Detecting Rogue AP with the Crowd Wisdom

Tongqing Zhou*, Zhiping Cai*, Bin Xiao†, Yueyue Chen*, Ming Xu*
*College of Computer, National University of Defense Technology, Changsha, China.
Email:{zhoutongqing, zpcai, yueyuechen, xuming}@nudt.edu.cn
†Department of Computing, The Hong Kong Polytechnic University, Hong Kong. Email: csbxiao@comp.polyu.edu.hk

***Abstract*—WiFi networks are vulnerable to rogue AP attacks in which an attacker sets up an imposter AP to lure mobile users to connect. The attacker can eavesdrop on the communication, severely threatening users' privacy. Existing rogue AP detection solutions are confined to some specific attack scenarios (e.g., by relaying the traffic to a target AP) or require additional hardware. In this paper, we propose a crowdsensing based approach, named CRAD, to detect rogue APs in camouflage without specialized hardware requirement. CRAD exploits the spatial correlation of RSS to identify a potential imposter, which should be at a different location from the legitimate one. The RSS measurements collected from the crowd facilitate a robust profile and minimize the inaccuracy effect of a single RSS value. As a result, CRAD can filter out abnormal samples sensed in the realtime by dynamically matching the profile. We evaluate our approach with both a public dataset and a real prototype. The results show that CRAD can yield 90% detection accuracy and precision with proper crowd presence, even when the rogue AP is launched close to the legitimate one (e.g., within $1m$).**

I. Introduction

The past few years have witnessed a surge in the popularity of Wireless Local Area Networks (WLAN). People rely more and more on the wireless Access Point (AP) to get access to the Internet. In order to attract customers, many public places (e.g., shops, hotels, airports, etc.) provide WiFi hotspot service for free. The openness of such places and the weak security mechanism taken by these hotspots make them vulnerable to fraud and identity spoof, known as the problem of rogue APs [1]. In such attacks, a rogue AP pretends to be a legitimate one by using the same name (SSID), but is actually launched by an attacker. Through fostering a stronger signal strength on some mobile devices, rogue APs can induce them to connect, and analyze or manipulate the communication, severely threatening users' privacy.

Extensive work has been devoted to addressing the problem of detecting rogue AP [2]. However, the problem remains to be largely open because of the detection scalability issue and hardware support requirement. Specifically, fingerprint-based approaches propose to identify the legitimate AP with additional hardware [3] [4] or wireless-oriented fingerprint [5] [6]. APs exhibiting different characteristics are determined to be rogue ones. However, such approaches are lack of applicability for requiring the setup of dedicated specialized hardware, such as Air Monitor (AM), Wireless Intrusion Detection System (WIDS), etc. On the other hand, some schemes have been proposed to analyze packet characteristics on the time domain [7] [8] [9]. The underlying idea is that if a rogue AP relays user traffic via the legitimate AP, then connections to the rogue AP would experience additional latency. These solutions depend on the scenario in which the rogue AP introduces one more wireless hop, which is not effective when the attacker has his/her own Internet access. Existing approaches for rogue AP detection only work on specific scenarios or hardware. Thus, we attempt to design an approach that is effective for all rogue AP types with non-specialized hardware.

This paper proposes a Crowdsensing based Rogue AP Detection approach (CRAD). As a new sensing paradigm, crowdsensing uses pervasive mobile devices to sense and collect information from the environment [10]. On the other hand, Received Signal Strength (RSS) is a typical wireless information, and is frequently sensed by mobile devices to estimate channel condition. RSS at several different locations can be used to localize a RF transmitter. Intuitively, such spatial correlation characteristic can also be used to identify a rogue AP with a different location from the legitimate one. Based on this concept, in this work, we propose to exploit the mobile crowd connected to a specific AP, which is also the potential victim, to collect RSS measurements, profile legitimate AP, and discover possible imposters. The advantages of exploring crowd wisdom here are three-fold: 1) it requires no additional hardware other than users' devices; 2) it ensures that frequently accessed locations are profiled, and vulnerable spots monitored; 3) it mitigates the misleading effect of error-prone wireless measurements.

