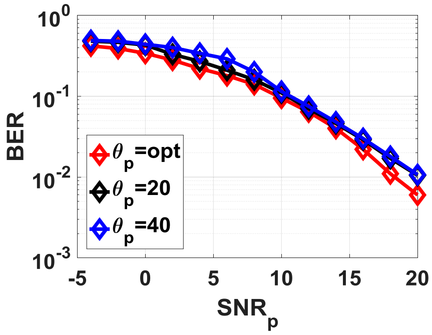


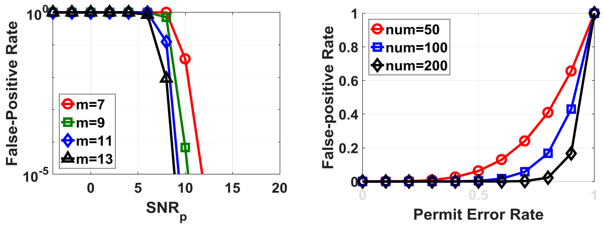
Fig. 10: θ_p Impact

2) *Detection Accuracy:*

Permit Error Rate. Since the one-way hash function is used to secure the authentication, CREAM has to ensure the correctness of each permit with 160 bits. Denote above permit BER as P_b. The permit length is $L = 160$, the permit error rate P_p can be calculated theoretically as follows:

$$\begin{aligned} P_p = 1 - (&\binom{m}{\lceil m/2 \rceil}(1-P_b)^{\lceil m/2 \rceil} P_b^{m-\lceil m/2 \rceil} \\ &+ \binom{m}{\lceil m/2+1 \rceil}(1-P_b)^{\lceil m/2+1 \rceil} P_b^{m-\lceil m/2+1 \rceil} \\ &+ \cdots + (1-P_b)^m)^L \end{aligned} \tag{17}$$

From Fig. 9b, we see that the permit error rate has a good performance above $SNR_p = 8dB$. Based on [33], the channel SNR in $[10, 15)$, $[15, 25)$, and $[25, 40)$ indicates very poor, poor, and very good wireless channels. Hence, the whole permit transmission can realize in CREAM even in poor channel conditions.



(a) Repetition Encoding Impact (b) Symbol Number Impact

Fig. 11: False-positive Rate

False-positive Rate and False-negative Rate. As shown in Fig. 11a, the false-positive rate performs better above $SNR_p = 5$dB, which means the aSU is mistakenly recognized as the uSU with an extremely low possibility even in a poor channel. Comparing Fig.9b and Fig.11a, m puts a more important impact to the permit error rate than to the false-positive rate. With the same number of transmitted message bits in each frame, the number of permits is decreased due to the low repetition rate. Therefore, we say that a large m lowers the permit transmission efficiency. Meanwhile, the number of OFDM symbols in each frame also affects the false-positive rate as shown in Fig.11b. With more OFDM symbols in each frame, each permit is transmitted more times. Since the verifier considers the transmitter as unauthorized when all the permits cannot be identified, the probability of identifying an incorrect aSU is lowered.

As for the false-negative rate, the probability that a uSU is identified as an aSU by successfully faking the 160-bit permit is $(1 - P_p)/2^{160}$. The probability is so small that the faking attack is considered as negligible.

3) *Intrusiveness to message:*

Finally, we compare the message BER performance between the case without the permit and CREAM in Fig. 12. Suppose that the SNR difference $SNR_\delta = 12dB$. When $SNR_p \in [4dB, 14dB]$, the actually received SNR at the aSU receiver is in $[-8dB, 2dB]$. From Fig. 12, we conclude that CREAM almost brings no negative effect on message transmission.

Instead, CREAM improves the message BER performance due to rotating the message constellation.

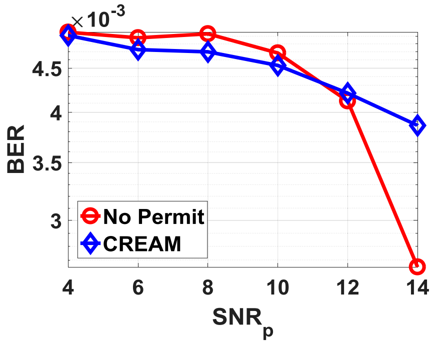


Fig. 12: Comparison

VIII. Conclusions

In this paper, we present a physical-layer unauthorized secondary user detection scheme referred to as CREAM. Combining the constellation rotation optimization, interleaving and superposition modulation in the OFDM framework, CREAM not only alleviates the negative effect of the aSU message transmission brought by fading, but also prevents the uSU from occupying the spectrum effectively. Detailed analysis and MATLAB simulation results have proven its accuracy, efficiency, security and low intrusion to message transmission.

References

[1] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2015-2020 white paper," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, Feb. 2016.

[2] X. Zhang, L. Guo, M. Li, and Y. Fang, "Social-enabled data offloading via mobile participation-a game-theoretical approach," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–6.

[3] Q. Dong, Y. Chen, X. Li, and K. Zeng, "An adaptive primary user emulation attack detection mechanism for cognitive radio networks," *arXiv preprint arXiv:1804.09266*, 2018.

[4] Q. Dong, Z. Yang, Y. Chen, X. Li, and K. Zeng, "Anomaly detection in cognitive radio networks exploiting singular spectrum analysis," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 2017, pp. 247–259.

[5] 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.

[6] M. S. Miah, M. M. Rahman, T. Godder, B. C. Singh, and M. T. Parvin, "Performance comparison of awgn, flat fading and frequency selective fading channel for wireless communication system using 4qpsk," *International Journal of Computer and Information Technology*, vol. 1, no. 2, pp. 82–90, 2011.

[7] R. Prasad, *OFDM for wireless communications systems*. Artech House, 2004.

[8] B. Sklar, *Digital communications*. Prentice Hall Upper Saddle River, 2001, vol. 2.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

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

[22] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. Prentice Hall PTR New Jersey, 1996, vol. 2.

[23] W. T. A. Lopes and M. S. de Alencar, "Performance of a rotated qpsk based system in a fading channel subject to estimation errors," in *Microwave and Optoelectronics Conference, 2001. IMOC 2001. Proceedings of the 2001 SBMO/IEEE MTT-S International*, vol. 1. IEEE, 2001, pp. 27–30.

[24] J. Boutros and E. Viterbo, "Signal space diversity: a power-and bandwidth-efficient diversity technique for the rayleigh fading channel," *IEEE Transactions on Information theory*, vol. 44, no. 4, pp. 1453–1467, 1998.

[25] M. N. Khormuji, U. H. Rizvi, G. J. Janssen, and S. B. Slimane, "Rotation optimization for mpsk/mqam signal constellations over rayleigh fading channels," in *Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on*. IEEE, 2006, pp. 1–5.

[26] A. Benjebbour, A. Li, Y. Saito, Y. Kishiyama, A. Harada, and T. Nakamura, "System-level performance of downlink noma for future lte enhancements," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 66–70.

[27] E. T. Jaynes, *Probability theory: The logic of science*. Cambridge university press, 2003.

[28] C. Walck, "Handbook on statistical distributions for experimentalists," 2007.

[29] N. Sklavos and X. Zhang, *Wireless security and cryptography: specifications and implementations*. CRC Press, 2007.

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

[31] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, 2016.

[32] "Fcc. report and order and second further notice of proposed rulemaking," https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-71A1.pdf, pp. 15–47, April 2015.

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