Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 2953986, 16 pages
https://doi.org/10.1155/2023/2953986

Research Article

Enhancing Spectral and Energy Efficiencies in a Cognitive Radio CRAN with PUEAs

Lilly Abau Yosia Odwa[1] **and Yueyun Chen**[1,2]

[1]*Department of Telecommunications Engineering, School of Computer & Communications Engineering, University of Science and Technology Beijing (USTB), 100083, No 30 Xueyuan Road, Haidan District, Beijing, China*
[2]*Shunde Innovation School, University of Science and Technology Beijing, Guangdong 528399, China*

Correspondence should be addressed to Yueyun Chen; chenyy@ustb.edu.cn

Received 6 September 2022; Revised 14 February 2023; Accepted 14 March 2023; Published 3 May 2023

Academic Editor: Fan-Hsun Tseng

In a cloud radio access network, malicious users mitigate the attributes of primary users in order to occupy a specific idle spectrum band by sending false signals or carry out a denial of service attack. Moreover, with the increase in number of users and limited spectral and energy resources, the malicious users will compete for the spectrum with legitimate users, thus resulting in increase in spectrum scarcity problem. The most widely used defense approach against malicious users is the received signal strength method. However, harmful users can still imitate signal attributes and transmit powers of the primary users. Therefore, in order to elaborate the best method to tackle this vulnerability and hence make more spectrum available, the modified adaptive orthogonal matching pursuit localization algorithm is proposed to detect harmful users existing in the network. However, in order to elaborate the convergence speed of the proposed method, the regularized particle filter algorithm is applied to evaluate the performance of the modified adaptive orthogonal matching pursuit under real-time conditions. The restricted isometry property is used for the performance evaluation. Further, spectral and energy efficiencies are used in the simulation results for performance evaluation, in order to observe spectrum and energy utilization efficiencies. The simulation results show that the proposed method is better in terms of computational complexity, spectral efficiency, and energy efficiency compared to other matching pursuit approaches.

1. Introduction

1.1. Motivation. Spectrum shortage problem experienced by wireless communication network users can be addressed by cognitive radio (CR) technology. In a CR network, secondary users (SUs) sense spectrum and access white space without bringing about any harmful interference to the primary users (PUs) [1]. However, the SUs generally have no overall information about the network spectrum resource utilization because a CR network should not interact with a primary network. Therefore, security is an essential problem among all the main technical issues of CR networks; however, it is not well addressed. Conventional wireless networks face security threats such as primary user emulation attacks (PUEAs) which is one of the common and severe denial of service attacks [2]. In PUEAs, a malicious attacker can imitate the characteristics of a PU and then send a false signal or conduct a wireless channel attack in order to occupy a specific unused frequency band [3]. Besides, the access node may prevent the SU from accessing the spectrum under the pretext that there is no free resource, when the SU wants to access spectrum resources. PUEAs restrain other legal SUs from using the spectrum hole or causing harmful interference to PUs. Nevertheless, cloud radio access network (CRAN) faces serious challenges of security threats and trust problems because of its transmission nature and self-organizing feature. Therefore, due to limited spectral and energy resources and increased number of connected devices, the malicious users cause spectrum unavailability to legitimate users by competing for the available spectrum with the PUs [4]. Therefore, there is a need for security approaches to sense and remove attacks from the system

without affecting spectral and energy utilization and causing delay. This paper focuses on detecting harmful users existing in a CRAN to guarantee the quality of experience of valid user.

1.2. Related Work. The received signal energy is used in most approaches in the literature to defend against PUEAs. An energy detection method and a cyclostationary calculation to indicate the features of the energy levels of a user have been proposed [5]. These features are then delivered into an artificial neural network. A new PUEA has been devised, a technique that estimates the invariance of the medium through which information is transmitted, and the variation of the PU received signal strength has been proposed [6]. This information is used to verify if it is a PU or a harmful user signal. Although the technique proves that the invariant of a medium is vital for PUEA prevention, if the PU received signal power is identical to the attacker's signal power, it will not work. Moreover, the received signal strength was proposed as a method to detect the PUEA location [7]. A method to confirm a transmitter based on the received signal strength through prove of the signal attributes, the intensity of the energy of the received signal, and the localization of the signal source has been devised [8]. Although this method can effectively defeat the PUEA, it intensifies load on the network and is easily disturbed by obstacles. The power level and the direction of arrival of a received signal are used by a SU to compare the received signal with that of the PU in order to differentiate the actual primary signal from malicious user's signal [9]. However, this method will fail if a harmful user is at a site where the direction of arrival and the received signal level are identical to the PU's signal. Furthermore, a novel multipath cluster-assisted single station localization method based on a genetic algorithm-based improved salp swarm algorithm was proposed to improve localization accuracy in an outdoor propagation environment. The localization is based on geometrical properties of propagation paths, such as angle of arrival and time of arrival [10]. However, the salp swam optimization algorithm has some conceptual and mathematical errors, which the improved version in [10] has tackled [11].

Nevertheless, cryptographic approaches have been proposed for the PUEA detection. A technique that produces an authentication tag and inserts it in the PU's signal has been presented [12]. This technique is noise sensitive, and thus, PU signals are distorted eventually. Moreover, the deployment of the advanced encryption standard at the transmitter, in order to prevent the PUEA without producing any change to the physical or system structure, has been proposed [13]. However, finding the location of the harmful user using the Taylor series necessitates a good initial value in order to give high-quality outcomes for the site of the intruder, and the accuracy of the method is low [14]. Nevertheless, in order to enable an SU to acquire authentic connection signatures of the helper node, a physical layer authentication scheme has been extensively studied. The signatures are acquired by placing a helper node near a PU, in order to verify whether the PU's signal is true or not [15]. However, the SUs cannot identify the authenticity of the information of the cryptographic signature and the signature authentic link when the helper node is assaulted.

Several studies propose the use of compressive sensing for detection. A sparse coding of the compressed received signal over a channel-dependent dictionary in order to detect primary user emulation and jamming attacks in CR using orthogonal matching pursuit (OMP) has been proposed [16]. Nevertheless, a Forward-Reverse OMP-Union-Subspace pursuit-based multiuser detection has been proposed, based on fused modified OMP-modified subspace pursuit algorithm to detect signal elements serially, in line with corresponding decrease in amplitude [17]. The use of one-class classification for detecting PUEA using sensing data collected at the fusion center in an infrastructure-based CR network has been investigated [18]. However, there are a number of drawbacks of one-class classification. There is a need to create complicated solutions that generalize well to more complex datasets. Besides, one-class classification cannot deal with adversarial data. Moreover, a deep network-based one-class classification approach is vulnerable to adversarial attacks. It is required to have a domain generalizable one-class classification. Further, it is hard to interpret decisions that one-class classification makes, and the proposed methods need to train one-class classifiers with distributed data [19]. A survey on various machine learning-based approaches in spectrum sensing, based on types of features extracted from PU signal has been conducted in the literature. It has been justified that supervised, unsupervised, and reinforcement machine learning algorithms are applicable in the cooperative spectrum sensing [20]. Moreover, in order to avoid the distributed denial of service attacks, a metaheuristic approach has been utilized to cluster the attack requests used on whale optimization algorithm-based clustering for distributed denial of service attack detection [21]. However, deep learning is costly, computationally extensive, and security-wise unreliable [22].

A number of studies were undertaken to investigate and utilize PUEA prediction methods. A joint Bayesian model and trilateration method is proposed in order to acquire a good approximation of a PU location using the received signal strength indicator [23]. Moreover, in order to reduce the impact of malicious attacks on a fading in wireless networks, a Neyman-Pearson composite hypothesis test-based analytical model was investigated in [24]. Furthermore, the PUEA in a CRN was considered, and Fenton's approximation and Wald's sequential probability ratio test were proposed to detect PUEAs without utilizing any location information [25]. However, the advantages between the Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test were analyzed [26]. It has been found that the Neyman-Pearson composite hypothesis test is more efficient against certain PUEAs than Wald's sequential probability ratio test analyzed, when the PUEA probability of signal loss is above a critical threshold. Moreover, both Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test do not apply to all network types. An improved energy detection approach than the conventional energy detection approaches was proposed using "hard" fusion OR/AND decision method that supposed a

PUEA assaults the network under a certain probability. [27]. However, costly hardware is required in situations where multiple transmitters or harmful users equipped with directional antenna exist [28].