Despite the above benefits, there are several challenges of applying crowdsensing to rogue AP detection: 1) How to maintain an effective profile for AP identification and measurements matching? 2) How to design a proper matching operation between the profile and the crowdsensing RSS measurements considering location distinction among different samples? For the first question, CRAD proposes a grid-based measurement profiling method to record the collected information. It provides flexibility for matching item and indexing during the matching process. CRAD attempts to tackle the second challenge based on an observation that locations near each other would observe similar RSS. CRAD checks each item of a new sample by comparing it with its nearest physical neighbor's record in the profile, and facilitate an overall evaluation for the corresponding AP with the majority voting. CRAD is designed to be running as a background service without user intervention.

The main contributions of this paper include:

1) We propose a novel rogue AP detection approach based on mobile crowdsensing, named CRAD, to formally

monitor WiFi network with non-specialized hardware in the background. As far as we know, it is the first attempt to exploit the crowd wisdom to detect rogue APs.

2) We propose a grid-based profiling method to maintain the crowdsensing measurements, and a matching mechanism to identify imposter with inter-neighbors' comparison and the majority voting.
3) We extensively evaluate CRAD with both a real-world dataset and our own implementation. Results show that CRAD can yield a high detection accuracy and precision under the normal attack model.

II. Attack Model

It is easy to deploy a rogue AP, especially in a public WiFi hotspot with weak security mechanism [9]. An attacker can use a hotspot router, a laptop with open access tools (e.g., Airbase-ng), or even a smartphone with tethering apps (e.g., Android WiFi tether) to impersonate a legitimate AP. In order to avoid scanning-based detection, the attacker would clone both the SSID and the MAC address of the legitimate target. Furthermore, the attacker would attempt to provide a stronger signal strength on the victims than the legitimate AP, either by moving close to the victim or increasing its transmission power. Note that the rogue AP does not have to use a power that fosters a strength advantage on every devices. So only some victims would be lured, while other devices in the field would still connect to the legitimate one but experience a different signal field. We assume that a rogue AP can only be present after the start-up of a hotspot (the attacker should find the target first). The administrator is not required to assist the detection. However, an unidentified AP placed near the public AP would very likely attract his/her attention.

Typically, there are two categories of rogue APs:

Coexistence. The legitimate AP and the rogue AP coexist at the spot when the attack goes on. This category can be further classified into two forms, namely, with or without relay. Initially, a rogue AP would spoof its network identifier and increase its signal strength to lure mobile users to connect. Then it can simply relay the network flow through the legitimate AP (i.e. with relay), or provide network access using its own Internet connection (i.e. without relay). The latter form could bypass most time-based detection approach.

Replacement. A powerful attacker may manage to replace the legitimate AP by shutting it down or DDoS attacks. In this case, only one active AP is available in the location, and users connect to the rogue AP with no other choices.

Based on a deployed rogue AP, an attacker can eavesdrop on the wireless communication of the connected devices, and launch a series of attacks, putting users' sensitive information in danger. We attempt to mitigate the above threats[1] with crowdsensing. Note that there may exist malicious users who intend to tamper their measurements and submit misleading reports [12], we defer such data credibility threat to future work. In other words, we believe in the majority's observations.

[1]Fake Base Station is a similar threat, while targeting base stations [11].

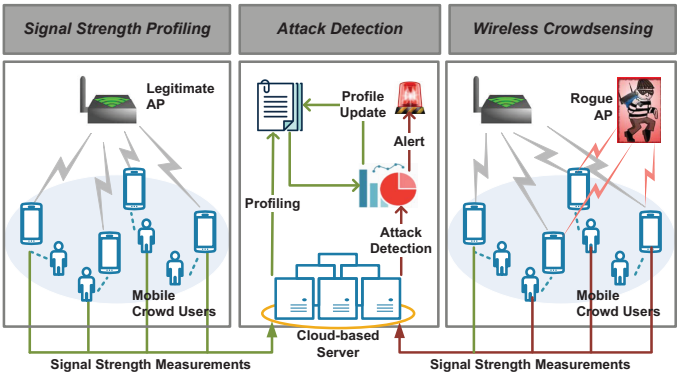


Fig. 1. Overview of the proposed approach.

