A Joint Rogue Access Point Localization and Outlier Detection Scheme Leveraging Sparse Recovery Technique

Qiaolin Pu, *Member, IEEE*, Joseph Kee-Yin Ng, *Senior Member, IEEE*, Mu Zhou, *Senior Member, IEEE*, and Jie Wang, *Senior Member, IEEE*

***Abstract*—With the pervasive deployments of Access Point (AP) in Wireless Local Area Network (WLAN), rogue AP has emerged as such a large threat to user's privacy, that it is expected to be detected and located accurately. Hence, in this paper, we propose a novel rogue AP localization scheme leveraging sparse recovery technique, which consists of three steps: 1) Coarse localization, which is the result of comparing the online records with clustered fingerprint database. A novel Object Weighting Affinity Propagation (OWAP) clustering method is proposed to group the offline fingerprints. When computing the similarities, unlike traditional affinity propagation clustering method which views each object equally, we utilize the prior physical coordinates information to assign weight to each object. 2) Compressive sensing (CS) kernel optimization, in which the minimum number requirement of monitors in localization system is deduced through analyzing the problem formulation theoretically, and an Equiangular Tight Frame (ETF) based monitors selection scheme is presented to achieve higher location accuracy. 3) Joint fine rogue AP localization and outlier detection through a formulation of an improved CS based sparse recovery model. It could localize the rogue AP and identify the monitors whose readings are either not available or erroneous simultaneously, which increases the localization robustness. We operate simulations as well as experiments to verify the superiority of the proposed scheme both theoretically and practically.**

***Index Terms*—Wireless LAN, Rogue Access Point localization, sparse recovery, clustering, outlier detection.**

Manuscript received July 11, 2020; revised December 12, 2020; accepted January 21, 2021. Date of publication January 28, 2021; date of current version March 10, 2021. The review of this article was coordinated by Dr. K. Bian.
(Corresponding author: Qiaolin Pu.)

Qiaolin Pu is with the Chongqing Key Lab of Mobile Communications Technology, School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China, and also with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, China (e-mail: puql@cqupt.edu.cn).

Joseph Kee-Yin Ng is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, China (e-mail: jng@comp.hkbu.edu.hk).

Mu Zhou is with the Chongqing Key Lab of Mobile Communications Technology, School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: zhoumu@cqupt.edu.cn).

Jie Wang is with the School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China, and also with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116023, China (e-mail: wangjie@dlut.edu.cn).

Digital Object Identifier 10.1109/TVT.2021.3055263

I. Introduction

Wireless Local Area Network (WLAN) is a pervasive infrastructure in communications which plays an increasing important role in our daily lives. Although that people could access the Internet any-time and any-where makes our lives easier and more convenient, there emerges increasing privacy and security threats. Rogue Access Point (AP), as one of the threats, is defined as an unauthorized AP, which is deployed by an adversary to operate a man-in-the-middle attack rather than the WLAN administrator [1]. As far as we know, adversaries usually install two wireless cards into a rogue AP, and one is used for connecting with any one of the authorized legitimate APs in the wireless network and the other is disguised as a legitimate AP for mobile users to connect with [2]. Under this setup, wireless communications could be eavesdropped successfully by a rogue AP, and once a mobile user connects with it, there may occur a variety of malicious attacks which would result in a disclosure of user's private information. Even worse, the connected wireless network may suffer from considerable damage. [3] reports that nowadays about 20% of the corporations exist rogue APs in their communication networks and these rogue APs have conducted numerous potential targeted cyber-attacks. Hence, both the academic and the industrial sector have focused on detecting and localizing rogue AP recently.

There are two techniques of rogue AP detection. The first one is realized through analyzing the characteristics of network traffic at the gateway, such as the connection time with mobile users [4] and the temporal traffic characteristics [5]. Another mostly used rogue AP detection technique is monitoring the wireless networks through keeping recording the properties of all APs in the network, such as MAC addresses, SSID, and vendor name. During the monitoring process, monitors distributed in the environment would periodically scan the spectrum at 2.4 and 5 GHz using wireless sniffers. A reference properties would be collected from legitimate APs and they would be compared with these new periodical records to distinguish whether rogue APs appear [6]. Actually, the second rogue AP detection technique performs good in general, and there are already some commercial products [7]. Therefore, in this paper, we mainly focus on rogue AP localization after detecting it appears in the communication network.

Rogue AP localization is a vital task to solve the potential privacy problem. Generally, there are two basic signal measurements adopted by localization systems, the Channel State Information (CSI) measurement and Received Signal Strength (RSS) measurement. The first one is a fine-grained information provided by commercial Wi-Fi cards from physical layer and is applied to many localization systems recent years. A direction determination approach is proposed in [8], which firstly utilizes the CSI amplitude of time domain to conduct the estimation of rogue AP's direction, and then applies triangulation method to determine where it is in. However, the drawback is that it works well in Line of Sight (LOS) environment, but if there are walls between the mobile user and the rogue AP, it needs to adjust the direction which brings in complexity and errors. The authors in [9] also present a developed self-adaptive MUSIC algorithm based on CSI measurement to estimate the rogue AP's direction. [10] proposes a method through simple gesture, besides adopting the CSI information to calibrate the direction of the rogue AP, it also utilizes the Fresnel zone information to calculate the rogue AP's location. Due that CSI measurement is from dozens of sub-carriers in physical layer which brings phase deviation and difficulty of data extraction, hence, RSS measurement is mostly adopted by localization systems with convenient data accessibility.

Localizing rogue AP exploiting RSS measurement has three typical techniques, signal model based, gradient based, and fingerprint based. For the first technique, a wireless signal attenuation model is firstly applied to calculate the distance between three or above known monitors' locations, and then it estimates the location of rogue AP based on the principle of triangulation [11]. Signal model based technique has also been applied to mobile user localization systems whose target of localization is mobile user, and it has a similar drawback that when the wireless signal attenuation model could not be appropriate to describe the environment, the location accuracy is low. Authors in [12] proposes a gradient based technique which firstly aims at finding the minus gradient of the rogue AP and then applies triangulation method based on the selected gradient directions to calculate rogue AP's location. However, the location accuracy of this technique fully depends on the estimation of rogue AP's gradient direction, once the gradient direction is wrong, localizing rogue AP fails. Fingerprint based technique is mostly utilized in recent years as compared to the above two mentioned techniques, since it offers both higher location accuracy and ubiquity. This popular technique is similarly applied to mobile user localization system, but there is a slight difference between them, which we will describe in details in section II.

Generally, there are two categories of localization methods based on fingerprinting rogue AP localization system. The first one is a signal-distance-based method which aims at selecting Reference Points (RPs) whose distances between the offline fingerprints and the online RSS measurements are smallest (i.e. smallest distances in signal space), and one of the most well-known distance metric is Euclidean distance, along with the most well-known K-Nearest Neighbor (KNN) localization method. The second one is a compressive sensing (CS) based sparse recovery method which is introduced in recent years [13]. It formulates the mobile user's location as a sparse vector in discrete spatial domain and applies the sparse recovery method to recover it. Although CS based sparse recovery method is one of the most prominent localization methods and has been widely utilized in mobile user localization systems, as far as we know, it has not been presented in rogue AP localization systems. In addition, when applying it to the mobile user localization system, we still face some challenges, i) a key factor of applying the CS based sparse recovery method successfully is choosing an appropriate CS kernel, hence, CS kernel optimization is important [14]; ii) it needs a coarse localization as the two-step procedure followed by fine localization, if it fails, it would lead to a wrong subset of RPs and the entire localization fails [15]; iii) the traditional CS model is sensitive to outliers, and it assumes the online RSS measurements only have normal noise, however, online measurements may experience outliers due to unforeseen reasons [16].

Actually, the CS kernel in mobile user localization system is always treated as the result of AP selection [17]. Similarly, in rogue AP localization system, we treat the CS kernel as the result of monitor selection, which contains the specific number of monitors and their selection scheme. Most researches utilize two existing AP selection methods to optimize CS kernel. For example, [18] proposes a Strongest based method which aims to select a subset of APs that provide coverage and accurate measurements for most of the time. Another typical AP selection method named as Fisher Criterion is proposed in [19], which quantifies the discrimination ability of fingerprints and takes the stability into account simultaneously. However, both of them are from the perspective of maximizing the discrimination ability of fingerprints rather than sparse recovery ability. Moreover, there is no guidance of choosing the specific number of APs.

A coarse localization stage could reduce the search space of the target location to a smaller number of RPs, and this procedure is typically called offline clustering, where the sub-set of RPs of a cluster are grouped together based on a similarity metric by computing their similarities of RSS measurements in signal space. However, these existing clustering methods which only consider the similarities in signal space may lead to a phenomenon that there may exist RPs belonging to the same group in signal space while their coordinates in physical space are far away from each other. For example, two typical existing clustering methods are the most well-known K-means clustering [20] and the affinity propagation clustering [21]. The clustering results only based on signal space would decrease the location accuracy.

