Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks

Yingying Chen, *Member, IEEE*, Jie Yang, *Student Member, IEEE*, Wade Trappe, *Member, IEEE*, and Richard P. Martin, *Member, IEEE*

***Abstract*—Wireless networks are vulnerable to identity-based attacks, including spoofing and Sybil attacks, which allows for many other forms of attacks on the networks. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible, because it requires key management and additional infrastructural overhead. In this paper, we propose a method for detecting both spoofing and Sybil attacks by using the same set of techniques. We first propose a generalized attack-detection model that utilizes the spatial correlation of received signal strength (RSS) inherited from wireless nodes. We further provide a theoretical analysis of our approach. We then derive the test statistics for detection of identity-based attacks by using the K-means algorithm. Our attack detector is robust when handling the situations of attackers that use different transmission power levels to attack the detection scheme. We further describe how we integrated our attack detector into a real-time indoor localization system, which can also localize the positions of the attackers. We show that the positions of the attackers can be localized using either area- or point-based localization algorithms with the same relative errors as in the normal case. We further evaluated our methods through experimentation in two real office buildings using both an IEEE 802.11 (WiFi) network and an IEEE 802.15.4 (ZigBee) network. Our results show that it is possible to detect wireless identity-based attacks with both a high detection rate and a low false-positive rate, thereby providing strong evidence of the effectiveness of the attack detector utilizing the spatial correlation of RSS and the attack localizer.**

***Index Terms*—Identity-based attack, localization, received signal strength (RSS), sensor network, spoofing attack, Sybil attack, transmission power, wireless network.**

I. Introduction

As MORE WIRELESS and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the two most harmful but easy to launch attacks: 1) *spoofing attacks* and 2) *Sybil attacks*. In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks. For instance, in an IEEE 802.11 network, it is easy for an attacker to modify its Media Access Control (MAC) address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point (AP) or an authorized client, an attacker can launch denial-of-service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

On the other hand, in Sybil attacks, a Sybil node can forge different identities to trick the network with multiple fake nodes. The Sybil attack can significantly reduce the network performance by defeating group-based voting techniques and fault-tolerant schemes (e.g., redundancy mechanisms [1], distributed storage [2], and multipath routing [3]).

Therefore, identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks. It is thus desirable to detect the presence of identity-based attacks and eliminate them from the network. The traditional approach to address identity-based attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In this paper, we take a different approach by using the physical properties associated with wireless transmissions to detect identity-based attacks. In particular, we utilize the received signal strength (RSS) measured across a set of landmarks (i.e., reference points with known locations) to perform detection of identity-based attacks. We focus on static nodes, which are common for most identity-based attacks scenarios [4]. Our scheme can detect both spoofing and Sybil attacks by using the same set of techniques and does not add any overhead to the wireless devices and sensor nodes.

We formulate a generalized attack-detection model by using statistical significance testing. We then provide theoretical analysis of exploiting the spatial correlation of the RSS inherited from wireless nodes for attack detection. In our theoretical analysis, we first derived the mathematical relationship between

Manuscript received May 28, 2009; revised August 22, 2009 and December 20, 2009; accepted February 3, 2010. Date of publication March 8, 2010; date of current version June 16, 2010. This paper was presented in part at the Fourth IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks and the Fourth IEEE International Workshop on Wireless and Sensor Networks Security. The review of this paper was coordinated by Dr. G. Cao.

Y. Chen and J. Yang are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: yingying.chen@stevens.edu; jyang@stevens.edu).

W. Trappe is with the Wireless Information Network Laboratory and the Department of Electrical and Computer Engineering, Rutgers, The State University of New Jersey, Piscataway, NJ 08854 USA (e-mail: trappe@winlab.rutgers.edu).