III. Design of CRAD

Generally, mobile users connected to one specific hotspot are the crowd. Signal strength sensed by each individual of the crowd constitute a unique spatial identifier for the hotspot. By passively monitoring the measurements collected by the crowd, we shall discover the appearance of an imposter.

As shown in Fig. 1, our approach consists of three phases. Signal strength profiling builds fingerprint for the legitimate AP based on signal strength measurements. For each AP, a profile is maintained in the cloud. Wireless crowdsensing is performed locally by the mobile crowd in the real time, and provides wireless features of the network for further security check. Finally, attack detection is carried out to compare the dynamically collected information with the profile, and triggers an alert to the crowd if a rogue AP is detected.

A. Background

In CRAD, we leverage the mobile crowd to accomplish profiling and sensing of the wireless network. Four basic questions need to be clarified before describing the details: 1) What are the incentives for mobile users to participate? 2) Why a crowd is required? 3) How to obtain the location? 4) Is location discrepancy a reasonable assumption?

The incentives. A critical issue for crowdsensing is the incentive for user participation. In fact, users have incentives to do so. First, the smartphone devices of users already perform wireless scan aggressively in the background, and the frequency is sufficient to facilitate effective run time monitoring. Second, the victims of rogue AP attacks are users themselves. It is reasonable for them to be suspicious of the hotspot and take actions to guarantee a benign environment.

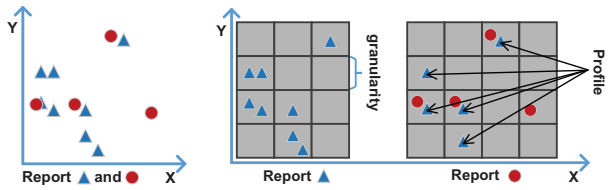
Crowd v.s. individual. A crowd of mobile sensors are essential for CRAD. If only one stationary smartphone is available, the attacker could create a similar RSS as undetectable camouflage by adjusting the transmission power of the rogue AP [8]. Adopting measurements of multiple locations can facilitate a robust fingerprint to avoid such misleading effect. Note that the crowd is actually a virtual crowd, wherein a moving device within a specific time interval can be regarded as independent sensors at different locations.

Location tag. We assume there is a location tag for each reported measurement. For the outdoor situation, such as campus wireless hotspots, the location information could be obtained with the GPS module. However, GPS becomes ineffective for indoor scenarios, as many public hotspots are. In our experiments, we provide a reference map, and collect location by manually clicking on it. Notice that this cannot serve as a robust solution. Alternatively, one can easily extend CRAD by adopting the state-of-the-art indoor localization method.

Location discrepancy. One basic assumption of CRAD is that there exists a location discrepancy between a legitimate AP and a rogue AP, as wished by attackers. First, a rogue AP would be easily exposed when set close to the legitimate one. On the other hand, by physically moving closer to some victims, a rogue AP could yield a stronger signal strength than the legitimate one on the victims' side, inducing them to connect with a high probability[2].

B. Signal Strength Profiling

CRAD collects RSS information presented in the form of $\langle SSID_i, BSSID_i, l_i, r_i\rangle$ for a set of APs, where l_i is the sensing location, and r_i is the set of RSS measurements sensed at location l_i. For a specific AP with identifier id, the corresponding RSS measurements within a time interval I construct a report, denoted as $\Re_{id} = \{\langle l_i, r_i\rangle | 1 \leq i \leq Dim\}$, where $Dim = \|\Re_{id}\|$ is the number of different locations, named measurement dimension. CRAD attempts to build a profile P_{id} based on $\Re_{id}$.