There are many causes leading to the online measurements experience outliers, such as the intermittent unavailability or error of transmitting devices, the introduce of extra indoor obstacles, or the transmit power adaption. If the online measurement is highly different from the corresponding offline fingerprint, it would reduce the location accuracy. While only few researches have focused on outlier detection in fingerprinting localization system. Hampel filter is introduced in [22], which utilizes the outlier-resistant median and median absolute deviation from the median to replace the outlier-sensitive mean and standard deviation estimates. [23] proposes a modified KNN method which detects the outliers through computing the Euclidean distance between the online measurements and fingerprint database over a modified sub-set of APs. However, these mentioned methods need an extra procedure before the fine localization, which increases the time consumption.

To respond to these mentioned challenges, in our work, we propose a joint rogue AP localization and outlier detection scheme leveraging CS based sparse recovery technique. Specifically, to optimize the CS kernel, first of all, the minimum number requirement of monitors is deduced through justifying the validity of the problem formulation theoretically. Then an Equiangular Tight Frame (ETF) based monitors selection scheme from the perspective of sparse recovery ability is proposed. Moreover, a novel Object Weighting Affinity Propagation (OWAP) method is proposed to cluster the offline fingerprints to do coarse localization. When computing the similarities, unlike traditional affinity propagation clustering method which views each object equally, we utilize the prior physical coordinates information to assign weight to each object. What's more, the traditional CS model is improved to jointly conduct rogue AP localization and outlier detection. The main contributions are summarized as follows.

i) It is the first work to apply the sparse recovery technique to rogue AP localization systems which formulates the rogue AP's location as a sparse vector in discrete spatial domain.

ii) The minimum number requirement of monitors are deduced, which is a guidance of designing localization systems.

iii) We proposed an ETF based monitors selection scheme which improves sparse recovery ability and the subsequent localization accuracy.

iv) A novel OWAP clustering method is proposed utilizing the prior knowledge of physical coordinates information. It avoids that RPs with small distance in signal space and large distance in physical space are grouped into one cluster, which is more suitable to localization systems.

v) We improve the CS model to do joint rogue AP localization and outlier detection, which increases the localization robustness to outliers and there is no need for an extra procedure of doing outlier detection.

The rest of this paper is organized as follows, the preliminary information of the traditional CS based sparse recovery theory and its application in mobile user localization system is given in Section II. Section III presents our main work of system description, OWAP offline clustering, CS kernel optimization, and joint fine rogue AP localization and outlier detection. The simulations and experiments are operated and the results are reported in Section IV. Finally, a conclusion of our work is provided in Section V.

II. Preliminary

A. Compressive Sensing Based Sparse Recovery Method

CS is a popular sparse recovery technique applied to sparse domain in signal processing of communication systems in recent years. Using this technique, we could adopt a much lower sampling frequency to recovery the original signals as compared with the traditional Nyquist criterion [24], so it could save channel resources significantly. Two fundamental premises for applying the CS technique are required, sparsity and incoherence. Here sparsity means there are only a small number of non-zero elements, and it refers that the original signal should be sparse or it is sparse in a certain domain. That is to say non-sparse original signal could be represented sparsely through transforming to another domain, such as Fourier domain and wavelet domain, and we call the corresponding domain as sparse domain. The later premise refers that the relationship between domain basis and CS kernel is incoherence.

Let the original signal y be a $N \times 1$ column vector in $\Re^N$, and it has a sparse representation in one certain sparse domain with the domain basis $\mathbf{\Psi} = [\Psi_1, \Psi_2, \ldots, \Psi_N]$, then y can be represented sparsely as

$$\mathrm{y} = \mathbf{\Psi}\mathrm{s} = \sum_{i=1}^{N} s_i \Psi_i \tag{1}$$

where s is the coefficient sequence of y in the transformed sparse domain and it is a sparse column vector, each Ψ_i is a column vector, $\mathbf{\Psi}$ is the domain basis. If we sample the original signal with a sampling matrix $\mathbf{\Phi}$ with dimension of $M \times N$, then the corresponding sampling result is

$$\mathrm{y}' = \mathbf{\Phi}\mathrm{y} = \mathbf{\Phi}\mathbf{\Psi}\mathrm{s} = \mathbf{\Theta}\mathrm{s} \tag{2}$$

where y' is a $M \times 1$ column vector, the sampling matrix $\mathbf{\Phi}$ is also called CS kernel, $\mathbf{\Theta} = \mathbf{\Phi}\mathbf{\Psi}$. Due that the y', $\mathbf{\Phi}$ and $\mathbf{\Psi}$ are already known by the signal receiving terminal, therefore, the CS technique aims to reconstruct the sparse vector s, so that it could recovery the original signal x using the inverse domain transform.

As we mentioned above, the relationship between domain basis and CS kernel should be incoherence. Previous research has proved that if $\mathbf{\Theta} = \mathbf{\Phi}\mathbf{\Psi}$ holds the Restricted Isometry Property (RIP) condition, their relationship is regarded as incoherence. Assuming s only has k non-zero elements (named as k-sparse vector) and $k < M \ll N$, under the parameters k and δ, if

$$1 - \delta \leq \frac{\|\mathbf{\Theta}\mathrm{v}\|_2^2}{\|\mathrm{v}\|_2^2} \leq 1 + \delta \quad \text{for} \quad \delta \in (0, 1) \tag{3}$$

holds for all $k-$sparse vector v, then we call $\mathbf{\Theta}$ satisfies RIP condition.

After satisfying these two premises, the sparse vector s could be well recovered adopting l_1-norm minimization

$$\begin{aligned} &\hat{\mathrm{s}} = \arg\min \|\mathrm{s}\|_1 \\ &\text{s.t. } \mathrm{y} = \mathbf{\Theta}\mathrm{s} \end{aligned}. \tag{4}$$

If the received sampling result y' has been corrupted with noise, then minimization turns to

$$\begin{aligned} &\hat{\mathrm{s}} = \arg\min \|\mathrm{s}\|_1 \\ &\text{s.t. } \|\mathrm{y} - \mathbf{\Theta}\mathbf{s}\|_2 < \varepsilon \end{aligned}. \tag{5}$$

Here ε represents the noise in the sampled data.

B. CS Application to Mobile User Localization System

This section provides the formulation of traditional mobile user localization system (aims estimating the location of mobile user) using the CS technique [25]. In the offline phase, the target environment is divided into a set of Reference Points (RPs) $\mathrm{V} = \{\mathrm{v}_j = (x_j, y_j) | j = 1, \ldots, N\}$, where V defines the set of RPs' coordinates, and N is the number of RPs. At each RP, the mobile device records the RSS measurements from L available APs, denoting as $\Psi_j = (rss_j^1, rss_j^2, \ldots, rss_j^L)^T$, then the entire fingerprint database can be represented as

$$\begin{aligned} \boldsymbol{\Psi} &= [\Psi_1, \Psi_2, \ldots, \Psi_N] \\ &= \begin{pmatrix} rss_1^1 & \ldots & rss_N^1 \\ \vdots & \ddots & \vdots \\ rss_1^L & \cdots & rss_N^L \end{pmatrix}. \end{aligned} \tag{6}$$

In the online phase, a mobile user at his current location generates one observation $\mathrm{y} = (rss^1, rss^2, \ldots, rss^L)^T$. Conventional KNN method finds the K nearest fingerprints through calculating the Euclidean distances between y and $\boldsymbol{\Psi}$, and then utilizes the associated RPs' locations to estimate the mobile user's location. While for the CS technique, it formulates the localization as a sparse signal recover problem. Specifically, the location of the mobile user is considered as a 1-sparse vector s in the discrete spatial domain, whose all elements are zero except $\mathrm{s}(o) = 1$, here o is the index of the RP at which the mobile user is located, denoted as

$$\mathrm{s} = [0, \ldots, \underset{\uparrow \text{the } o\text{-th column}}{1}, \ldots, 0]^{\mathrm{T}}{}_{\mathrm{N}\times 1}. \tag{7}$$

Theoretically, there is

$$\mathrm{y} = \begin{bmatrix} rss^1 \\ rss^2 \\ \vdots \\ rss^L \end{bmatrix} = \begin{pmatrix} rss_1^1 & \ldots & rss_N^1 \\ \vdots & \ddots & \vdots \\ rss_1^L & \cdots & rss_N^L \end{pmatrix} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}. \tag{8}$$