R. P. Martin is with the Wireless Information Network Laboratory and the Department of Computer Science, Rutgers, The State University of New Jersey, Piscataway, NJ 08854 USA (e-mail: rmartin@cs.rutgers.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2010.2044904

the distance of RSS in signal space and the node distance in physical space. We then developed the analytical expression of the detection rate, false-positive rate, and accuracy of determining whether two nodes reside at the same location based on the RSS distance in signal space. In addition, we derived the optimal threshold that can minimize the detection errors. The theoretical analysis provides both the theoretical support for detecting identity-based attacks by using the spatial correlation of RSS and the analytic results on detection effectiveness.

Furthermore, by examining the clustering effects of RSS over time in signal space, we found that the distance between the centroids of clusters derived by the K-means algorithm in signal space is a good test statistic for effective attack detection. In addition, we developed a mechanism called difference of two (DoT), which utilizes the difference of RSS between landmarks to help detect Sybil attacks launched by a Sybil node that varies its transmission power levels to trick the attack-detection scheme. Thus, our attack detector is robust to detect identity-based attacks that use different transmission power levels.

Detecting the presence of identity-based attacks in the network provides first-order information toward defending against attackers. Furthermore, learning the physical location of the attackers allows the network administrators to further exploit a wide range of defense strategies. We then explore how we can find the positions of the adversaries by integrating our attack detector into a real-time indoor localization system. Our cluster-analysis-based attack detector is not specific to any RSS-based localization algorithms and is thus general. For two kinds of algorithms, area- and point-based algorithms, we show that using the centroids of the clusters that are returned by the attack detector in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

Moreover, to evaluate the effectiveness of our attack detector, we conducted experiments by using both an IEEE 802.11 network and an IEEE 802.15.4 network in two real office building environments. In particular, we have built an indoor localization system that can localize any transmitting devices on the floor in real time. We evaluated the performance of our attack detector by using a detection rate and receiver operating characteristic (ROC) curve. We found that the performance of the attack detector is in line with the analytical results, suggesting that our attack detector is highly effective with more than 95% detection rates and less than 5% false-positive rates.

In addition, we observed that, when using the centroids of clusters returned by the attack detector in signal space, a broad family of localization algorithms achieve the similar performance as when using the averaged RSS in traditional localization attempts. In particular, for spoofing attacks, our experimental results show that the distance between the localized results of the spoofing node and the original node is directly proportional to the true distance between the two nodes, thereby providing strong evidence of the effectiveness of both our detection scheme and our approach of localizing the positions of the adversaries.

The rest of this paper is organized as follows. In Section II, we first study the feasibility and threats of identity-based attacks and their impacts. In Section III, we then formulate the detection problem of identity-based attacks, provide theoretical analysis of using the spatial correlation of RSS for attack detection, and propose our cluster-analysis-based attack detector for both spoofing and Sybil attacks. We next describe our evaluation metrics in Section IV and present our experimental methodology in Section V. We present the performance evaluation of detecting spoofing and Sybil attacks in Sections VI and VII, respectively. We introduce the real-time localization system and present how we can find the positions of the attackers in Section VIII. Section IX describes the previous research in addressing spoofing and Sybil attacks. Finally, we conclude our paper in Section X.

II. Feasibility of Attacks

In this section, we provide a brief overview of identity-based attacks and their impact to the wireless and sensor networks.

A. Spoofing Attacks

Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and utilize the identity information to launch identity-based spoofing attacks in wireless and sensor networks. For instance, in an 802.11 network, it is easy for a wireless device to acquire a valid MAC address and masquerade as another device. The IEEE 802.11 protocol suite provides insufficient identity verification during message exchange, including most control and management frames. Therefore, the adversary can utilize this weakness and request various services as if it were another user. Identity-based spoofing attacks are a serious threat in the network, because they represent a form of identity compromise and can facilitate a series of traffic injection attacks, including spoofing-based DoS attacks.

For instance, an adversary can launch a deauthetication attack. After a client chooses an AP for future communication, it must authenticate itself to the AP before the communication session starts. Both the client and the AP are allowed to explicitly request for deauthentication to void the existing authentication relationship with each other. Unfortunately, this deauthentication message is not authenticated. Therefore, an attacker can spoof this deauthentication message, either on behalf of the client or on behalf of the AP [5], [6]. The adversary can persistently repeat this attack and completely prevent the client from transmitting or receiving.