(a) Naive method (b) Grid-based profiling method

Fig. 2. Illustration of signal strength profiling method for a specific AP. Two reports are collected with the former one (i.e. blue triangle) for profiling, and the latter one (i.e. red circle) for matching. For simplicity, CRAD maps the RSS measurements to a two-dimensional physical space, which can be interpreted as the xy-coordinates of the mobile devices.

A naive method to profile the legitimate AP is to set $P_{id} = \{\langle l_i, Avg(r_i)\rangle\}$, namely, regarding l_i as the attribute, and mean of r_i as the value, as shown in Fig. 2(a). During the profiling phase, user mobility provides CRAD the ability to collect RSS measurements with a larger measurement dimension. However, since the location is spatially continuous, the profile of such method would have an inflated scale with consecutive arriving reports. Moreover, it is intractable to perform effective matching between such profile (i.e. blue triangle in Fig. 2(a)) and a sample (i.e. red circle in Fig. 2(a)) as they are not aligned on the attribute domain (i.e. locations).

[2]By default, given a set of AP with the same SSID, wireless device will select the AP with the highest SINR to connect to.

Algorithm 1 Grid-based Signal Strength Profiling

Input:
Report $\Re_{id}$, Area A_{id} enclosed by locations of $\Re_{id}$, Granularity threshold $\hat{g}$, Measurement index i, j $(i \neq j)$.

Output:
Profile P_{id} for AP_{id}

1: Compute the inter-distance $d_{i,j}$ between $\Re_{id}.l_i$ and $\Re_{id}.l_j$
2: Compute the strength distance $\triangle r_{i,j}$ between $Avg(\Re_{id}.r_i)$ and $Avg(\Re_{id}.r_j)$
3: Set threshold $\triangle r = \frac{1}{\|\Re_{id}\|} \cdot \sum_{i=1}^{\|\Re_{id}\|} Std(\Re_{id}.r_i)$
4: Sort (in ascending order) distances $\{d_{i,j}\}$ into $D = \{d_k\}$
5: **for** $k = 1 \rightarrow \|D\|$ **do**
6: $\quad i = d_k(1), j = d_k(2)$
7: $\quad$ **if** $\triangle r_{i,j} > \triangle r$ **then**
8: $\quad\quad \bar{d} = 1/2 \cdot (d_{k-1} + d_k)$
9: $\quad\quad$ break
10: $\quad$ **end if**
11: **end for**
12: Granularity is calculated as $g = max\{\bar{d}, \hat{g}\}$
13: Divide area A_{id} into cells $C = \{c_i\}$ with granularity g
14: $P_{id} = \{\langle c_i, r_{c_i}\rangle |\ l_{c_i}\ is\ within\ c_i\}$

CRAD proposes a grid-based method to perform AP profiling, as described in Algorithm 1. Through transforming the sensing area into small cells, and maping RSS measurements into them, the algorithm attempts to construct a coarse profile as shown in Fig. 2(b). The rationale is that RSS are spatial correlated during the same time interval. In other words, RSS measurements within a certain distance are similar with each other, so a fine-grained profile is indeed not necessary.

Specifically, CRAD first calculates a granularity as the maximum value of a predefined granularity $\hat{g}$ and a dynamically obtained value $\bar{d}$. For $\bar{d}$, the algorithm finds the minimum distance between a pair of measurements whose RSS difference is larger than threshold $\triangle r$, and sets $\bar{d}$ as the mean of this distance and the proximate distance smaller than it. The threshold $\triangle r$ is set to be the mean value of RSS deviation at each location. The underlying reason is that if two neighbors' RSS are undistinguishable, they could be regarded as measurements from one unit. Note that it is still possible for two neighbor locations to exhibit quite different RSS (e.g., misbehavior of the wireless interface), resulting in a small $\bar{d}$. Parameter $\hat{g}$ is introduced to avoid such small granularity. Given the granularity g, CRAD then generates cells with size $g \times g$ to fill in the sensed space. Finally, the profile is constructed using the set of cells and the RSS measurements within each cell. The characteristic value of each cell would be calibrated with verified new arriving reports to update the profile in the real time.