Methods based on user position are stronger than the received signal strength- (RSS-) based defense techniques. The reason is that in most cases for RSS-based defense methods, harmful users are able to imitate the signal attributes and transmit powers of PUs. Therefore, if a harmful user is at a location where the direction of arrival and the received signal level are identical to the PU's signal, the malicious user would not be detected [2, 13]. As a target localization technique, compressed sensing (CS) is a spectrum sensing approach because of its accuracy, smaller sensing period, and sampling frequency [28]. Among the various methods of CS theory for localization, OMP method is more desirable due to its fast convergence and good reconstruction performance [2]. However, OMP algorithm has to run until the number of iterations equals to the number operations based on the number of transmitters and users [29]. Since the number of operations is constant, accuracy cannot guarantee for all the time. Moreover, the number of detection targets variation has not been considered in the literature. Therefore, in order to achieve a better performance, when the transmitters are varying and unknown with time, a CS theory for localization of signal sources based on adaptive orthogonal matching pursuit (AOMP) algorithm has been proposed [2]. However, the number of measurements can still be high since the AOMP has to run until the average mean square error meets a predefined stopping criterion. The modified adaptive orthogonal matching pursuit (MAOMP) was proposed as a gesture recognition algorithm [29]. Nevertheless, MAOMP has been proposed to detect PUEAs in cognitive radio network heterogeneous-CRAN (H-CRAN) [30]. In order to decrease the number of measurements to some extent and improve accuracy, the MAOMP method adopts sparsity estimation along with adjustable step size [29]. However, it does not provide a clear prove of how the method is fast. Moreover, the motivation and significance of MAOMP in CR networks were not identified. In order to reduce the number of iterations, the MAOMP approach adopts a bigger step size at the beginning. The step size is then reduced slowly, in order to improve accuracy. However, the computational complexity of the initial estimation of sparsity is increased. Therefore, the choice of the initial step size matters. When the initial step size is smaller, the step size will reduce to 1 quickly. Moreover, it is slow to converge when the initial sparsity is not close to the real sparsity. Nevertheless, it has been shown that when the real sparsity is greater, the real sparsity is twice the initial sparsity for any value of the restricted isometric property (RIP) constant [31]. Therefore, there is a big gap between the initial sparsity and the real sparsity. Hence, more iterations are needed for the algorithm to converge. Therefore, in order to overcome these setbacks, an appropriate step size coefficient to adjust the step size has been proposed [29]. Hence, due to the smaller number of measurements, the MAOMP can be faster than the preceding methods and thus can give excellent performance in real-time system conditions.

Several works that exist in the literature propose methods to solve problems such as in the medical field and in road traffic control. The authors of [32] proposed a method to detect human health. Useful information about a given sample placed in a collimator is obtained from the difference between former and latter sensed optical spectrum. In [33], particle filtering algorithms combined with the optimal parameter search criterion are used for the accurate extraction of autoregressive model-based respiratory rate from pulse oximeter recordings over a broad range. The discrete wavelet transform and OMP techniques are used to extract different coefficients from the electroencephalographic signals for automatic seizure detection from the continuous electroencephalographic monitoring data [34]. A compressive sensing based on OMP method and a rigrsure adaptive soft threshold noise reduction based on discrete wavelet transform method are proposed to extract the respiratory and heartbeat signals in patients [35, 36].

Moreover, in [37], road images were used to detect and count vehicles in order to control traffic flow in an intelligent manner. Medium filters were used for foreground processing, while histogram oriented gradient was used for training cascade classifier. In order to set a priority of a road, selection algorithm is used. Further, a real-time state estimator and predictor are presented in [38]. The authors focused particularly on enabling of detector fault alarms and also its relation to queue-length-based traffic control using particle filter. Unlike the works in [32–38], the proposed method in this paper uses previous RF channel state to predict the next channel state and then applies MAOMP to detect PUEAs existing in the network.

In the medical field, particle filtering gave accurate results [33]. Besides, the OMP has been proved to be specific, accurate, and sensitive in its results. Moreover, OMP combined with discrete wavelet transform effectively suppresses noise in remote monitoring of human vital signs [34–37]. Furthermore, particle filters used in traffic control produce results that are satisfactory and promising for further work on developing a hybrid model that may be more practical to achieve automatic adaptation to changing system conditions [38]. The physical implementations of the studies in [32–38] are different from the one in this paper. Particle filtering and sparse representation are used to solve problems in the medical field and road traffic control [32–38]. In this paper, an optimized regularized particle filter (RPF) is used to predict the next state of an RF channel in a CRAN with cognitive radios. The RPF is fast and useful for real-time tracking [39–41]. Moreover, MAOMP is a sparse representation method with improved accuracy and speed than OMP. Thus, it can give excellent performance in real-time system conditions [29]. Therefore, it is promising that more accurate and faster results can be obtained when RPF MAOMP is applied in both medical applications and road traffic control than the methods in [32–38].

1.3. Contributions. In this paper, the RPF algorithm has been applied in order to evaluate the performance of MAOMP under real-time conditions. The proposed method consists of two parts: spectrum prediction and PUEA detection.

Once the next state of the channel is predicted, the MAOMP algorithm is applied in order to detect and drop PUEAs existing on the network. Hence, this approach will contribute greatly in efficient spectral and energy resource utilization. The novelty of this study is as follows:

(1) In order to identify the existence or absence of harmful users in the network, the MAOMP method is utilized when the RPF channel state prediction algorithm is used and when it is not used

(2) In order to reduce the computational complexity, an appropriate step size coefficient is used to adjust the step size

(3) To evaluate the performance of the MAOMP algorithm, the RIP is utilized. Spectral and energy efficiencies are used to evaluate the performance of the proposed algorithm. Moreover, the acquired detection results are compared with OMP, AOMP, and sparsity adaptive matching pursuit (SAMP) methods

(4) The computational complexity of OMP, AOMP, SAMP, and MAOMP algorithms is calculated, and the results are illustrated in graphs

The organization of the remaining part of this paper is as follows. The proposed method is illustrated in Section 2. The problem formulations and algorithm are presented in Section 3. The simulation results are presented and discussed in Section 4. Lastly, the conclusion of this paper is presented in Section 5.

2. Proposed Method

2.1. System Model. Consider a centralized CRAN setting in which baseband units (BBUs) and transmitters are connected by a common public radio interface (CPRI); the configuration is shown in Figure 1. Each BBU, located in the BBU pool, is assigned to each RRH. The BBU functions as a virtual base station to process baseband signals and optimize resource allocation of the network. In downlink, the RRHs transmit the radio frequency (RF) signals to user equipment (UE) while in uplink; they forward the baseband signals from UE to the BBU pool for further processing. A set $M = \{m_1, m_2, m_3, \cdots, m_M\}$ of M transmitters is assumed to serve n users. Each transmitter is assumed to have its own capacity of channels. Suppose the total number of users assigned to be served by all transmitters is represented by the set $U = \{u_1, u_2, u_3, \cdots, u_n\}$. The configuration is shown in Figure 1. The users are uniformly distributed within the coverage area of each transmitter. All transmitters are expected to provide coverage to users that are located within their coverage area.

Consider that a cloud computing unit stores location information of free spectrum bands. The cloud is used to analyze the sensed information and store the locations of the free spectrum bands. Each spectrum sensor reports its sensing information to the cloud server. A location database is maintained in the server located in the cloud. The location database is used to store position information of free bands and SUs and update the information in real time.

Let us consider transmitters m1 and m2 in Figure 1 for simplicity. Suppose a set of SUs located within the coverage area of a transmitter, with demands greater than the available bandwidth, want to gain access to the transmitter. Due to the limited bandwidth, some SUs are deprived of gaining access to the spectrum on the transmitter. Therefore, they will monitor the spectrum on other neighboring transmitters to opportunistically gain access to those transmitters. Assume that some SUs at the edge of their transmitters act as adversary SUs by imitating the PUs. Hence, the PUEAs should be detected with accuracy and proper number of iterations. The links between the transmitter and the PUs, SUs, and PUEAs are shown in blue, green, and red colors, respectively, as illustrated in Figure 1.

Let us assume that the current state of a channel $x_{(t)}$ changes from the previous state $x_{(t-1)}$ based on the channel impulse response $h^m_{u\,(t)}$. Based on the current channel state, a user objective is obtained and denoted by $y_{(t)}$ at time episode t. The function that links the state $x_{(t)}$ to the user objective is denoted by $\gamma_{(t)}$. Therefore, the system model is given by

$$x_{(t)} = h^m_{u\,(t)} x_{(t-1)} + \nu_{t-1}, \tag{1}$$

$$y_{(t)} = \gamma_{(t)} x_{(t)} + z_t, \tag{2}$$

where ν_{t-1} and z_t are additive white Gaussian noises with zero mean and unit variance.

Assuming that the SUs are uniformly distributed within the coverage area of the transmitters, the received power of the PUs and SUs depends on the pathloss, the shadow fading, and the transmit power of the transmitters. Therefore, the received power of user u is calculated by

$$P_u = P_t + \mathrm{SF}^m_u - \mathrm{PL}^m_u, \tag{3}$$

where P_t is the remote radio head (RRH) transmit power, SF^m_u is the shadow fading, and PL^m_u is the pathloss. The pathloss depends on the environment of the user. The fading channel between transmitter m and user u at time episode t is modeled by the p^{th} order autoregression process (AR(p)) [39]. Therefore, the channel impulse response at time episode t is given by

$$h^m_{u\,(t)} = \sum_{i=1}^{p} \propto_i h^m_{u\,(t-1)} + \beta \nu^m_{u\,(t)}, \tag{4}$$

where $h^m_{u\,(t-1)}$ is the channel fading impulse for transmitter m and user u at time episode $t-1$. $\propto_i$ and β are the autoregression (AR) parameters, which assume that $\propto_i = J_0(2\pi i f_d T_d)$. J_0 is a zero order the Bessel function of the first kind, f_d is the Doppler frequency, and T_d is the coherence time of the channel. Suppose other users try to cause interference to user u as they attempt to connect to the same channel with u