In the above equation, the non-sparse vector y can be regarded as having a sparse representation in one certain domain with domain basis $\boldsymbol{\Psi}$, and the location sparse vector s is the coefficient sequence vector in the sparse domain, i.e., $\mathrm{y} = \boldsymbol{\Psi}\mathrm{s}$. Hence, in order to apply the CS technique, it needs further to construct a CS kernel $\boldsymbol{\Phi}_{M\times L} = [\phi_1, \ldots, \phi_M]^T (M \ll L)$. As far as we know, all the current researches treat the CS kernel as an an sampling matrix of APs (AP selection), so each row ϕ_i is a $L \times 1$ column vector with all elements equal to zero except $\phi_i(l) = 1$. Here M and l are the number and the index of selected APs, respectively.

$$\phi_m = [0, \ldots, 0, 1, 0, \ldots, 0]^T \quad \forall m = 1, 2, \ldots, M. \tag{9}$$

Based on the above description, the sampled online RSS measurements can be expressed as

$$\mathrm{y}'_{M\times 1} = \boldsymbol{\Phi}\mathrm{y} = \boldsymbol{\Phi}\boldsymbol{\Psi}\mathrm{s} + \varepsilon. \tag{10}$$

Here ε is the noise. Compared to Equation (2), we can see the above equation is a typical CS model, whose target is to obtain the mobile user's location through reconstructing the sparse vector s using l_1−norm minimization. It noteworthy that here the vector s is 1-sparse in theory, while in practice, due to the noise in the online RSS measurements or the mobile user's location deviation from its nearest RP, it would be recovered as a k-sparse vector with few non-zero coefficients, which indicates the probabilities of a mobile user located in the corresponding RPs. Besides, this k-sparse vector would not affect the positioning performance, since as we mentioned above, two key factors affecting the sparse recovery ability are the sparsity and incoherence, which means that we only need to guarantee the sparsity without considering its degree of sparsity. Moreover, due that y and $\boldsymbol{\Psi}$ are known and immutable, the CS kernel $\boldsymbol{\Phi}$ is the heart of applying the CS technique successfully.

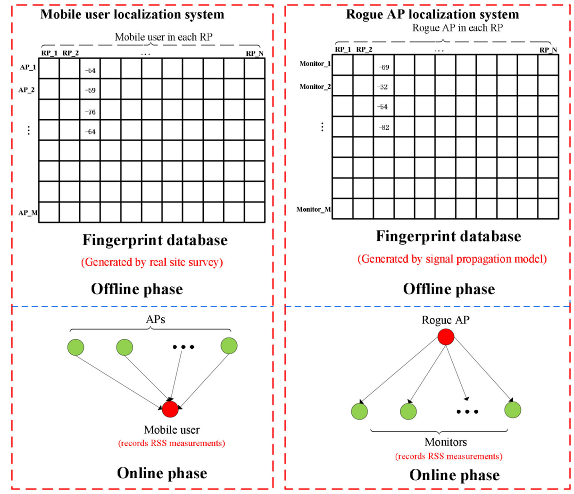


Fig. 1. Comparison between mobile user and rogue AP localization systems.

C. Comparison Between Mobile User and Rogue AP Localization Systems

As mentioned in section I, the fingerprint based technique applied to rogue AP and mobile user localization systems are similar but have slightly difference. It also has two phases, the offline database construction phase and the online location estimation phase [7]. In the offline phase, due that a rogue AP has the same probability in each RP, so each RP should be placed a rogue AP in theory, and then the distributed monitors in the environment would collect RSS measurements from these rogue APs to build the fingerprint database. While, unlike the fingerprint database of mobile user localization system which is a real site survey, in rogue AP localization system, placing a rogue AP in each RP is not available in practice, so that all previous researches adopt the signal propagation model to establish fingerprint database. In the online phase, the constructed fingerprint database would be compared with the new periodical RSS observations to estimate the rogue AP's location. Fig. 1 shows these two localization systems' compositions, from which we can further see that the role of monitor selection in rogue AP localization system is the same as the AP selection in mobile user localization system.

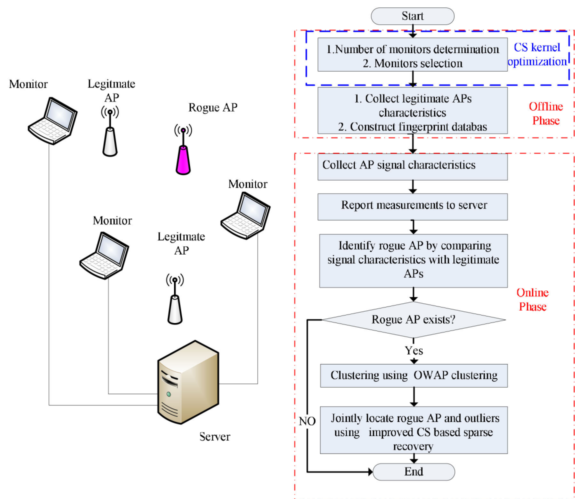


Fig. 2. The entire system architecture: detection and localization.

III. Joint Rogue AP Localization and Outlier Detection

A. System Architecture

Since the rogue AP localization process starts after it is detected in the environment, although our work does not contain rogue AP detection, in order to fully understand how the system works, an entire system architecture containing rogue AP detection and localization is presented in Fig. 2. The system is a client-server architecture, where several monitors are distributed into the environment as clients to periodically collect all available APs' data transmission and signal characteristics, and then they would report these measurements to the server to conduct detection procedure through comparing them with pre-constructed database of these legitimate APs. Once a rogue AP has a high probability to appear in the network, the sever would start to conduct localization procedure.

B. Coarse Localization: Object Weighting Affinity Propagation (OWAP) Based Offline Clustering

Offline clustering narrows the searching area into a subset of the RPs, which would decrease the computational complexity in the online phase. Traditional researches utilize the clustering algorithms directly, which cluster these RPs into several groups in terms of the similarities of RSS measurements. However, only considering RSS measurements in signal space would bring a shortcoming that there may exist RPs whose RSS measurements belonging to the same group while their coordinates in physical space are far away from each other. This clustering results would decrease the location accuracy. Therefore, in this paper, we propose a novel OWAP clustering method which combines the RSS measurements in signal space with the prior physical coordinates information together. When computing the similarities, unlike traditional affinity propagation clustering method which views each object equally, we utilize the prior physical coordinates information to assign weight to each object.

The traditional affinity propagation clustering method is a popular in recent years. It has many advantages as compared to the mostly used K-means, such as i) there is no need to determine the specific number of clusters in advance. ii) it is not sensitive to the selection of initial value. iii) it does not require the symmetry of distance matrix. First of all, an input metric of the similarity between pairs of objects is taken into account by the traditional affinity propagation algorithm, and then it recursively transmits the real-valued messages between the neighboring objects until a set of exemplars and corresponding clusters generates. The key factor of this clustering method is the similarity function, which is defined as the negative summation of squared RSS measurement distances between two RPs (objects) in localization systems

$$s(i,j) = -\sum_{l=1}^{L} \left\| rss_i^l - rss_j^l \right\|^2 \quad \forall i,j \in \{1,2,\ldots,N\} \tag{11}$$

where $s(i,j)$ is the RSS measurements similarity between the i^{th} and j^{th} RP. L and N are the number of monitors distributed in the environment and RPs, respectively. rss_i^l is the RSS recorded at the i^{th} RP from the l^{th} monitor.

Considering that we know the physical coordinates of RPs in advance, so we assign a weight w to each pair of RPs to avoid RPs far away from each other in the physical space are clustered in the same cluster in the signal space. Specifically, the weights will be used to penalize the RPs with large physical distances and give an advantage to the RPs with small physical distances. The weight-dependent similarity function is as follows

$$s(i,j,w) = -w_{ij} \sum_{l=1}^{L} \left\| rss_i^l - rss_j^l \right\|^2 \quad \forall i,j \in \{1,2,\ldots,N\} \tag{12}$$

where $s(i,j,w)$ and w_{ij} are the similarity score and weight between the i^{th} and j^{th} RPs, respectively. L and N are the number of monitors distributed in the environment and RPs, respectively. rss_i^l is the RSS recorded at the i^{th} RP from the l^{th} monitor. Here a modified *Silhouette* weighting scheme [26] is adopted to calculated it. The Silhouette width λ_{ij} is defined as

$$\lambda_{ij} = \frac{\rho_i - d_{ij}}{\max(\rho_i, d_{ij})} = \begin{cases} 1 - \frac{d_{ij}}{\rho_i} & \text{if } \ d_{ij} < \rho_i \\ 0 & \text{if } \ d_{ij} = \rho_i \\ \frac{\rho_i}{d_{ij}} - 1 & \text{if } \ d_{ij} > \rho_i \end{cases}, \quad \forall i,j \in \{1,2,\ldots,N\} \tag{13}$$

where d_{ij} is the physical coordinates' Euclidean distance between the i^{th} and j^{th} RP, and ρ_i is the average physical coordinates' Euclidean distance between the i^{th} RP and all the RPs except the j^{th} RP. Then the weight is

$$w_{ij} = \frac{1 - \lambda_{ij}}{2}, \forall i,j \in \{1,2,\ldots,N\}. \tag{14}$$

From the above definition we can easily see that $-1 \leq \lambda_{ij} \leq 1; 0 \leq w_{ij} \leq 1$, which means the weight w_{ij} is non-negative, so we can see the bigger the weight, the smaller the similarity $s(i,j,w)$.