C. Rogue AP Detection

CRAD uses the profile as a fingerprint, and check each new arrival report $\Re$ by matching with the profile. Specifically, we need to first find the corresponding item in P_{id} to match with

for each measurement in $\Re$, and then determine whether $\Re$ indicates an abnormal considering the overall matching level.

For the first part, CRAD maps the RSS items $\{\langle l_i, r_i\rangle\}$ in new report $\Re$ to cells in P_{id} to obtain a sample $S = \{\langle c_j, r_{c_j}\rangle\}$, where $c_j.x = \lceil(\Re.l_i.x - x_0)/g\rceil$, and $c_j.y = \lceil(\Re.l_i.y - y_0)/g\rceil$. The number of items in S is called the crowd presence. If an item is out of the area A_{id} or the profile's corresponding cell is null (i.e. not measured before), we mark it as unchecked. By doing this, we find the nearest neighbor for each item of $\Re$ in P_{id}, as shown with the red circles in Fig. 2(b). Here, the grid-based profile provides the ability to find the target cell for new measurement by a simple transformation instead of calculating and sorting the inter-distances.

The matching operation is performed based on two basic observations: 1) RSS measured at one location are similar to each other, and 2) locations near each other would observe similar RSS. With these observations, CRAD performs rogue AP detection by comparing sample value with profile record in each cell, which are supposed to be similar. Specifically, the difference between the mean value of the record and sample measurements are calculated, and then compared with a threshold $ME \cdot Std(P_{id}.r_{c_i})$. Wherein, $Std(P_{id}.r_{c_i})$ is the standard deviation of the recorded RSS in c_i, and ME is a spatial and temporal variation factor. A difference bigger than the threshold is suggested to be obvious, and the sample value is marked as an abnormal measurement. Otherwise, the sample value is marked as normal. Thus, with a small ME, the detection algorithm would be sensitive to the variation in measurements (*Type I error*), while a big ME would ignore some abnormal measurements (*Type II error*). In this paper, we set parameter ME to

$$ME = max(R(P_{id}.r_{c_i})/Std(P_{id}.r_{c_i}), R(S.r_{c_i})/Std(S.r_{c_i})),$$

where $R(X)$ is the range of set X. ME is adjusted according to the range of measurements in both profile and samples.

After going through all the cells, CRAD estimate the security of current AP using the majority voting. Through majority voting, the wisdom of crowd is exploited to identify rogue, since it is abnormal for most locations to observe a drastic change in RSS. Specifically, if more abnormal measurements are observed than the normal ones among the matching results, then a rogue AP attack is supposed to be on-going. In such situation, the crowd will receive an alert and be suggested to disconnect from the malicious AP. On the other hand, the samples are considered as normal, and used to update or complete (with the items labelled unchecked) the profile.

We propose to introduce a reset mechanism initiated by the administrator to report an AP movement event, and rebuild the profile with subsequent crowdsensing reports.

IV. Experiments

In this section, we evaluate the effectiveness of the proposed CRAD approach for detection of rogue AP, on an indoor localization dataset UJIIndoorLoc [13] and a proof-of-concept prototype. We first show the approach feasibility with UJIIndoorLoc, then evaluate the performance with the prototype.