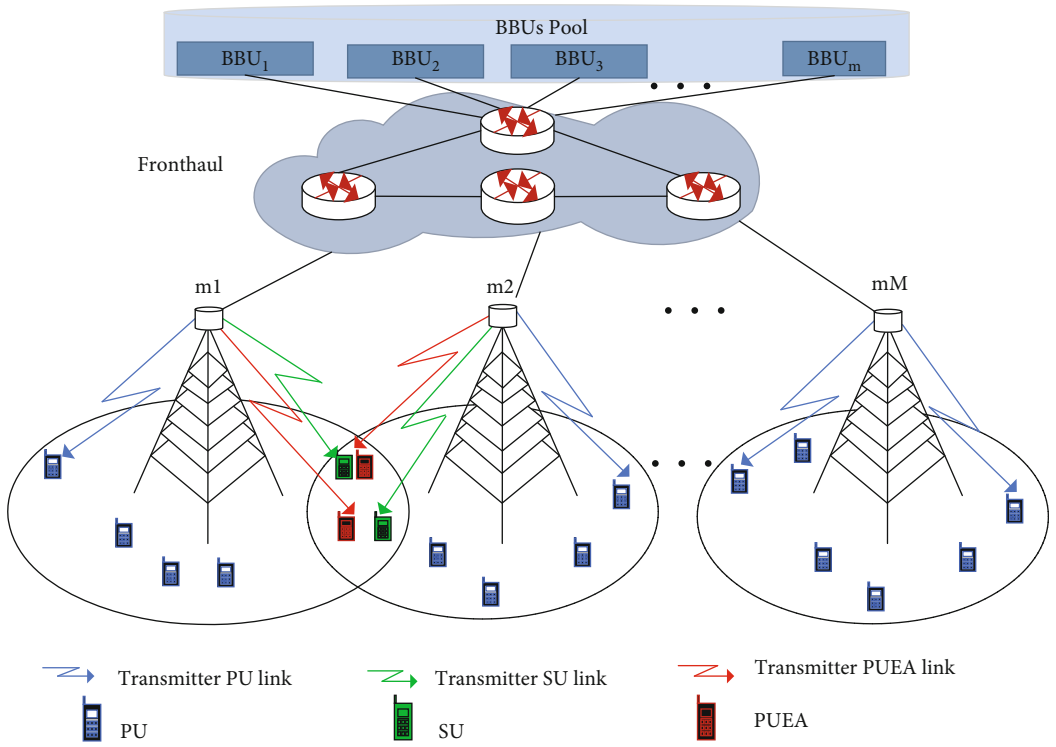

FIGURE 1: A system model for a cognitive CRAN configuration with PUEAs. Due to the limited bandwidth, some SUs at the edge of their transmitters will monitor the spectrum on other neighboring transmitters to opportunistically gain access to those transmitters. However, some SUs will imitate PUs causing PUEA.

, the signal to noise plus interference ratio (SINR) is expressed by

$$\gamma^{m}_{u\,(t)} = \frac{P_u \left| h^{m}_{u\,(t)} \right|^2}{\sum_{\substack{k=1 \\ k \neq u}}^{K} a^{m}_{k} P_k \left| h^{m}_{k\,(t)} \right|^2 + N_0 B^m}, \tag{5}$$

where k is an interferer, P_k is the power that the interfering user exchanges with other users communicating over channel m, a^m_k is a binary index that indicates whether channel m is chosen by k or not, and B^m is the bandwidth of channel m. Each user is permitted to choose one channel only. The power spectral density of noise, denoted by N_0, is assumed equal for the entire spectrum. Thus, the total user rate over channel m at time t is given by

$$r^{m}_{(t)} = \sum_{u=1}^{n} a^{m}_{u} B^m \log_2 \left(1 + \gamma^{m}_{u\,(t)} \right). \tag{6}$$

2.2. Channel State Prediction. This section discusses RPF algorithm, which is used to predict the channel state and the rate [40]. Suppose a channel state changes from $x_{(t-1)}$ to $x_{(t)}$ at time episode t, the channel impulse response $h^{m}_{u\,(t)}$ in equation (4) governs the channel's state change. However, every user desires higher throughput. Therefore, the function that links the state $x_{(t)}$ to the objective is expressed in equation (5). In order to obtain the current channel state, likelihood equation is utilized. Consider a set of sample $H^{m}_{(t)} = \{h^{m}_{1\,(t)}, h^{m}_{2\,(t)}, h^{m}_{3\,(t)}, \cdots, h^{m}_{n\,(t)}\}$, drawn from a random distribution whose probability density function is parameterized by θ [40]. θ is assumed to be the population that contains all possible values of $H^{m}_{(t)}$, where n is the number of subcarriers. The likelihood equation is expressed by

$$p\left(x_{(t)} \middle| x^{m}{}_{(t-1)} \right) = \max_{h^m \epsilon \theta} \exp\left(-\frac{1}{2\sigma^2} \sum_{u=1}^{N} \left(h^{m}_{u\,(t)} - \theta_{(t)} \right)^2 \right), \tag{7}$$

where σ is the variance. Further, the posterior probability uses the predicted channel state to predict the rate. Let us assume that each channel state is associated with its weight $w^{m}{}_{(t)}$; the weights are normalized such that $\sum_{m=1}^{M} w^{m}{}_{(t)} = 1$. Using Bayesian assumption and given the importance density $\eta(x_{(t)} | x^{m}_{(t-1)}, y_{(t)}) = p(x_{(t)} | x^{m}{}_{(t-1)})$, the optimal channel weights can eventually be expressed by [40, 41].

$$w^{m}{}_{(t)} \propto w^{m}{}_{(t-1)} p\left(x_{(t)} \middle| x^{m}{}_{(t-1)} \right). \tag{8}$$

Moreover, a kernel function δ_b is needed to smoothen the posterior density. Thus, the posterior density estimation is given by

$$p\left(y_{(t)}\middle|x_{(t)}\right) \approx \sum_{m=1}^{T} w^{m}{}_{(t)}\delta_b\left(x_{(t)} - x^{m}{}_{(t)}\right), \tag{9}$$

where

$$\delta_b(h) = \frac{1}{b^{n_x}}.\delta\left(\frac{x}{b}\right). \tag{10}$$

$\delta(.)$ is the rescaled kernel density, b is the kernel bandwidth, and n_x is the dimension of the channel state $x_{(t)}$. The kernel density and bandwidth are chosen to minimize the mean integrated square error between the actual posterior density and the corresponding regularized observation in equation (9). In a uniformly weighted sample, the optimal choice of the kernel is the Epanechnikov kernel [40–43].

$$\delta_{\text{opt}} = \begin{cases} \frac{n_x + 2}{2C_{n_x}}\left(1 - \|x\|^2\right), & \text{if } \|x\| < 1, \\ 0, & \text{Otherwise,} \end{cases} \tag{11}$$

where C_{n_x} is the volume of the unit hyper sphere in $\mathbb{R}^{n_x}$. Moreover, for a Gaussian with a unit covariance, the optimal kernel bandwidth is expressed by

$$b_{\text{opt}} = A.N^{-1/(n_x+4)} \text{ with } A = \left[8C_{n_x}{}^{-1}(n_x + 4)\left(2\sqrt{\pi}\right)^{n_x}\right]^{1/(n_x+4)}. \tag{12}$$

Let us assume that μ is uniformly distributed and λ is the acceptance probability. The current channel state $x^{\text{m}}{}_{(t)}$ is moved to a new state $x^{m+}{}_{(t)}$ based on the Metropolis-Hastings algorithm [40, 41]. The acceptance probability to move to the new state is given by

$$\lambda = \min\left\{1, \frac{p\left(y^{m+}{}_{(t)}\middle|x^{m+}{}_{(t)}\right)p\left(x^{m+}{}_{(t)}\middle|x^{m}{}_{(t-1)}\right)}{\left(y_{(t)}\middle|x^{m}{}_{(t)}\right)p\left(x^{m}{}_{(t)}\middle|x^{m}{}_{(t-1)}\right)}\right\}. \tag{13}$$

Therefore, the next channel state is given by

$$x^{m+}{}_{(t)} = x^{m}{}_{(t)} + b_{\text{opt}}Q_{(t)}\epsilon^{m}, \tag{14}$$

where $Q_{(t)}$ is the empirical covariance of the channel and ϵ^m is the channel impulse response drawn from the Epanechnikov kernel [41]. Therefore, the channel state $h^{m}{}_{(t)}$ is moved to the next state if $\mu \le \lambda$ according to (13); otherwise, the move is rejected.

3. Problem Formulations and Algorithm

Suppose the locations of the connected transmitters are represented in matrix D; in order to attain a sparse coefficient $\widehat{D}$, the $L1$ minimization is used to obtain the number of non-zero components. The sparse coefficient is expressed by [44, 45]

$$\widehat{D} = \min D_1 \text{ st.} \left\|\bar{\Phi} - \varphi D\right\|_2 \le \nu. \tag{15}$$

Many methods for solving the minimization problem in equation (15) are available. However, in this paper, the least square method is used to solve it.

Some of the SUs at the edges of the transmitters are assumed to imitate the signal characteristics of PUs of the neighboring transmitters with stronger signal power. Eventually, this causes PUEAs on those particular neighboring transmitters. The nonzero elements in $\widehat{D}$ apparently indicate the PUEAs that exist in the network, since the rest of the elements with values equal to zero represent the sites of the PUs.

3.1. Localization. Although the number of users as well as their demands varies, it is crucial to know the positions of active users and RRHs they are connected to. Thus, let $D_{N\times M}$ denote user sites, which is represented by

$$D = [s_1, s_2, \cdots, s_m, \cdots, s_M], \tag{16}$$

where each s_m is an $N \times 1$ vector with an element $s_m(u) = 1$ for a particular user u connected to transmitter m, while the rest of the elements are equal to zero. Therefore, D is M-sparse.