Effectiveness demonstration: To prove the effectiveness of the proposed *Silhouette* weighting scheme, we consider the following three situations.

a) If $d_{ij} < \rho_i$,and we assume there is an extreme situation that the i^{th} and j^{th} RPs are the closest in the physical domain, i.e., the coordinates' Euclidean distance $d_{ij} \approx 0$. Hence, according to equations (13) and (14), we have $\lambda_{ij} \approx 1; w_{ij} \approx 0$. Taking them into equation (12), then we can see it devotes the biggest contribution to similarity $s(i, j, w)$.

b) If $d_{ij} > \rho_i$,and we similarly assume there is an extreme situation that the i^{th} and j^{th} RPs are the farthest in the physical domain, i.e., the coordinates' Euclidean distance $d_{ij} \approx \propto$. Then we have $\lambda_{ij} \approx -1; w_{ij} \approx 1$. According to equation (12), we can see it devotes the smallest contribution to similarity $s(i, j, w)$.

c) If $d_{ij} = \rho_i$, which represents that the distances from the i^{th} RP and other RPs are approximately equal, then we distribute weight $w_{ij} \approx 1/2$.

Overall, from the above theoretical effectiveness derivation, we can see that higher weights will be given to RPs with large physical distances, and these weights will decrease the similarity score according to equation (12), which attains our goal of avoiding the phenomenon that RPs whose RSS measurements belonging to the same cluster while their coordinates in physical space are far away from each other. After clustering, the original fingerprint database will be divided into several clusters with a subset of RPs and the online RSS measurements would firstly compare with the centers of them to find the nearest cluster, which is a coarse localization procedure.

C. Monitors Selection: Minimum Number Derivation and ETF-Based Selection Scheme

As far as we know, although the CS based sparse recovery technique has frequently appeared in mobile user localization systems in recent years, it has not been applied to rogue AP localization systems. Therefore, we similarly formulate the rogue AP's location as a 1-sparse vector and apply sparse recovery technique to estimate its location. Moreover, as we stated above, central to succesful application of the CS technique is the CS kernel, and it is treated as an AP selection result in mobile user localization system. Similarly, the CS kernel optimization in rogue AP localization system is treated as monitor selection, which contains the number of monitors and their selection scheme. To our best knowledge, traditional AP selection schemes applied to CS based localization systems are from the perspective of maximizing the discrimination ability of fingerprints instead of the CS recovery ability. Moreover, there are no previous works focusing on the guidance of selection number. Therefore, this section aims to address these two problems.

Since the monitors are related to the whole environment, so we conduct the derivation based on the whole fingerprint database rather than sub-database produced by clustering. Not considering the existing of outliers and assuming the number of selected monitors as M, the rogue AP localization model based on CS is

$$\begin{aligned}
&\mathrm{y}'_{M\times 1} = \mathbf{\Phi}\mathrm{y} = \mathbf{\Phi\Psi}\mathrm{s} + \varepsilon \\
&\mathbf{\Phi}_{M\times L} = [\phi_1, \ldots, \phi_M]^T \ (M < L) \\
&\phi_m = [0, \ldots, 0, \underbrace{1}_{\text{Index of selected monitor}}, 0, \ldots, 0]^T \\
&\forall m = 1, 2, \ldots, M
\end{aligned} \tag{15}$$

where L is the total number of monitors distributed in the environment, $\mathbf{\Phi}$ is the CS kernel which indicates the selected number and index of monitors, the online RSS measurements generating by these selected monitors are ${\mathrm{y}'}_{M\times 1}$, $\mathbf{\Psi}$ and s are the fingerprint database and location sparse vector, respectively.

1) Minimum Number Derivation: As stated in section II A, successful application of the CS technique requires satisfying the premises of sparsity and incoherence. Formulating the rogue AP's location as a sparse vector in discrete spatial domain has met the first premise. Therefore, the next step we need to do is to testify whether $\mathbf{\Theta} = \mathbf{\Phi\Psi}$ holds the RIP condition.

We utilize the COST231 signal propagation model to describe the indoor signal attenuation property, since it is a good compromise of the flexibility, practicability, and computation complexity, as shown below

$$rss(dBm) = rss_{d_0} - 10\gamma \log\left(\frac{d}{d_0}\right) - P_{wf} + \pi \tag{16}$$

where rss and rss_{d_0} are the RSS measurements collected from monitors to the rogue AP with d and d_0 meters respectively. d_0 is a reference distance, and we usually set it as $d_0 = 1$. P_{wf} is a signal fading factor brought by the floors and walls. γ is the path-loss exponent. π is a shadowing noise follows Gaussian distribution $N(0, \sigma^2)$.

Assuming $\{l_1, \ldots, l_M\}$ is the location index of these selected monitors, then $\mathbf{\Theta} = \mathbf{\Phi\Psi}$ can be written as

$$\mathbf{\Theta}(mW) = \begin{pmatrix} \frac{P_0 {\pi'}_{l_1,1}}{d_{l_1,1}} & \cdots & \frac{P_0 {\pi'}_{l_1,N}}{d_{l_1,N}} \\ \vdots & \ddots & \vdots \\ \frac{P_0 {\pi'}_{l_M,1}}{d_{l_M,1}} & \cdots & \frac{P_0 {\pi'}_{l_M,N}}{d_{l_M,N}} \end{pmatrix} \tag{17}$$

where $\pi'_{l_i,1}$ follows the Gaussian distribution $N(0, {\sigma_1}^2)$, (x_i, y_i) is the location coordinate of the i^{th} RP, and $d_{l_i,j} = \sqrt{(x_{l_i} - x_j)^2 + (y_{l_i} - y_j)^2}$. The below theorem is proved by us and the proving process has exploited some theoretical results from the literature [25].

Theorem: the probability for $\mathbf{\Theta}$ satisfying equation (3) for all k-sparse vector v would tend to 1 as long as the number of monitors M is $O(k\log(N/k))$.

Proof: Conducting normalization of the i^{th} row of $\mathbf{\Theta}$, we obtain

$$\langle\mathbf{\Theta}\rangle_i = \eta \cdot \left\langle \frac{P_0 {\pi'}_{l_i,1}}{d_{l_i,1}}, \ldots, \frac{P_0 {\pi'}_{l_i,N}}{d_{l_i,N}} \right\rangle \tag{18}$$

where η is the normalization constant

$$\eta = \sqrt{\frac{N}{M} \cdot \frac{1}{\sum_{j=1}^{N} \frac{{\sigma_1}^2}{{d_{l_i,j}}^2}}}. \tag{19}$$

As these monitors are randomly deployed in the target environment, then $\langle\mathbf{\Theta}\mathrm{v}\rangle_i$ is regarded to follow the Gaussian distribution, whose mean value is zero and the variance is

$$ {\sigma_2}^2 = \eta^2 \cdot \frac{1}{N} \cdot \left(\sum_{j=1}^{N} \frac{{\sigma_1}^2}{{d_{l_i,j}}^2}\right) \cdot \sum_{h=1}^{k} {v_h}^2 \tag{20}$$

where $v_h (1 \leq h \leq k)$ represents the h^{th} non-zero values of the 1-sparse vector v. As such $\|\mathbf{\Theta}\mathrm{v}\|_2^2$ satisfies χ^2-distribution (freedom degree is M), whose mean value is $M{\sigma_2}^2$ and the variance is $2M{\sigma_2}^4$. Sincce $M > 1$, $\frac{\|\mathbf{\Theta}\mathrm{v}\|_2^2}{\|\mathrm{v}\|_2^2}$ can be approximated as a Gaussian distribution whose mean value is

$$\frac{M{\sigma_2}^2}{\sum_{h=1}^{k} {v_h}^2} = M \cdot \eta^2 \cdot \frac{1}{N} \cdot \left(\sum_{j=1}^{N} \frac{{\sigma_1}^2}{{d_{l_i,j}}^2} \right) = 1 \tag{21}$$

and the variance is $\frac{2}{M}$. From the Chernoff bound, we have the following probability

$$\Pr\left\{ \left| \frac{\|\mathbf{\Theta}\mathrm{v}\|_2^2}{\|\mathrm{v}\|_2^2} - 1 \right| > \delta \right\} \leq 2e^{-\frac{\delta^2 \cdot M}{8}}. \tag{22}$$