A. Feasibility Evaluation

With UJIIndoorLoc, we attempt to prove that it is feasible to identify AP with crowdsensing RSS. To do this, we first generate a fingerprint[3] for each AP from the training subset. Here, fingerprint of an AP consists of measurements from all the locations that observe it. Then we randomly choose measurements of the 520 APs to construct test samples. Two test groups of samples are generated, one from the training subset and one from the validation subset, to conduct two independent tests. Finally, we iteratively regard each AP as the target and compare its fingerprint with the generated test samples to find the best match as follows:

$$M_i = \underset{1\le j\le 520}{argmin}\left(\frac{1}{N_i}\cdot\sqrt{\sum_{loc=1}^{N_i}(FP_i^{loc} - S_j^{loc})}\right),$$

where M_i is the index of the best match AP, FP_i^{loc} is the fingerprint element from location loc for the i-th AP, and S_j^{loc} is the corresponding test measurement from the j-th sample. Note that we do not use the proposed method, because the best match is what we try to obtain here. For each FP_i being checked, the best match sample is supposed to be the sample from the i-th AP (i.e. S_i), namely, we expect $i = M_i$.

TABLE I
Matching results. Each row shows the test group, the number of fingerprint and valid test, the number of match, and the number of mismatch. Test sample that includes measurements for target AP is defined as a valid test.

Test Group	# FP	# Valid test	# Match	# False
subset 1	520	363	335 (92.3%)	28
subset 2	520	161	132 (82.0%)	29

The matching results are concluded in Table I. We can see that successful matching ratio is 92.3% (with 3% matching with its neighbor) and 82% (with 60% matching with its neighbor[4]) for the two subsets, respectively. The decrease of matching ratio for subset 2 can be explained by involving fewer sensing locations. Hence, it is reasonable to use crowdsensing RSS as an identifier for a legitimate AP.

B. Performance Evaluation

1) ***Setup****:* Our testbed consists of a $10 \times 8m$ section of a laboratory environment. As shown in the map area of Fig. 3, we have installed three IEEE 802.11b/g APs: one is treated as the legitimate AP (we name it A), and the remaining APs (we name them B and C) act as rogue APs. The APs are off-the-shelf NETGEAR WG102 units, and are mounted on the desk. They are configured with the same SSID, while the MAC addresses are not modified to obtain the ground truth. In the profiling stage, only A is switched on. In the detection stage, B and C are switched on one by one.

[3]In this part, we do not build a grid-based profile for the AP as measurements of fingerprinting and testing round are from the same locations.

[4]The positions of APs in UJIIndoorLoc are unknown, we guess dense deployed APs are utilized with some of them very close to each other.

Fig. 3. Screenshot of the programmed phone. Down below the interface is a loaded reference map describing the testbed environment.

We develop a RSS measuring and recording prototype based on android, named *CrowdMeasure*. Fig. 3 presents the interface of *CrowdMeasure*. One can load a map and mark a location (as an alternative to indoor localization technique) to perform RSS measuring. We have a researcher walking around with a smartphone (Huawei Mate 7 with android 6.0) installed *CrowdMeasure* to collect RSS information. It collects RSS measurements every $1sec$. During profiling phase, the smartphone is put on the middle of the desks. During test samples collection, we put the device on a random place of each desk, which is supposed to be different from the corresponding profiling location.

Finally, we realize CRAD's detection logic in Matlab (this can be easily extended to the cloud environment), and use it to analyze the collected data. Considering the experiment environment, the granularity threshold $\hat{g}$ is set to be $1m$, same as the length of the desk.

*2) **RSS Observations**:* We first investigate the RSS difference between dynamically collected samples and profile records. As shown in Fig. 4, samples from the legitimate AP tend to be similar with the records, while samples from the rogue AP are quite different. For most locations, we can easily distinguish normal samples from abnormal ones. However, for several locations (4 in this experiment), RSS of the legitimate one and rogue one all match well with the profile (location 15, 16 and 18), or even worse, RSS of the rogue one is more similar to the record than its counterpart (location 3). The former situation is actually normal when the sensing location is on or near the perpendicular bisector of the line segment between the location of rogue and legitimate AP. We owe the latter situation to a bad record in the profile, which may be caused by sensor error or the mixture of noise. Regardless of such undistinguishable situations, CRAD can identify the rogue by referring to the majority observation of the crowd, in which ≥ 6 sensing locations are enough to detect an abnormal. Note that the bad records would be calibrated to prevent the spread of misleading effect on receiving a normal report.