Consider a Rayleigh energy decay model expressed by [2]

$$R_u^m = P_0 \frac{h_u^m}{d_u^{me}}, \tag{17}$$

where P_0 is the power density of transmitter m and $e\,\epsilon(2, 5)$ is the pathloss exponent determined by the environment. The energy decay for the M transmitters is represented by [2]

$$\Psi = P_0\begin{bmatrix} \frac{h_1^1}{d_1^{1e}} & \cdots & \frac{h_1^M}{d_1^{Me}} \\ \vdots & \ddots & \vdots \\ \frac{h_N^1}{d_N^{1\,e}} & \cdots & \frac{h_N^M}{d_N^{Me}} \end{bmatrix}. \tag{18}$$

Therefore, the energy fading in (17) can also be expressed by

$$X = \Psi D. \tag{19}$$

Consider an arrangement of G measurement entities for each BBU. Therefore, a measurement matrix of size $G \times M$ is represented by

$$\Phi = [\Phi(1), \Phi(2), \cdots \Phi(G)]. \tag{20}$$

Each element $\Phi(g)$ $(1 \le g \le G)$ of matrix Φ is of the size $1 \times M$. Let us suppose that $(1 \le m \le M)$ represents the index of the transmitter to which the g^{th} measurement entity is connected. Moreover, assume that element $\Phi(g, m)$ of the $1 \times M$ vector $\Phi(g)$ is connected to transmitter m. Let us assume for transmitter m, that "Φ" ("g, m") = 1, while the rest of the elements equal to zero. The value of $\Phi(g, m) = 1$ for transmitter m, while the rest of the elements equal to zero. Suppose the measurement entities receive new user demands as

$$\bar{\Phi} = \Phi X. \tag{21}$$

The measurement matrix $\bar{\Phi}$ is used as a recovery matrix. We can see that X is common in (19) and (21). Thus, substituting (19) in (21) gives us

$$\bar{\Phi} = \Phi \Psi D. \tag{22}$$

A particular number of transmitters are used to localize equation (15) accurately for G number of measurements as represented in equation (22). Let $\varphi = \Phi\Psi$; therefore, the compressive measurement can be expressed by

$$\bar{\Phi} = \varphi D. \tag{23}$$

Thus, the noisy measurement of matrix $\bar{\Phi}$ can be added in order to improve robustness, which eventually is expressed by [2]

$$\bar{\Phi} = \varphi D + v, \tag{24}$$

where $v_{N \times M}$ is an additive white Gaussian noise.

3.2. Performance Evaluation. In order to evaluate equation (23), the RIP is utilized. The goal is to reconstruct the $\bar{\Phi}_{G \times M}$ matrix in order to obtain a guaranteed unique solution provided that it obeys the RIP as expressed in [30, 31, 40]

$$\left\| \bar{\Phi}\varphi \right\|_2 < \frac{1 - \delta_s}{\sqrt{1 + \delta_s}} \left\| \bar{\Phi} \right\|_2, \tag{25}$$

where $\delta_s \in (0, 1)$ is the RIP constant. The noisy measurement is categorized based on the minimum residual error.

3.3. The MAOMP Algorithm. Suppose the reference for the sparsity estimation is denoted by S and the initial sparsity by S_0. The MAOMP requires the usage of the theoretical sparsity S. However, MAOMP examines a match in order to estimate S_0. A projection set Y containing the residual error and the corresponding sets that represent the transmitters and the respective user is computed. The L^{th} largest value in Y is selected, and the index of the selected transmitter and the corresponding set are obtained. The corresponding set is the support set of the selected transmitter. The support set is denoted by D_t at time (t), and its length is obtained from the estimated value, which satisfies the condition of the match. The indices of D_t are kept in index set Λ_M. The L^{th} largest value is chosen among the elements in the projection set $Y = |\langle \varepsilon_t, D_l \rangle| l = 1, 2, \cdots, T$, where ε_t denotes the residual error. The corresponding index values of the L^{th} largest values are kept in F_0. Subsequently, the values in D_T and Λ_t are updated as $D_T = D_{t-1} \cup D_l \, (l \in F_0)$ and $\Lambda_t = \Lambda_{t-1} \cup F_0$, respectively. Then, the residuals are updated as [29]

$$\varepsilon_t = \bar{\Phi} - \varphi_{tL} \widehat{D}_{t_L}. \tag{26}$$

The stage and the variable step size are used to adjust the filtered values, in order to achieve a better sparse representation of $\widehat{D}$. The MAOMP is a scheme that utilizes step size coefficient $\beta_0 \in (0, 1)$ in order to obtain variable step size. Initially, a larger step size is adopted in order to lower the number of measurements and then slowly decrease the step size, and therefore, accuracy is increased. The step size denoted by step_j can be expressed by [29]

$$\text{step}_{j+1} = \left[\beta_0 \times \text{step}_j \right], \tag{27}$$

where j is the number of iterations and β_0 is the step size coefficient. In every iteration, the estimated sparsity L_j is computed by

$$L_{j+1} = L_j + \text{step}_{j+1}. \tag{28}$$

According to (27), the step size is greater at the beginning of the iteration, but it reduces gradually to 1. This implies that if the theoretical sparsity and initial sparsity are not close to one another, the convergence of the estimated value to the theoretical sparsity is slow. Therefore, since the initial step size is greater, the sparsity estimation would converge to the theoretical sparsity quickly. Nevertheless, in order to have accurate sparsity estimation, a smaller step size is used, such that the estimated sparsity may not be deficient or overestimated. The OMP method is utilized to solve equation (15). The L^{th} greatest value in the projection set y in step 8 of Algorithm 1 is selected based on the correlation between the sensing matrix and the residual error [29]. The MAOMP steps are shown in Algorithm 1.

Algorithm 2 shows the proposed method for detecting PUEAs that exist in the network. This method predicts the next state of a channel then detects the malicious users that illegally use spectrum. Eventually, the PUEAs will not be granted access to the spectrum, leaving more available spectrum.

3.4. Spectral and Energy Efficiencies. Let us assume a set $K = \{u_1, u_2, u_3, \cdots, u_k\}$ of k malicious users, where u_k denotes a PUEA. Suppose the total bandwidth used by all active users including the PUEAs is denoted by B and the

1. **Input:** $D_{N\times M}$, $\bar{\Phi}_{N\times M}$, δ_s.
2. **Output:** $\widehat{D}$ and Λ.
3. Initialization: *step* = step size, S_0, ε, Λ_t, D_t.
4. Compute projective set Y.
5. Test RIP, If true then $S_0 = S_0 + 1$.
6. Compute ε_0, Set stage and count to 1, $L = S_0$.
7. Calculate Y, choose L^{th} highest value in Y, update Λ_t and D_t.
8. Compute $\widehat{D} = \min_{D_1} \|\bar{\Phi} - \varphi D\|_2$, choose L^{th} greatest value, update Λ_t and D_t, update ε_0 .
9. If $\varepsilon_0 < v$, go to 2.
10. If $\varepsilon_0 \geq$ previous ε_0, $step_{j+1} = \lceil \beta_0 \times step_j \rceil$, $L = L + step_{j+1}$ go to step 6. Else update Λ_t, go to step 6.

Algorithm 1: MAOMP.

1. Establish network topology (RRHs and their respective users).
2. Obtain channel values and calculate the rate per RRH.
3. Predict the next channel state of RRH users using RPF algorithm.
4. Apply MAOMP (in Algorithm 1).
5. Drop detected PUEAs in 4.
6. Calculate the rate based on legitimate users.
7. Evaluate SE and EE based on equations (29) and (30).

Algorithm 2: RPF MAOMP.

bandwidth occupied by the PUEAs is B^m; the spectral efficiency (SE) in b/s/Hz with M active RRHs and G BBUs is expressed by

$$\mathrm{SE} = \frac{\sum_{m=1}^{M} r^m(t)}{G \times (B - B^m)}, \tag{29}$$

where $r^m(t)$ is the rate at transmitter m at time stamp (t). Consequently, energy efficiency (EE) in b×s/Joule can be obtained by

$$\mathrm{EE} = \frac{\mathrm{SE}}{\sum_{\mathrm{all}\, G} \sum_u^n P_u}. \tag{30}$$

4. Results and Discussion

This paper proposes an RPF MAOMP method to detect PUEAs existing in a network. The PUEAs are detected based on the predicted channel state. Given the previous state of channel $x_{(t-1)}$, the current state $x_{(t)}$ is predicted based on the current impulse response $h^m_{u\,(t)}$ in equation (4). In order to get user objective $y_{(t)}$, the function $\gamma_{(t)}$ in equation (5) links $x_{(t)}$ to $y_{(t)}$ as shown in equations (1) and (2).

In order to enhance spectral and energy efficiencies, the main idea is to accurately detect PUEAs present on the network. Therefore, a sparse representation of the detected transmitter is required. For a system of linear equations represented by D, the problem is formulated as $\|D\|_1$ subject to $\|\Phi - \varphi D\|_2$. The $L1$ minimization looks for a sparse solution for a problem; hence, it is used to obtain the sparse representation $\widehat{D}$. However, $L2$ produces a unique solution with smooth fitting. Therefore, based on the channel state $x_{(t)}$ and user objective $y_{(t)}$, the MAOMP is used to detect the PUEAs present in the network using the $L1$ minimization. The RIP is used to characterize matrices which are linearly orthogonal [46]. Therefore, the RIP is used to evaluate the performance in order to obtain a guaranteed unique solution to the sparse matrix $\widehat{D}$.