Since the total number of possible k-sparse vector is

$$\binom{N}{k} \leq (eN/k)^k \tag{23}$$

then the probability that there is at least one k-sparse vector

$$\begin{aligned} \mathrm{P}_1 = \Pr&\left\{ \left| \tfrac{\|\mathbf{\Theta}\mathrm{v}\|_2^2}{\|\mathrm{v}\|_2^2} - 1 \right| > \delta \text{ for at least exists one vector} \right\} \\ &\leq \left(\tfrac{eN}{k}\right)^k \cdot 2e^{-\frac{\delta^2 \cdot M}{8}} = 2e^{-\frac{\delta^2 \cdot M}{8} + k\log\left(\frac{N}{k}\right) + 1} \end{aligned}. \tag{24}$$

Due to $M = O(k\log(N/k))$, (24) would tend to 0, therefore, the probability becomes

$$\Pr\left\{ \left| \frac{\|\mathbf{\Theta}\mathrm{v}\|_2^2}{\|\mathrm{v}\|_2^2} - 1 \right| \leq \delta \text{ for all possible v} \right\} = 1 - \mathrm{P}_1 = 1. \tag{25}$$

From it we can see equation (3) is satisfied, which indicates it can hold the RIP condition, and the minimum requirement of number of monitors of the CS based sparse recovery technique is obtained in terms of $M = k\log(N/k)$ from the above derivation,.

2) ETF-Based Monitors Selection Scheme: As stated above, besides the number of monitors, the monitor selection scheme is another important step to CS kernel optimization. Recall that the CS kernel is treated as the AP selection result in mobile user localization system, and two popular AP selection schemes mostly utilized to generate the CS kernel by previous researches are the Strongest based and Fisher Criterion based methods. however, they are not proposed from the perspective of CS recovery ability. Compared to them, an ETF based algorithm is proposed by us to optimize the CS kernel.

ETF is one of the indicators to find an optimal CS kernel [29], which is applied to signal recovery field. Defining the column coherence of matrix $\mathbf{\Phi}\Psi = \mathbf{\Theta}_{M\times N} = [\theta_1, \ldots, \theta_N]$ as

$$\mu = \max_{1\leq i,j\leq N, i\neq j} |\langle \theta_i, \theta_j \rangle| \tag{26}$$

where θ_i is the i^{th} column of $\mathbf{\Theta}$. If the condition of $N \leq M(M+1)/2$ is satisfied, then it regards that the column coherence of matrix $\mathbf{\Theta}$ has an infimum (which is also called as Welch Limit) of

$$\mu \geq \sqrt{\frac{N-M}{(N-1)M}}. \tag{27}$$

When the equal sign works in equation (27), the corresponding matrix is regarded as ETF, which is marked as $\mathbf{\Theta}^o$. Then it can find the optimal kernel $\mathbf{\Phi}^o$ through calculating $\mathbf{\Phi}^o = \mathbf{\Theta}^o \mathbf{\Psi}^{-1}$.

It is noteworthy that although ETF provides a guidance in theory, obtaining such an optimal kernel ETF is difficult. Moreover, localization system has an additional constraint of the kernel that the non-zero elements' values $\mathbf{\Phi}$ should be 1 (see equation (15)). Therefore, we develop it to search for a suboptimal kernel which is the closest to the optimal ETF through the below objective function

$$\mathbf{\Theta} = \min \max_{1\leq i,j\leq N, i\neq j} |\langle \theta_i, \theta_j \rangle| \tag{28}$$

Finally, we can solve (28) by exhaustive searching.

D. Joint Fine Localization and Outlier Detection

Although outliers may occur in the offline phase as well as the online phase, our outlier detection mainly focus on the online phase due to the fact that the offline fingerprints are collected over a long period and validation has been taken place. An outlier is defined as that the online RSS measurement from a monitor is obviously different from any other measurements from the same monitor in the neighborhood area. If the selected monitor provides highly different recordings in the online phase, the online RSS measurement and the offline fingerprint may have a large deviation, which would result in low location accuracy. In addition, outliers can not be detected by monitor selection methods as they are mainly focus on selecting monitors for the largest incoherence between RPs, even worse, these outliers may contribute more of fingerprint incoherence. Therefore, we propose to utilize the concept of sparsity promoting regression to jointly conduct rogue AP localization and outlier detection. It's noteworthy that our goal of outlier detection does not focus on the detection accuracy, but aim to improve the localization robustness to outliers through the formulation of outlier term.

Similar to the formulation of rogue AP's location as a 1-sparse vector, the outliers are explicitly modelled as a k-sparse vector in the online RSS measurements. Specifically, with τ denoting the outliers sparse vector, the online RSS measurements adhere to the improved CS model is

$$\mathrm{y}' = \mathbf{\Phi}\mathrm{y} = \mathbf{\Phi}\mathbf{\Psi}^o \mathrm{s}^o + \tau + \varepsilon \tag{29}$$

where $\mathbf{\Psi}^o$ and s^o are the fingerprint sub-database and location sparse sub-vector generated by the nearest cluster after coarse localization procedure, respectively. As long as the number of corrupted monitors is small, the outlier sparse vector τ will be guaranteed. Therefore, it can be estimated jointly with the location sparse vector with l_1-minimization

$$\begin{aligned} (\hat{\mathrm{s}}, \hat{\tau}) &= \arg\min\, [\|\mathrm{s}\|_1 + \mu\|\tau\|_1] \\ \text{s.t. } &\|\mathrm{y}' - \mathbf{\Phi}\mathbf{\Psi}^o \mathrm{s}^o - \tau\|_2 < \varepsilon \end{aligned} \tag{30}$$

where μ is a tuning parameter.

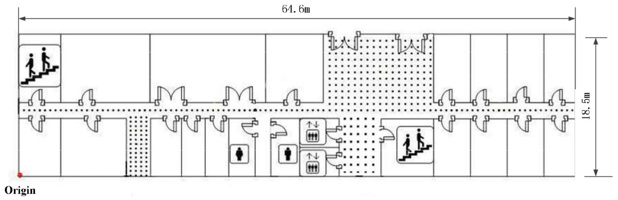


Fig. 3. Simulation Environmental layout.

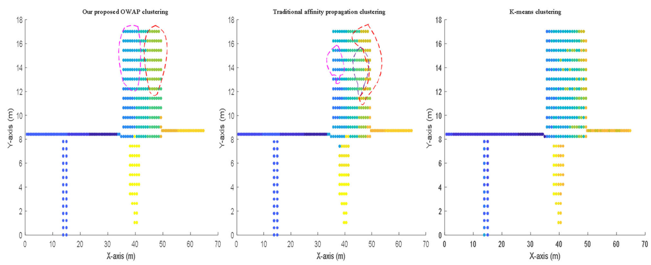
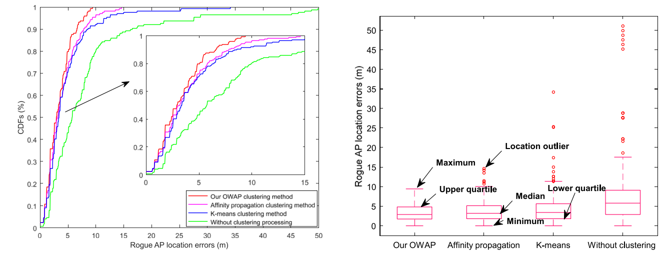
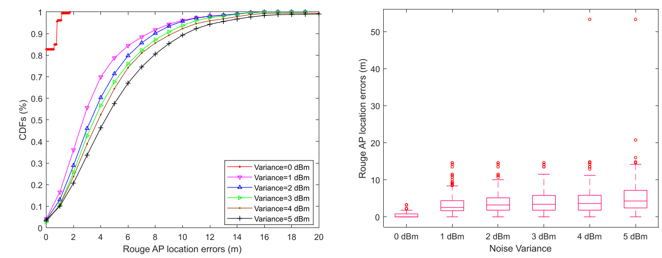


Fig. 4. Display of clustering results in physical space.



(a) (b)

Fig. 5. Rogue AP location errors under different clustering processing. (a) CDFs of rogue AP location errors. (b) Rogue AP statistical location errors.



(a) (b)

Fig. 6. Rogue AP location errors under different noise variances. (a) CDFs of rogue AP location errors. (b) Rogue AP statistical location errors.

IV. Simulation and Experimental Results Analysis

In this section, the effectiveness of the proposed OWAP clustering method, CS kernel optimization which contains minimum number and selection scheme of monitors, and the improved CS model based joint fine rogue AP localization and outlier detection, which aims to improve the localization robustness to outliers are studied and analyzed through simulations as well as experiments.