Furthermore, an attacker can utilize identity spoofing and launch the rogue AP attack against the wireless network. In the rogue AP attack, the adversary first sets up a rogue AP with the same MAC address and service set identifier as the legitimate AP but with a stronger signal. When a station enters the coverage of the rogue AP, the default network configuration will make the station automatically associate with the rogue AP, which has a stronger signal. Then, the adversary can take actions to influence the communication. For example, it can direct fake traffic to the associated station or drop the requests made by the station. Aside from the basic packet-flooding attacks, the adversary can make use of identity spoofing to perform

more sophisticated flooding attacks on APs, such as probe request, authentication request, and association request flooding attacks [7].

B. Sybil Attacks

The term *Sybil attack* was first introduced in [8] to denote an attack where the attacker, i.e., a Sybil node, tries to forge multiple identities in the context of peer-to-peer distributed systems. Sybil attacks are particularly easy to launch in wireless sensor networks where the communication medium is open and broadcast. By broadcasting messages with multiple identifications, a Sybil node can rig the vote on group-based decisions and also severely disrupt network middleware services [9].

Furthermore, by using a single node to present multiple identities in the network, the Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as redundancy mechanisms [1], distributed storage [2], dispersity and multipath routing [3], and topology maintenance [10]. The Sybil attack can defeat the redundancy mechanisms, storage partitions, and routing algorithms by making the mechanisms believe that they are using multiple nodes but are, in fact, using a single Sybil node.

Therefore, the identity-based attacks, both spoofing and Sybil attacks, will significantly impact the network performance. The conventional approaches to address identity-based attacks use authentication. However, the application of authentication requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply authentication because of its infrastructural, computational, and management overhead. Furthermore, cryptographic methods are susceptible to node compromise, which is a serious concern, because most wireless nodes are easily accessible, allowing their memory to be easily scanned.

Thus, it is desirable to use properties that do not require overheads and changes on nodes and cannot be undermined even when nodes are compromised. We propose to use RSS, a property that is associated with the transmission and reception of communication (and, hence, does not rely on cryptography), as the basis for detecting identity-based attacks. Employing RSS as a means of detecting spoofing and Sybil attacks will not require any additional cost to the wireless devices themselves—they will merely use their existing communication methods, whereas the wireless network will use a collection of APs to monitor RSS for the potential of identity-based attacks. Our proposed techniques will handle the problem of the unreliable time-varying nature of RSS [11], [12]. These techniques will also address the issues when an attacker varies its transmission power to launch attacks and trick the system.

III. Attack Detector

In this section, we present our attack detector. We first formulate the attack-detection problem using significance testing. We then provide a theoretical analysis on our RSS-based attack detection. We next develop the test statistics for attack detection and present the detection philosophy for spoofing and Sybil attacks.

A. Formulation of Attack Detection

RSS is widely available in deployed wireless communication networks, and its values are closely correlated with location in physical space. In addition, RSS is a common physical property used by a widely diverse set of localization algorithms [13]–[16]. In spite of its several-meter-level localization accuracy, using RSS is an attractive approach, because it can reuse the existing wireless infrastructure, and it is sufficient to meet the accuracy requirement of most applications. For example, during health care monitoring, a doctor may only need to know in which room the tracked patient resides. We thus derive an attack detector for identity-based attacks by utilizing properties of the RSS.