4.1. Simulation Setup. This paper considers a CRAN with 9 RRHs operating at 5.25 GHz frequency with 20 MHz band and 23 dBm transmit power for each RRH. Small-scale fading and large-scale fading are considered as the radio propagation channel models. Assume user u is located at a distance of d^m_u meters away from transmitter m, and a line of sight (LOS) connection is considered between RRH m communicating with user u in an urban environment. The pathloss model is obtained by [40]

$$\mathrm{PL}^m_u = 9\log_{10}(d^m_u) + 35.77 + 30.2\log_{10}(f) + \psi. \tag{31}$$

However, the pathloss model for outdoor users is given by the nonline of sight (NLOS) model:

$$\mathrm{PL}^m_u = 48.1\log_{10}(d^m_u) + 3.67 + 39.1\log_{10}(f) + \psi, \tag{32}$$

where f denotes the frequency in GHz and ψ is the large-scale variability of signal against the distance in a straight path.

A user rate of 1 Mbps and a predefined stopping error of 1×10^{-6} are considered in the simulation environment. In order to calculate the optimal kernel bandwidth, the dimension n_x of channel x is one (1), and the volume of a unit sphere C_{n_x} is π. The RIP constant and step size coefficient obviously affect the number of measurements and sparsity

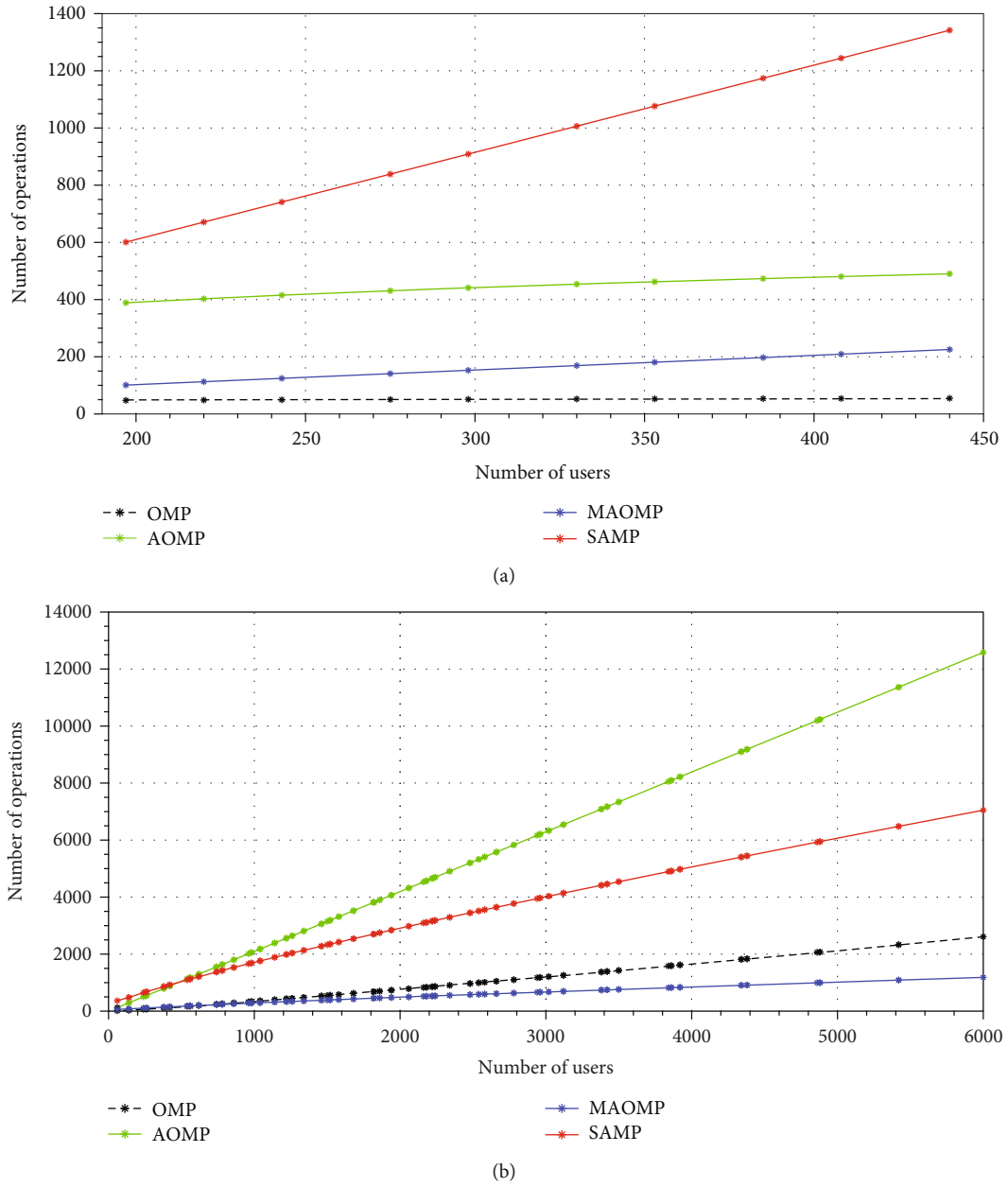

Figure 2: Number of operations for the OMP, AOMP, SAMP, and MAOMP algorithms.

estimation. Therefore, in order to reduce the number of iterations and avoid over estimation, the RIP constant is set to $\delta_s = 0.2$, and the step size coefficient is $\beta_0 = 0.4$ [29]. The number of steps for both SAMP and MAOMP algorithms is equal to $O(n/\log(M))$. However, the number of operations for OMP and AOMP algorithms is equal to $O(n \log(M))$ and $O(n \log(n/M))$, respectively [2, 29].

The simulation is run 10 times, each at various user capacities of up to 50 users per RRH, using MATLAB software. Up to ten PUEAs are set randomly for each RRH. However, at most three randomly selected PUEAs are successful in emulating PUs of a particular transmitter. For simplicity, the transmitter whose PUEA has the highest RSS is chosen and used for performance evaluation. Thus, the SE and EE values are based on the throughput of the selected transmitter in the support set. Figures 2–7 show results for the performance comparison between OMP, AOMP, SAMP, and MAOMP without and with RPF-based channel state prediction [40]. The RPF has been proven to be fast and useful for real-time tracking of channels [39]. Therefore, in this study, MAOMP is simulated with and without applying RPF algorithm in order to evaluate its performance. The computational complexity and the spectral and energy efficiencies are used to evaluate the performance of MAOMP.

4.2. Simulation Results

4.2.1. Number of Operations. Figure 2 shows the number of operations for OMP, AOMP, SAMP, and MAOMP

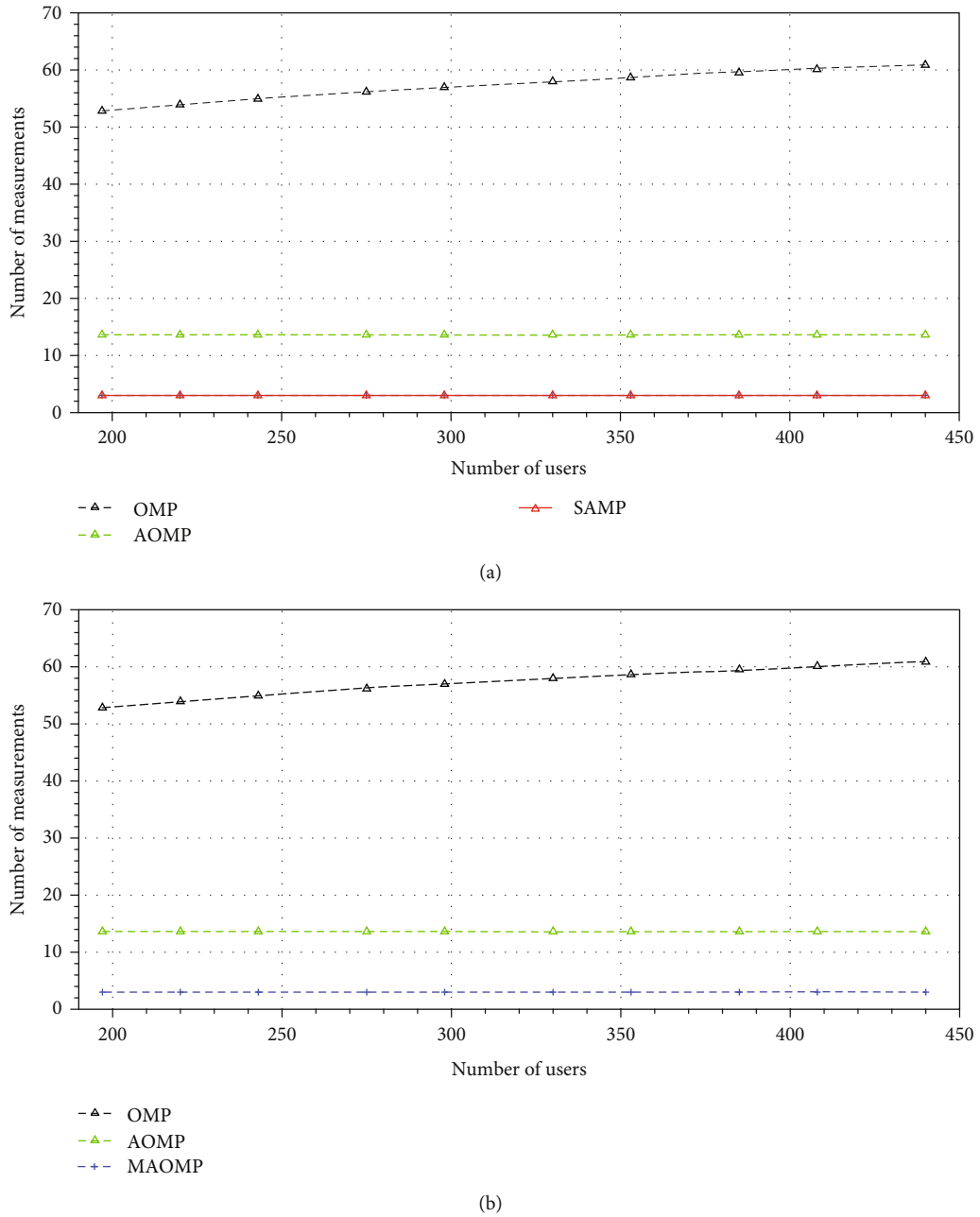

Figure 3: Number of measurements for the OMP, AOMP, SAMP, and MAOMP algorithms.

algorithms, respectively, based on the number of users and the number of transmitters that have been considered in this paper. Figure 2(a) considers a small number of users per transmitter, while Figure 2(b) includes larger number of users for each transmitter. Thus, Figure 2(a) is the zooming of Figure 2(b) for small number of users. It has been shown in Figure 2(a) that the number of operations is 50, 100-200, 400-500, and 600-1350 for OMP, MAOMP, AOMP, and SAMP, respectively. According to Figure 2(a), OMP converges faster than the other three algorithms, while SAMP is slow to converge. However, Figure 2(b) shows that the convergence of both MAOMP and SAMP improves when the number of users in a transmitter is high. Thus, AOMP is the slowest, while MAOMP is the fastest to converge when the number of users in a transmitter is high.