A. Simulations

In the simulations, we select a real building structure with a long corridor and rectangular rooms, which are two typical indoor architecture elements, as shown in Fig. 3. This building with the dimensions of 64.6 m by 18.5 m has 363 RPs (indicated as ".") divided with the same interval of 1.2 m, and its dimensions are 64.6 m by 18.5 m. In our simulation, to be consistent with the mathematical analysis in section III C, we use the same COST231 signal attenuation model. Generally, in the offline phase, we would collect RSS measurements in a long period at each RP and use the mean RSS value to construct the fingerprint database, which indicates the probability of existing noise is very low. However, in the online phase, the time interval for data collection is short in general, therefore, besides the number of monitors and their selection scheme, the noise parameter π should also be considered.

1) Offline Clustering Results: The performance of our proposed OWAP clustering method is compared with the traditional affinity propagation clustering method and the popular K-means clustering method. Actually, for fingerprinting localization systems, besides the location accuracy, a direct criterion of clustering performance is whether the RPs clustered in one group are also close to each other in the physical space, due that once the RPs far away from each other are clustered in the same group could significantly reduce the location accuracy. The physical display of clustering results adopting these three clustering methods with six monitors is shown in Fig. 4. Obviously, our OWAP is better than both of them, as there are more RPs of different clusters cross each other with these two methods (in order to see clearly, a part of clusters are circled in different line colors). To testify the effectiveness of our proposed clustering method, we also provide the location accuracy results as compared to these three clustering methods and a method without clustering processing, which is shown in Fig. 5. Two measurement indexes of Cumulative Distribution Functions (CDFs) of location errors and statistical location errors are adopted. It demonstrates that the proposed OWAP clustering method outperformes than others.

2) Rogue AP Localization Results: i) Discussion of Gaussian noise π. Fig. 6 shows the locating performance under different values of noise variance, from which we can see that the location accuracy becomes lower as the increasing of variance. This is a common phenomenon since the variance denotes the short time recorded online fingerprint' range of deviation from the corresponding long time recorded offline fingerprint. It's noteworthy that variance equaling to 0 dBm represents the environment is ideal where no noise exists in the online records, and the probability of this environment is about 82%, which proves the effectiveness of the improved CS based sparse recovery technique theoretically.

ii) Discussion of the number of monitors selected M. To verify the influence of M to location accuracy and the correctness of the derivation of minimum number required, we operate simulations under three cases: variance $=$ 0 dBm, variance $=$ 3 dBm and variance $=$ 5 dBm. The reason why we choose these three situations is that noise variance $=$ 0 dBm means the environment is ideal, where we could verify the effectiveness of our derivation theoretically, and variance $=$ 3 dBm and variance $=$ 5 dBm represent two typical environments which have normal noise and strong noise, respectively. Simulation results are shown in

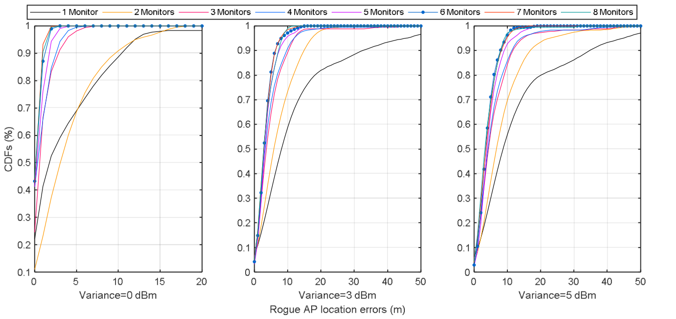


Fig. 7. CDFs of rogue AP location errors under different number of monitors with different noise variances.

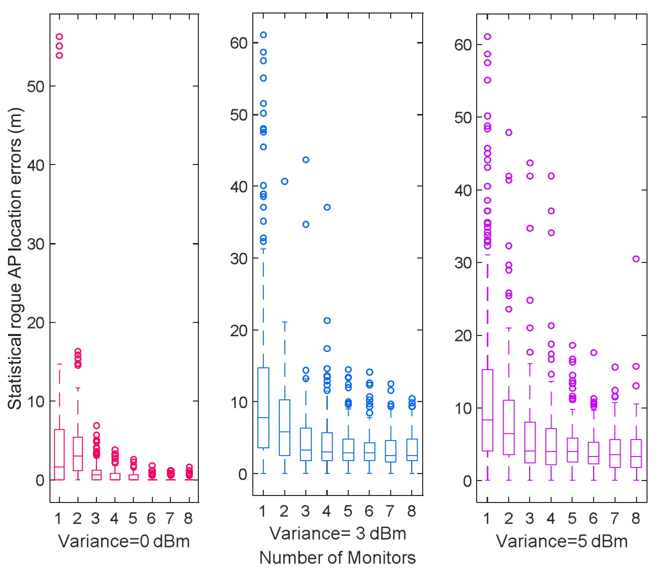


Fig. 8. Statistical rogue AP location errors under different number of monitors with different noise variances.

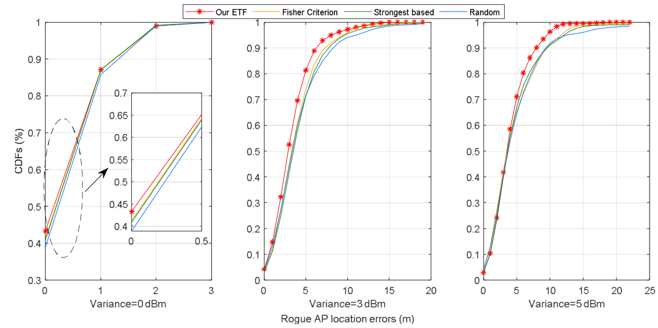


Fig. 9. CDFs of rogue AP location errors under different selection schemes with different noise variances.

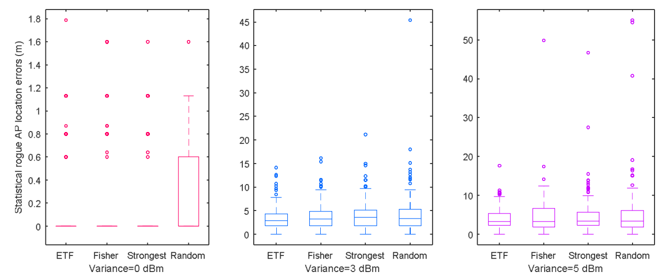


Fig. 10. Statistical rogue AP location errors under different selection schemes with different noise variances.

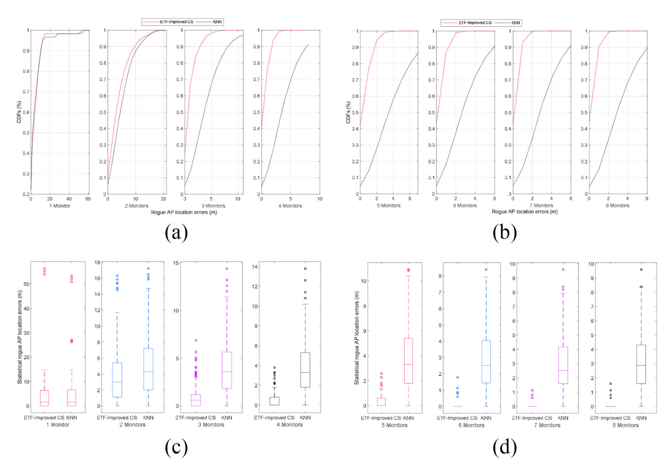


Fig. 11. Rogue AP location errors with ETF-CS and KNN methods respectively. (a) CDFs of rogue AP location errors with 1–4 monitors. (b) CDFs of rogue AP location errors with 5–8 monitors. (c) Statistical rogue AP location errors with 1–4 monitors. (d) Statistical rogue AP location errors with 5–8 monitors.

Fig. 7 and Fig. 8, from which we can see that in these three cases, the location accuracy is prone to stable when the number of monitors is 6 ($\log(N) = 5.89$), which proves the effectiveness of the analysis of minimum value of M in section III C.

iii) Comparison among different monitor selection schemes. In our simulation, we compare our ETF based method with two mostly utilized AP selection methods to construct the CS kernel in the mobile user localization system, the Fisher Criterion based method [19] and the Strongest based method [18], and a random selection scheme. Similarly, we operate simulations under the above three noise environments. Fig. 9 and Fig. 10 show the results, from which we can see that, on the whole, our propose ETF based selection scheme outperforms the others, although when the noise variance equals to zero, the performances among these mentioned methods are very close to each other, this is because when the environment is ideal, the signal overlaps among RPs are so small that they have the strongest discrimination, which lead to high location accuracy, and in this situation the impacts of selection schemes become small.

iv) Comparison with the popular KNN method. The popular KNN method is compared with our presented improved CS based sparse recovery technique o further verify the effectiveness of our method. Both methods are operated under the same ETF monitor selection, and our method is abbreviated as ETF-Improved CS. To test their location accuracy theoretically (without noise), we set variance = 0 dBm, and Fig. 11 provides the result of rogue AP location errors. We can see that the ETF-Improved CS method has wonderful performance when the environment is ideal, but in the same environment, KNN method performs poorly.