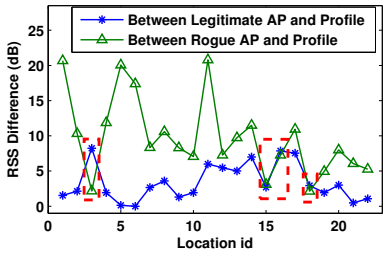


Fig. 4. The absolute RSS differences between profile records and samples from rogue AP and legitimate AP. The comparison is carried out at 22 different locations. The red dashed rectangles enclose several locations where rogue presents a RSS that is similar or undistinguishable with the legitimate one.

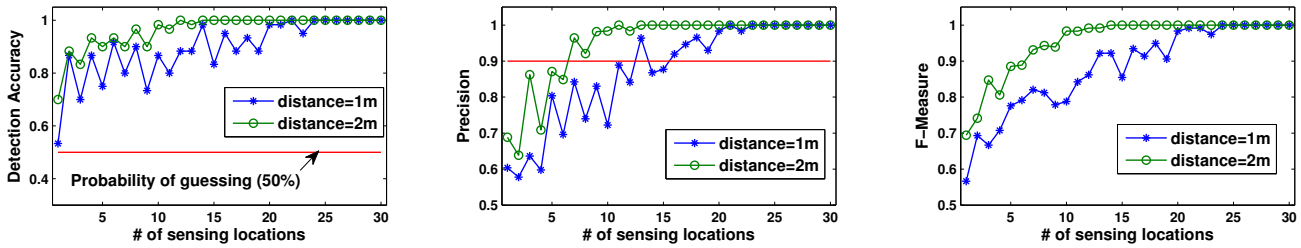
*3) **Distance between Rogue AP and Legitimate AP**:* We switch on one rogue AP each time, and investigate the impact of distance between rogue AP and legitimate AP on CRAD's effectiveness under the replacement attack model. We test two distances separately under different crowd presence. During each test, we change the crowd presence with the number of sensing locations increasing from 1 to 30. For each presence level, the test is repeated 60 times by randomly selecting the sensing locations.

Fig. 5 illustrates the test results. The detection accuracy (i.e. recall) in Fig. 5(a) is the ratio of the number of tests in which the rogue AP is correctly identified over 60 times. As expected, CRAD's detection accuracy increases with more sensing locations. For $distance = 1m$, we can obtain accuracy of 0.9 when the number of locations reach half of the profile size (i.e. 15). In contrast, for $distance = 2m$, the detection accuracy reaches 0.9 with only 4 different locations, while reaching 100% with around half of the profile size.

The precision in Fig. 5(b) is the ratio of the number of actually true detection over all reported detections. A high precision means that the ratio of *Type I error* is small, and vice versa. Similar to the performance on detection accuracy, CRAD's precision is positive correlated to the crowd presence. As we can see, the precision for $distance = 2m$ is better than $distance = 1m$ for most reports. Specifically, when the rogue is $1m$ away from its legitimate target, the precision keeps fluctuating until the presence of around 15 sensing points. In the other situation, only 7 sensing locations are required to obtain a precision of 0.9, and the false alarm is nearly 0 with more than 10 reporting locations.

Finally, we compute the F-Measure as $\frac{2 \cdot Accuracy \cdot Recall}{Accuracy + Recall}$ in Fig. 5(c). For both scenarios, F-measure is fairly high and increases with more crowd reports. Meanwhile, CRAD's F-Measure regarding $distance = 2m$ outperforms its performance when $distance = 1m$ by a wide margin.