4.2.2. Average Number of Measurements. In order for AOMP, SAMP, and MAOMP algorithms to stop running, the residual error has to meet a predefined stopping criterion. In case of AOMP algorithm, the average mean square error has to be nearest to the predefined stopping criterion for the iteration to stop. However, MAOMP algorithm adopts sparsity estimation along with adjustable step size. Since the step size is adjustable, the number of iterations that MAOMP algorithm can run is reduced compared to AOMP. Figure 3 shows the number of measurements for OMP,

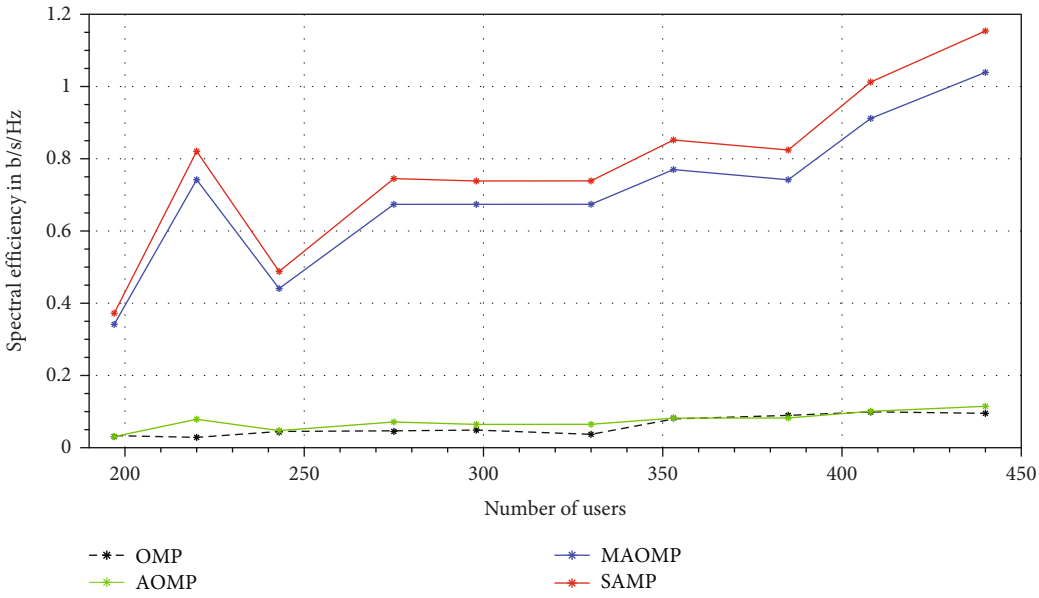

Figure 4: SE performance without RPF.

AOMP, SAMP, and MAOMP, respectively. It can be seen in Figure 3 that for all scenarios, the number of iterations is 52-60 for OMP, 14 for AOMP, and 3 for both SAMP and MAOMP, respectively. Since the number of measurements for both SAMP and MAOMP is the same, Figure 3(b) is for clarification. It is clear that the number of measurements for OMP is the highest; thus, it is the slowest. Moreover, Figure 3 shows that both SAMP and MAOMP are the fastest. However, since the number of operations of MAOMP is smaller than the number of operations of SAMP, according to Figure 2, MAOMP is the fastest.

4.2.3. Spectral Efficiency. Figure 4 shows the SE performance of MAOMP compared to OMP, AOMP, and SAMP without RPF channel state prediction. Noticeably, the SE values for OMP and AOMP are the same in all scenarios. The SE values range between 0.03 and 0.10 b/s/Hz, 0.03-0.12 b/s/Hz, 0.34-1.2 b/s/Hz, and 0.35-1.15 b/s/Hz for OMP, AOMP, SAMP, and MAOMP, respectively, when RPF is not applied as shown in Figure 4.

The SE performance of the proposed method is presented in Figure 5, when RPF prediction is utilized. The SE values for OMP and AOMP are the same in all scenarios. Figures 5(a) and 5(b) are shown in order to clarify that both AOMP and SAMP methods give similar SE values. It can be seen in Figures 5(a) and 5(b) that the SE values range between 0.15 and 0.22 b/s/Hz for OMP, AOMP, and SAMP and between 1.45 and 2.25 b/s/Hz for MAOMP algorithms, respectively, when RPF is applied. The SE for the proposed method is higher than that of the OMP, AOMP, and SAMP methods. It can clearly be seen in all scenarios that the SE of MAOMP is higher than that of the OMP, AOMP, and SAMP.

4.2.4. Energy Efficiency. Figure 6 shows the EE performance of MAOMP compared to OMP, AOMP, and SAMP without RPF channel state prediction. The EE values for OMP and AOMP are similar in all scenarios. Since both OMP and AOMP produce the same graph, Figures 6(a) and 6(b) are presented for clarification. Figure 6 shows that the values of EE range between 0.03×10^{-4} and 0.06×10^{-4} b×s/Joule for both OMP and AOMP, 0.33×10^{-4} and 0.92×10^{-4} b×s/Joule for SAMP, and 0.28×10^{-4} and 0.65×10^{-4} b×s/Joule for MAOMP, respectively, when RPF method is not applied. It is evident from Figure 6 that the EE for MAOMP is higher than that of the OMP and AOMP. However, MAOMP is less energy efficient than SAMP when RPF is not applied.

The EE values for the proposed method are presented in Figure 7. It can be observed from Figure 7 that the range of the EE values for OMP, AOMP, and SAMP is very similar for all scenarios. The EE values range between 0.09×10^{-4} and 0.03×10^{-4} b×s/Joule for OMP, AOMP, and SAMP and between 0.6×10^{-4} and 2.4×10^{-4} b×s/Joule for MAOMP, respectively, when the RPF is used. It can be seen that, for all methods, the EE curve is higher with smaller number of users, and it drops gradually as the number of users increases.

4.3. Discussions. This section provides the discussion for the simulation results obtained in Section 4.2. The purpose of the study is to assess the performance of MAOMP algorithm in real-time conditions. Since RPF has been proved to be fast and useful for real-time tracking of channels [40], in this study, MAOMP is simulated with and without applying RPF in order to evaluate its performance. The spectral and energy efficiencies are used to evaluate the performance of MAOMP.

The number of measurements of OMP is the highest as illustrated in Figure 3. However, in order to improve accuracy, MAOMP algorithm has to run a number of times until a predefined stopping criterion is met, before the execution