3) Joint Rogue AP Localization and Outiler Detection Result: To evaluate the proposed formulation of joint rogue AP

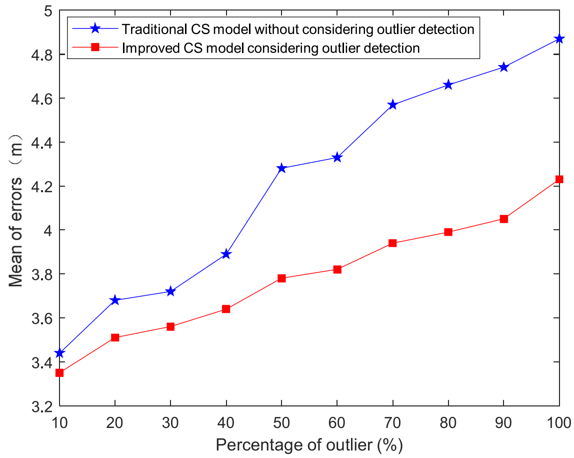
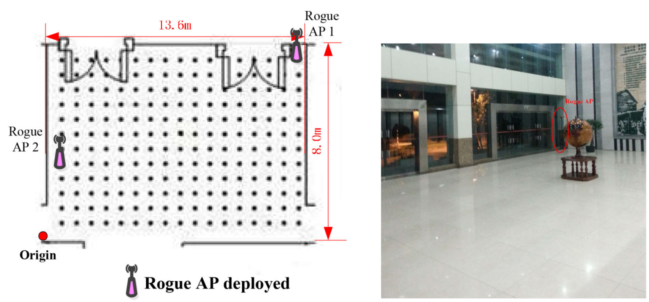


Fig. 12. Mean of rogue AP location errors comparison between the traditional CS model and improved CS model.



(a) (b)

Fig. 13. Experimental environment of scenario 1. (a) Environmental layout. (b) Photos of the environment.

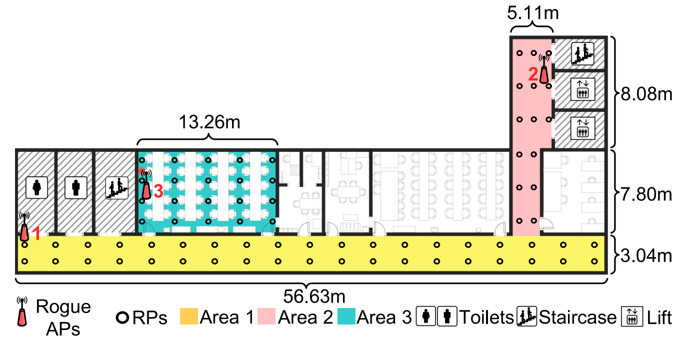
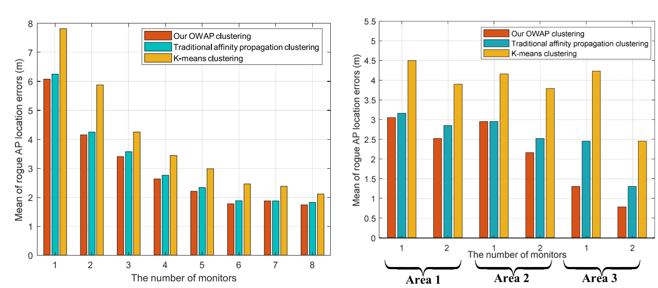


Fig. 14. Experimental environment of scenario 2–4.

(a) (b)

Fig. 15. Interface of our developed software for RSS data recording. (a) Parameters setting. (b) Data display.



(a) (b)

Fig. 16. Mean of rogue AP location errors adopting different clustering methods. (a) Scenario 1. (b) Scenario 2-4.

localization and outlier detection, a total number of 10 monitors have been used, which may randomly be corrupted by outliers. As we stated above, the improved CS model aims at improving the localization robustness to outliers rather than focusing on outlier detection accuracy, hence, Fig. 12 shows the comparison of location errors between the traditional CS model without considering outlier detection and our improved CS model considering outlier detection. We can see that the traditional CS model is more sensitive to outliers especially when there is large number of monitors are corrupted.

B. Experimental Results

In order to prove the practicability of the proposed OWAP clustering method, ETF based selection scheme, and the derivation of minimum number of monitors required, we apply them to two real wireless environments. These two real environments contain four typical scenarios, 1) typical vacancy hall with Line-of-sight condition, as shown in Fig. 13; 2) corridor with Non-line-of-sight condition (Area 1 in Fig. 14); 3) near the lift with moving objects as interference (Area 2 in Fig. 14); 4) crowded rooms with many students (Area 3 in Fig. 14).

In the real environment, the RSS measurements are collected at each RP by a SAMSUNG mobile phone using our developed signal recording software (as shown in Fig. 15).

To verify the effectiveness of our proposed OWAP clustering method, we measure the mean of rogue AP location errors while adopting our proposed OWAP clustering method, the traditional affinity propagation clustering method, and the K-means clustering method, as shown in Fig. 16, from which we can see that, overall, the OWAP clustering method performs better in both real environments, although the localization performances of these four scenarios are different.

Similarly, we provide the location accuracy comparison among KNN method, the improved CS model based on Fisher Criterion selection scheme (Fisher-Improved CS), the improved CS model based on Strongest selection scheme (Strongest-Improved CS) and the improved CS model based on our ETF selection scheme (ETF-Improved CS), which are given in Table I

TABLE I
LOCATION ACCURACY COMPARISON IN THE SCENARIO 1

Number of monitors	**Mean of errors (m)**					
	KNN	**Fisher-Improved CS**	**Strongest-Improved CS**	**ETF-Improved CS**	**Traditional CS without considering outlier**	**Improved CS considering outlier**
1	6.43	6.54	6.25	6.08	1.88	1.79
2	5.22	5.25	5.35	4.15	1.92	1.83
3	4.30	3.80	3.97	3.40	2.42	2.14
4	3.18	3.28	3.88	2.63	2.55	2.19
5	2.25	2.19	2.50	2.21	3.63	2.37
6	2.07	1.99	2.16	1. 77	3.71	2.55
7	2.05	1.91	2.05	1. 87	3.82	2.64
8	2.09	1.89	2.12	1. 74	5.57	3.16

TABLE II
LOCATION ACCURACY COMPARISON IN THE SCENARIO 2–4

Number of monitors		**Location errors (m)**					
		KNN	**Fisher-Improved CS**	**Strongest-Improved CS**	**ETF-Improved CS**	**Traditional CS without considering outlier**	**Improved CS considering outlier**
Area 1	1	3.05	3.05	3.14	3.05	3.14	2.52
	2	3.79	2.52	3.79	2.52	4.18	3.05
Area 2	1	6.92	4.17	4.17	2.95	3.45	2.52
	2	4.17	3.79	4.17	2.16	4.17	2.95
Area 3	1	1.3	2.45	2.45	1.3	2.45	1.3
	2	1.3	0.78	0.78	0.78	4.23	1.3

and Table II. Here we should note that, in scenario 1, the number of monitors varies from 1 to 8, however, in the scenario 2-4, it varies only from 1 to 2. This is because the number of RPs in these four scenarios are different (215 RPs in the scenario 1, 38 RPs in the scenario 2, 15 RPs in the scenario 3, and 20 RPs in the scenario 4).

We can see that the improved CS sparse recovery method outperforms the KNN method in general, but it is noteworthy that once we choose an inappropriate CS kernel, the location accuracy of the improved CS method may be lower than the KNN method, which further proves the importance of kernel optimization when applying the sparse recovery. The last two columns of Table I and Table II are the location errors of the traditional CS model without considering outlier detection and our improved CS model considering outlier detection. The number of monitors here means the monitors corrupted by outliers. We can see the improved CS model is effectiveness and robustness.

V. CONCLUSION

This paper investigates the problem of joint rogue AP localization and outlier detection in WLAN using the improved CS based sparse recovery method. We formulate the rogue AP location and the outiers as sparse vectors in discrete spatial domain and signal domain, respectively, then apply the improved CS based sparse recovery method to recover these two sparse vectors to jointly estimate rogue AP's location and do outlier detection, which increases the localization robustness. To achieve high sparse recovery ability, the CS kernel optimization is conducted which contains deducing the minimum number of monitors required for rogue AP localization and proposing an ETF based monitors selection scheme. It provides a guidance to system design and monitors layout. In addition, a novel OWAP clustering method is also proposed to conduct coarse localization. It utilizes the prior knowledge of physical coordinates which is more suitable for localization systems. Moreover, both simulations and experiments have demonstrated the superiority of our scheme as compared to the most popular methods.