The performance gap of CRAD under different rogue-legitimate distances in Fig. 5 is due to the characteristic of RSS correlation. In other words, RSS of the rogue AP and its target AP observed at the same location become more and more different as the distance between them increases. We emphasize that $distance = 1m$ (even $2m$) is a special case,



(a) Detection accuracy under different distances (b) Precision under different distances (c) F-Measure under different distances

Fig. 5. The performance of CRAD against crowd presence (number of sensing locations) under different rogue and legitimate distances.

and it is actually not easy for a rogue to get that close without being noticed. Even for this case, CRAD can successfully pick out the imposter provided adequate crowd presence.

*4) **Attack Model**:* Two common forms of rogue APs are considered in this work. Section IV-B3 discusses the impact of distance of replacement attacks. In this part, we investigate the performance of CRAD when dealing with coexistence attacks. Here, we set up the imposter $2m$ away from the legitimate one.

As shown in Fig. 6, CRAD's performance increases with more locations involved, and can formally detect the potential rogue without false alarms when enough crowd present (i.e. 15 different locations, about half of the profile size). Compared to the replacement situation in Fig. 5(a), CRAD requires 6 more (i.e. 10) presented devices to converge to the accuracy level of 0.9. On the other hand, the precision of CRAD achieves 0.9 with 11 different sensing locations, also 3 more locations than its counterpart requires in Fig. 5(b). We owe such performance degradation to the mixture of RSS measurements from legitimate AP and rogue AP at the receiver side in the coexistence attack scenarios.

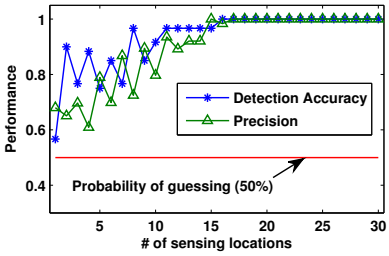


Fig. 6. The performance of CRAD under the coexistence attack model.

V. Conclusion

In this paper, we proposed CRAD, a crowdsensing based approach to detect rogue AP in any possible camouflage with non-specialized hardware. CRAD exploits the RSS measurements of crowd mobile devices to identify potential imposters. A grid-based profiling method was designed to build profile with crowdsensing collections, and a matching algorithm was presented to detect abnormal samples based on the majority voting. We conducted experiments with both a public dataset and prototype implementation. CRAD is effective in detecting rogue APs regarding detection accuracy and precision. Its performance increases with more crowd presence.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant Nos. 61379144, 61379145, 61672195, 61402513, 61501482.

References

[1] K. Sui, Y. Zhao, D. Pei, and L. Zimu, "How bad are the rogues' impact on enterprise 802.11 network performance?" in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 361–369.

[2] B. Alotaibi and K. Elleithy, "Rogue access point detection: Taxonomy, challenges, and future directions," *Wireless Personal Communications*, pp. 5021–5028, 2016.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (Mobicom)*. ACM, 2008, pp. 116–127.

[4] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2009.

[5] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM)*, 2008, pp. 1768–1776.

[6] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel & Distributed Systems*, vol. 24, no. 1, pp. 44–58, 2013.

[7] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics & Security*, vol. 7, no. 5, pp. 1638–1651, 2012.

[8] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue ap detection," *IEEE Transactions on parallel and distributed Systems*, vol. 22, no. 11, pp. 1912–1925, 2011.

[9] H. Mustafa and W. Xu, "Cetad: Detecting evil twin access point attacks in wireless hotspots," in *IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2014, pp. 238–246.

[10] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.

[11] Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, and Y. Liu, "Fbs-radar: Uncovering fake base stations at scale in the wild," in *NDSS*, 2017.

[12] T. Zhou, Z. Cai, M. Xu, and Y. Chen, "Leveraging crowd to improve data credibility for mobile crowdsensing," in *Proceedings of the 21th IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2016, pp. 561–568.

[13] J. Torres-Sospedra, R. Montoliu, A. Martínez-Usó, J. P. Avariento, T. J. Arnau, M. Benedito-Bordonau, and J. Huerta, "Ujiindoorloc: A new multi-building and multi-floor database for wlan fingerprint-based indoor localization problems," in *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. IEEE, 2014, pp. 261–270.