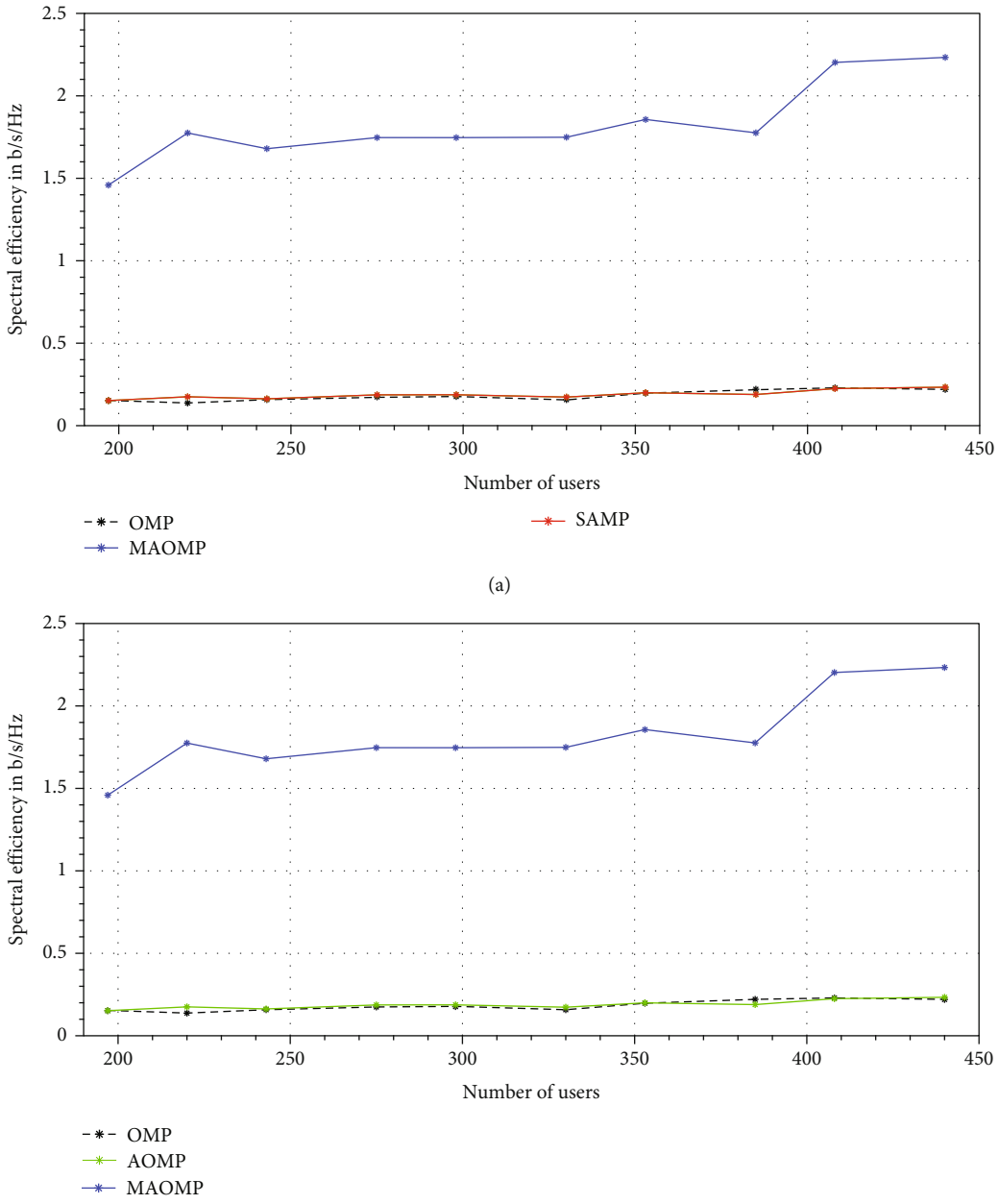

Figure 5: SE performance with the RPF method.

is passed on to the next iteration. Likewise, AOMP algorithm has to run until the average mean square error meets the predefined stopping criterion, leading to a higher number of iterations. Unlike MAOMP, which adopts adjustable step size in order to reduce the number of iterations, AOMP algorithm can run for a number of iterations before it outputs the detected PUEAs. The number of measurements in Figure 3 shows the number of times AOMP, SAMP, and MAOMP algorithms can run before moving on to the next iteration, respectively. When the number of users is small, OMP is the fastest because it runs once and does not have the subiteration for accuracy test that AOMP, MAOMP, and SAMP algorithms have. However, the convergence of both MAOMP and SAMP improves when the number of users in a transmitter is high. AOMP is the slowest to converge, while MAOMP is the fastest to converge when the number of users in a transmitter is high. It is clear in Figure 2 that MAOMP outperforms OMP, AOMP, and SAMP. This is because the sparsity estimation for MAOMP is adopted along with an adjustable step size in order to reduce the number of measurements to some extent and improve accuracy [28, 47].

In Figures 4 and 5, the SE performance of the proposed method is the best compared to that of OMP, AOMP, and SAMP methods due to the improved accuracy for MAOMP [29]. Moreover, the number of operations of MAOMP is

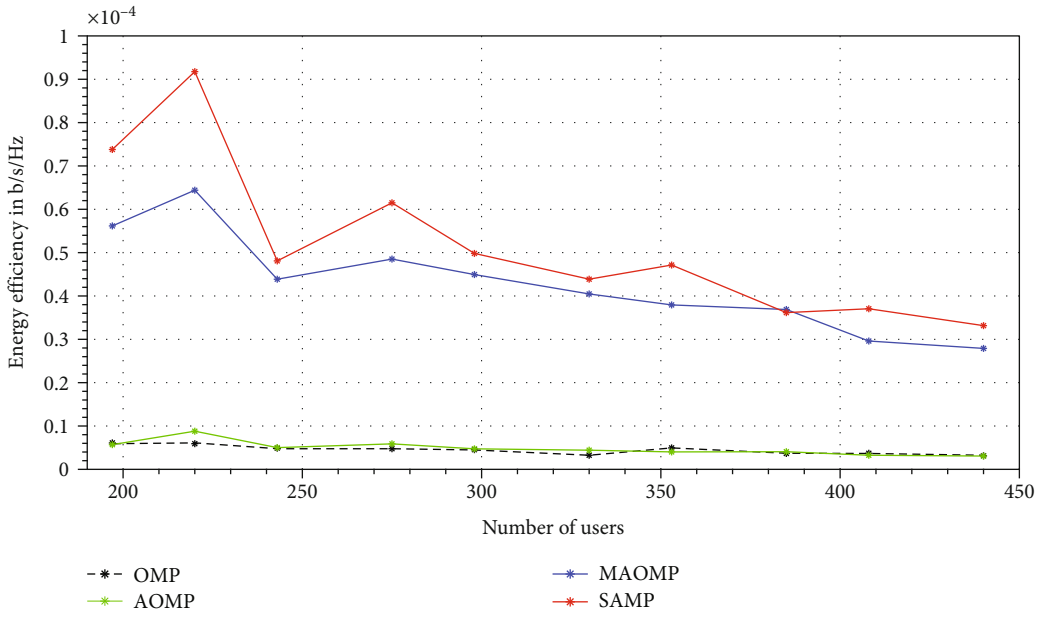

Figure 6: EE performance without RPF.

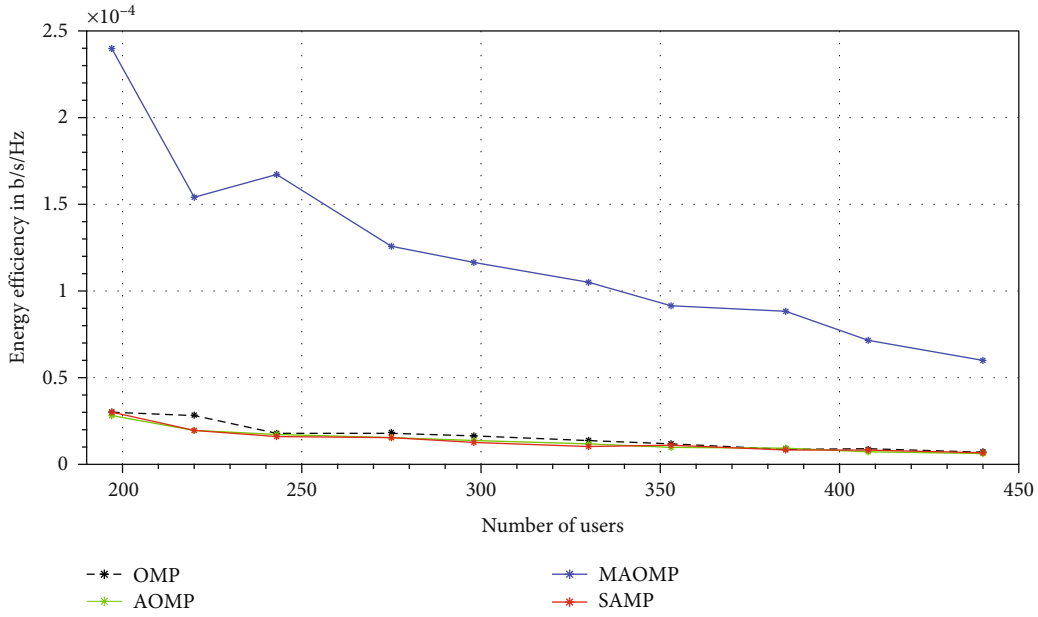

Figure 7: EE performance with RPF.

small and thus can detect more PUEAs leading to more available spectrum. Additionally, MAOMP can be faster and thus can give excellent performance in real-time system conditions for dense networks. It is worth noting that, due to RPF's real-time high capability of tracking and high performance even when the number of users is high and also when small dynamical noise is expected, RPF predicts the next state of a channel and allocates users to the best channels [29, 40]. Therefore, it can be seen in Figure 5 that the SE for all of the algorithms increases greatly compared to Figure 4.

The simulation results for the EE are shown in Figure 7. According to equation (30), as SE increases, the EE should increase as well. However, the EE will decrease with increase in power of active users. Therefore, it can be seen in Figure 7 that the EE increases generally for all of the algorithms when RPF is applied.

It has been shown in the simulation results that the SE of MAOMP is 91.2-91.6% and 90-91.2% greater than the SE of OMP and AOMP, respectively, when RPF is not applied. However, the SE for MAOMP is less than that of the SAMP method by 2.9% when the number of users

is small then increases up to -2.9-4.2% as the number of users increases. Although the performance of all OMP, AOMP, SAMP, and MAOMP methods increases when RPF algorithm is applied, the proposed method outperforms the other methods by 89.6-90.2% and 85-87.5% in SE and EE, respectively. The SE and EE of MAOMP are increased by 46.6-76.5% and 83-88.3%, respectively, when RPF is applied.

5. Conclusions

It has been shown in the simulation results that the performance of OMP, AOMP, SAMP, and MAOMP algorithms is generally improved when RPF is used. MAOMP is faster than the other three methods as its number of operations is low. Due to the inability of OMP, AOMP, and SAMP to detect some PUEAs as a result of their lower speed when the RPF is utilized, outstanding spectral and energy efficient results have been shown for MAOMP method. The SE and EE of the proposed method are 89.6-90.2% and 85-87% higher than that of the OMP, AOMP, and SAMP methods, respectively, when RPF algorithm is applied. Moreover, the SE and EE of MAOMP method are increased by 46.6-76.5% and 83-88.3%, respectively, when RPF is applied. The EE is very small, that is, in mb×s/Joule. Therefore, in the future, more study is needed to improve EE.