REFERENCES

[1] Y. L. Hsu, F.-H. Hsu, and C.-S. Wang, "A solution to detect the existence of a malicious rogue AP," *Comput. Commun.*, 2019.

[2] H. Han, B. Sheng, C. Chiu, Q. Tan Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912–1925, Nov. 2011.

[3] W. Wu, X. Gu, K. Dong, X. Shi, and M. Yang, "PRAPD: A novel received signal strength-based approach for practical rogue access point detection," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 8, 2018.

[4] S. B. Vanjale, and P. B. Mane, "Multi parameter based robust and efficient rogue AP detection approach," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 139–156, 2018.

[5] R. Jang, J. Kang, A. Mohaisen, and DaeHun Nyang, "Rogue access point detector using characteristics of channel overlapping in 802.11 n," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst.*, 2017, pp. 2515–2520.

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, 2008, pp. 1768–1776.

[7] T. M. Le, P. R. Liu, and M. Hedley, "Rogue access point detection and localization," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun.*, 2012, pp. 2489–2493.

[8] C. Wang, X. Zheng, Y. J. Chen, and J. Yang, "Locating rogue access point using fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 16, no. 9, pp. 2560–2573, Sep. 2017.

[9] L. Gong *et al.*, "LAMP: Lightweight and accurate malicious access points localization via channel phase information," in *Int. Conf. Wireless Algorithms, Syst. Appl.*, 2018, pp. 748–753.

[10] Y. Chen, X. Wang, D. Yu, Y. Yang, and J. Chen, "Localizing access point through simple gesture," *IEEE Access*, vol. 6, pp. 38870–38880, 2018.

[11] W. Liu, X. Luo, Q. Mu, Y. Liu, and F. Liu, "An indoor Wi-Fi access points localization algorithm based on improved path loss model parameter calculation method and recursive partition," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 5, 2019, Art. no. 1550147719852034.

[12] F. Zhao, H. Luo, H. Geng, and Q. Sun, "An RSSI gradient-based AP localization algorithm," *China Commun.*, vol. 11, no. 2, pp. 100–108, 2014.

[13] C. Feng, S. Valaee, and Z. Tan, "Multiple target localization using compressive sensing," in *Proc. GLOBECOM IEEE Global Telecommun. Conf.*, 2009, pp. 1–6.

[14] K. Yan, H.-C. Wu, H. Xiao, and X. Zhang, "Novel measurement matrix optimization for source localization based on compressive sensing," in *Proc. IEEE Global Commun. Conf.*, 2014, pp. 341–345.

[15] J. Deng, Q. Cui, X. Zhang, and X. Xu, "Compressive sensing based indoor positioning with denosing and filtering in LF space," in *Proc. 23rd Int. Symp. Pers. Indoor Mobile Radio Commun.*, Sep. 2012, pp. 2477–2482.

[16] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern WLAN fingerprinting indoor positioning methods and deployment challenges." *IEEE Commun. Surv. Tut.*, vol. 19, no. 3, pp. 1974–2002, Jul.–Sep. 2017.

[17] C. Feng, W. S. A. Au, S.Valaee, and Z. Tan, "Compressive sensing based positioning using RSS of WLAN access points," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[18] M. A. Youssef, A. Agrawala, and A. U. Shankar, "WLAN location determination via clustering and probability distributions," in *Proc. IEEE 1st Int. Conf. Pervasive Comput. Commun.*, Mar. 2003, pp. 143–150.

[19] A. Kushki, K. N. Plataniotis, and A. N. Venetsanopoulos, "Kernel- based positioning in wireless local area networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 6, pp. 689–705, Jun. 2007.

[20] T. Zhang, F. Ma, D. Yue, C. Peng, and G. MP O'Hare, "Interval type-2 fuzzy local enhancement based rough k-means clustering considering imbalanced clusters," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 9, pp. 1925–1939, Sep. 2020.

[21] U. Bodenhofer, A. Kothmeier, and S. Hochreiter, "APCluster: An R package for affinity propagation clustering," *Bioinformatics*, vol. 27, no. 17, pp. 2463–2464, 2011.

[22] Y. C. Chen, W. C. Sun, and J. C. Juang, "Outlier detection technique for RSS-based localization problems in wireless sensor networks," in *Proc. SICE Annu. Conf.*, Aug. 2010, pp. 657–662.

[23] C. Laoudias, M. P. Michaelides, and C. G. Panayiotou, "Fault detection and mitigation in WLAN RSS fingerprint-based positioning," in *Proc. Int. Conf. Indoor Position. Indoor Navig. (IPIN)*, Sep. 2011, pp. 1–7.

[24] Z. Gao, L. Dai, S. Han, I. Chih-Lin, Z. Wang, and L. Hanzo, "Compressive sensing techniques for next-generation wireless communications," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 144–153, Jun. 2018.

[25] C. Feng, W. S. A. Au, S. Valaee, and Z. Tan, "Received-signal-strength-based indoor positioning using compressive sensing," *IEEE Trans. Mobile Comput.*, vol. 11, no. 12, pp. 1983–1993, Dec. 2012.

[26] A. Gondeau, Z. Aouabed, M. Hijri, P. Peres-Neto, and V. Makarenkov, "Object weighting: A new clustering approach to deal with outliers and cluster overlap in computational biology," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, to be published, doi: 10.1109/TCBB.2019.2921577.

[27] T. GeokKim, F. Hossain, and A. T. W. Chiat, "A novel 3D ray launching technique for radio propagation prediction in indoor environments," *PLoS One* 13, no. 8, 2018, Paper e0201905.

[28] B. Zhang, X. Cheng, N. Zhang, Y. Cui, Y. Li, and Q. Liang, "Sparse target counting and localization in sensor networks based on compressive sensing," in *Proc. IEEE INFOCOM*, 2011, pp. 2255–2263.

[29] C. D. Sigg, T. Dikk, and J. M. Buhmann, "Learning dictionaries with bounded self-coherence," *IEEE Signal Process. Lett.*, vol. 19, no. 12, pp. 861–864, Dec. 2012.

Qiaolin Pu (Member, IEEE) received the B.Sc. and M.Sc. degrees in information and communication engineering from the Chong Qing University of Posts and Telecommunications (CQUPT), China, in 2011 and 2016, respectively. She joined CQUPT as an Assistant Professor after graduation. She is currently working toward the Ph.D. degree with Hong Kong Baptist University in computer science. Her research interests include indoor localization, signal processing, and ubiquitous/pervasive computing.

Joseph Kee-Yin Ng (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science all from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 1986, 1988, and 1993, respectively. He joined Hong Kong Baptist University, Hong Kong, in 1993, and is currently a Professor and the Director of the Research Centre for Ubiquitous Computing, Department of Computer Science. He is also the Program Coordinator of the Computer Science degree program and introduced Health Information Technology and Health Informatics into the undergraduate as well as the graduate program in HKBU. He has obtained two patents and authored or coauthored more than 150 technical papers in journals and conferences. His current research interests include real-time & embedded systems, multimedia communications, and ubiquitous/pervasive computing.

Mu Zhou (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in information and communication engineering from the Harbin Institute of Technology, China, in 2006, 2008, and 2012, respectively. He was a Joint-cultivated Ph.D. Student with the University of Pittsburgh, USA and a Postdoctoral Research Fellow with the Hong Kong University of Science and Technology, China. Later, he joined Chongqing University of Posts and Telecommunications (CQUPT), China, where he has been a Full Professor with the School of Communication and Information Engineering since 2014. He was supported by the Chongqing Municipal Program of Top-Notch Young Professionals for Special Support of Eminent Professionals and awarded with Outstanding Scientist of Chinese Institute of Electronics and Outstanding Cooperation Project Award from Huawei Technologies Co., Ltd. He has authored or coauthored more than 100 peer-review research papers such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE, and served on Technical Program Committees of IEEE ICC, GLOBECOM, WCNC, VTC, and more. His main research areas include wireless localization and sensing, signal processing and detection, and machine learning and information fusion.

Jie Wang (Senior Member, IEEE) received the B.S. degree from the Dalian University of Technology, Dalian, China, in 2003, M.S. degree from Beihang University, Beijing, China, in 2006, and the Ph.D degree from the Dalian University of Technology, Dalian, China, in 2011, all in electronic engineering.

He is currently a Full Professor with Dalian Maritime University. He used to be an Associate Professor with Dalian University of Technology from 2014 to 2017. He was a Visiting Researcher with University of Florida from 2013 to 2014. His research interests include wireless localization and tracking, radio tomography, wireless sensing, machine learning, wireless sensor networks, and cognitive radio networks. He is an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.