Abbreviations

AOMP: Adaptive orthogonal matching pursuit
AR: Autoregression
AR(p): p^{th} order autoregression process
BBU: Baseband unit
CPRI: Common public radio interface
CR: Cognitive radio
CRAN: Cloud radio access network
CS: Compressed sensing
dBm: Decibel meter
EE: Energy efficiency
GHz: Gigahertz
H-CRAN: Heterogeneous-CRAN
LOS: Line of sight
MAOMP: Modified adaptive orthogonal matching pursuit
MHz: Megahertz
Mbps: Megabits per second
NLOS: Nonline of sight
OMP: Orthogonal matching pursuit
PUEAs: Primary user emulation attacks
PUs: Primary users
RF: Radio frequency
RIP: Isometric property
RPF: Regularized particle filter
RRH: Remote radio head
RSS: Received signal strength
SAMP: Sparsity adaptive matching pursuit
SE: Spectral efficiency
SINR: Signal to noise plus interference ratio
SUs: Secondary users
UE: User equipment.

Data Availability

The code data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Acknowledgments

This work is supported by the Foshan Science and Technology Innovation Special Fund Project (No. BK22BF004); part of the work is supported by the National Key R&D Program of China (No. 2020YFB1807900).

References

[1] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," *IEEE Network*, vol. 30, no. 6, pp. 62–69, 2016.

[2] M. Dang, Z. Zhao, and H. Zhang, "Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks," in *2013 International Conference on Wireless Communications and Signal Processing*, Hangzhou, China, 2013.

[3] F. Tian, P. Zhang, and Z. Yan, "A survey on C-RAN security," *IEEE Access*, vol. 5, pp. 13372–13386, 2017.

[4] N. Mishra, S. Srivastava, and S. N. Sharan, "Countermeasures for primary user emulation attack: a comprehensive review," *Wireless Personal Communications*, vol. 115, no. 1, pp. 827–858, 2020.

[5] D. Pu, Y. Shi, A. V. Ilyashenko, and A. M. Wyglinski, "Detecting primary user emulation attack in cognitive radio networks," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, pp. 1–5, Houston, TX, USA, 2011.

[6] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Ráez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *2009 IEEE 28th International Performance Computing and Communications Conference*, pp. 208–215, Scottsdale, AZ, 2009.

[7] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *2011 IEEE Wireless Communications and Networking Conference*, Cancun, Mexico, 2011.

[8] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[9] C. Chen, H. Cheng, and Y. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[10] X. Liao, S. Wang, Y. Wang, Y. Che, J. Zhou, and J. Zhang, "Multipath cluster-assisted single station localization based on SSA-GA in outdoor NLOS environment," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 8585978, 9 pages, 2022.

[11] M. Castelli, L. Manzoni, L. Mariot, M. Nobile, and A. Tangherloni, "Salp swarm optimization: a critical review,"

Expert Systems with Applications, vol. 189, article 116029, 2022.

[12] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2935–2939, Vancouver, BC, Canada, 2013.

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

[14] W. R. Ghanem, M. Shokair, and M. I. Desouky, "An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm," in *2016 33rd National Radio Science Conference (NRSC)*, pp. 178–187, Aswan, Egypt, 2016.

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

[16] H. Furqan, M. Aygül, M. Nazzal, and H. Arslan, "Primary user emulation and jamming attack detection in cognitive radio via sparse coding," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, 2020.

[17] O. Oyerinde, "Forward-reverse orthogonal matching pursuit-union-subspace pursuit-based multiuser detector for uplink grant-free NOMA networks," *Electronics*, vol. 11, no. 1, p. 125, 2022.

[18] B. Chhetrya and N. Marchanga, *Detection of primary user emulation attack (PUEA) in cognitive radio networks using one-class classification*, Elsevier, 2021.

[19] P. Perera, P. Oza, and V. Patel, "One-class classification: a survey," 2021, https://arxiv.org/abs/2101.03064.

[20] D. Janu, K. Singh, and S. Kumar, "Machine learning for cooperative spectrum sensing and sharing: a survey," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 1, 2022.

[21] M. Shakil, A. Fuad, R. Arul, A. Bashir, and J. Choi, "A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022.

[22] R. T. Rodoshi, S. Shin, and W. Choi, "A Survey on Applications of Deep Learning for Cloud Radio Access Network," *IEEE Access*, pp. 61972–61997, 2021.

[23] W. F. Fihri, H. El Ghazi, N. Kaabouch, and B. A. El Majd, "Bayesian decision model with trilateration for primary user emulation attack localization in cognitive radio networks," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, Marrakech, Morocco, 2017.

[24] M. Kumar, "Analytical model for mitigating primary user emulation attack using hypothesis testing in cognitive radio networks," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 11, pp. 486–500, 2021.

[25] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *2009 IEEE International Conference on Communications*, Dresden, Germany, 2009.

[26] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 74–85, 2009.

[27] Y. Zheng, Y. Chen, C. Xing, J. Chen, and T. Zheng, "A scheme against primary user emulation attack based on improved energy detection," in *2016 IEEE International Conference on Information and Automation (ICIA)*, pp. 2056–2060, Ningbo, China, 2017.

[28] S. Deshmukh and S. Bhuyan, "Compressive sensing based energy efficient wideband cognitive radio network," in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 137–142, Bengaluru, India, 2018.

[29] B. Li, Y. Sun, G. Li et al., "Gesture recognition based on modified adaptive orthogonal matching pursuit algorithm," *Cluster Computing*, vol. 22, S1, pp. 503–512, 2019.

[30] L. A. Y. Odwa, Y. Chen, and Z. Mai, "Detection of primary user emulation attack based on modified adaptive orthogonal matched pursuit for cognitive radio networks in HCRAN," in *Proceedings of the ACM Turing Celebration Conference*, pp. 1–7, Chengdu, China, 2019.

[31] M. A. Saleh and A. Abdul Manaf, "A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks," *The Scientific World Journal*, vol. 2015, Article ID 238230, 19 pages, 2015.

[32] U. Masud, M. Ali, F. Qamar, A. Zeeshan, and M. Ikram, "Dual mode spectroscopic biomedical sensor: technical considerations for the wireless testbed," *Physica Scripta*, vol. 95, no. 10, article 105206, 2020.

[33] J. Lee and K. H. Chon, "An autoregressive model-based particle filtering algorithms for extraction of respiratory rates as high as 90 breaths per minute from pulse oximeter," *IEEE Transactions on Biomedical Engineering*, vol. 57, no. 9, pp. 2158–2167, 2010.

[34] A. Zarei and B. M. Asl, "Automatic seizure detection using orthogonal matching pursuit, discrete wavelet transform, and entropy based features of EEG signals," *Computers in Biology and Medicine*, vol. 131, article 104250, 2021.

[35] Y. Wang, Y. Shui, X. Yang, Z. Li, and W. Wang, "Multi-target vital signs detection using frequency-modulated continuous wave radar," *EURASIP Journal on Advances in Signal Processing*, vol. 2021, no. 1, 2021.

[36] Y. Wang, W. Wang, M. Zhou, A. Ren, and Z. Tian, "Remote monitoring of human vital signs based on 77-GHz mm-wave FMCW radar," *Sensors*, vol. 20, no. 10, p. 2999, 2020.

[37] U. Masud, F. Jeribi, M. Alhameed, A. Tahir, Q. Javaid, and A. F. Akram, "Traffic congestion avoidance system using foreground estimation and cascade classifier," *IEEE Access*, vol. 8, pp. 178859–178869, 2020.

[38] H. Y. Sutarto, E. Joelianto, and T. S. Sumardi, "Estimation and prediction of road traffic flow using particle filter for real-time traffic control," 2013, https://www.researchgate.net/publication/281436339.

[39] M. B. Ghorbel, B. Khalfi, B. Hamdaoui, and M. Guizani, "Resources allocation for large-scale dynamic spectrum access system using particle filtering," in *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 219–224, Austin, TX, USA, 2014.

[40] L. A. Y. Odwa and Y. Chen, "Throughput enhancement based on optimized regularized particle filter for H-CRAN," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5672–5683, 2019.

[41] B. Ristic, S. Arulampalam, and N. Gordon, *Beyond the Kalman filter: particle filters for tracking applications*, Artech House Publishers, 2004.

[42] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking," *IEEE Transactions on Signal Processing*, vol. 50, no. 2, pp. 174–188, 2002.

[43] C. Musso, N. Oudjane, and F. Le Gland, "Improving regularised particle filters," in *Sequential Monte Carlo Methods in Practice*, A. Doucet, N. Freitas, and N. Gordon, Eds., Statistics for Engineering and Information Science, Springer, New York, NY, 2001.

[44] R. Baraniuk, M. Davenport, R. DeVore, and M. A. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, no. 3, pp. 253–263, 2008.

[45] X. Zhang, Y. Liu, and X. Wang, "A sparsity preestimated adaptive matching pursuit algorithm," *Journal of Electrical and Computer Engineering*, vol. 2021, Article ID 5598180, 8 pages, 2021.

[46] E. J. Candes, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics*, vol. 59, pp. 1207–1223, 2006.

[47] Z. Liquan, M. Ke, and J. Yanfei, "Improved generalized sparsity adaptive matching pursuit algorithm based on compressive sensing," *Journal of Electrical and Computer Engineering*, vol. 2020, Article ID 2782149, 11 pages, 2020.