We formulate attack detection as a statistical significance testing problem, where the null hypothesis is

$$\mathcal{H}_0 : \text{normal (no attack)}.$$

In significance testing, a test statistic $\mathbf{T}$ is used to evaluate whether observed data belong to the null hypothesis. For a particular significance level α (defined as the probability of rejecting the hypothesis if it is true), there is a corresponding *acceptance region* Ω such that we declare the null hypothesis valid if an observed value of the test statistic $\mathbf{T^{obs}} \in \Omega$ and reject the null hypothesis if $\mathbf{T^{obs}} \notin \Omega$ (i.e., declare that an attack is present if $\mathbf{T^{obs}} \in \Omega^c$, where Ω^c is the *critical region* of the test). In our attack-detection problem, the region Ω and decision rule are specified according to the form of the detection statistic $\mathbf{T}$ (e.g., when using distance in signal strength space for $\mathbf{T}$, the decision rule is compared with a threshold), and rejection of the null hypothesis corresponds to declaring the presence of an attack.

B. Theoretical Analysis of the Spatial Correlation of RSS

Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks [17]. The RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

According to the propagation model, the RSS at a landmark from a wireless node is given by [18]

$$P(d_i)\ [\text{dBm}] = P_i(d_0)\ [\text{dBm}] - 10\gamma \log\left(\frac{d_i}{d_0}\right) + S_i \quad (1)$$

where i is the ith wireless node, $P_i(d_0)$ represents the transmitting power of node i at the reference distance d_0, d_i is the distance between the wireless node and the landmark, γ is the path loss exponent, and S_i is the shadow fading that follows zero-mean Gaussian distribution with δ standard deviation [18], [19]. We assume that the wireless nodes have the same transmission power. In Sections VI-B and VII-B, we will discuss how we

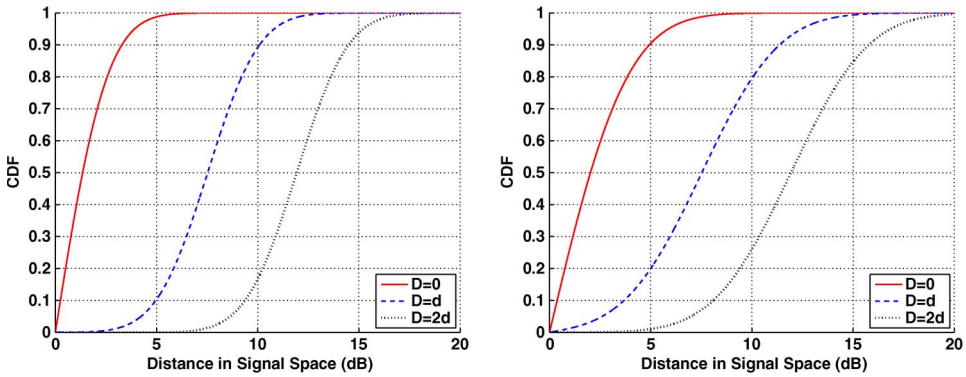


Fig. 1. CDF of the distance in signal space when the distance between two nodes are 0, d, and $2d$, respectively. The distance between the landmark and the closer node is d. (a) $\delta = 2$ dB. (b) $\delta = 3$ dB.

can detect identity-based attacks when attackers use different transmission power levels. Thus, the RSS distance between two nodes in signal space at the landmark is given by

$$\Delta P = 10\gamma \log\left(\frac{d_2}{d_1}\right) + \Delta S \tag{2}$$

where ΔS follows zero-mean Gaussian distribution with $\delta/\sqrt{2}$ standard deviation.

We depict the cumulative distribution function (CDF) of the RSS distance in signal space in Fig. 1 when the distance between two nodes are 0, d, and $2d$, respectively, whereas the distance from the landmark to the closer node is d. The path loss exponent is set to 2.5. In Fig. 1(a), the standard deviation of shadowing is 2 dB, whereas it is 3 dB for Fig. 1(b). We found that the curves shift to the right with the increasing RSS distance when the physical distance between two nodes increases. It is obvious that, when two nodes are at the same location, the RSS distance is small, i.e., around 5 dB, which is most likely caused by the variation of RSS under different σ.

Based on the key observation of the strong spatial correlation of RSS, it is thus important to analyze how we can derive a threshold under which the RSS distance can effectively be exploited to perform attack detection with low false positives. According to (2), when the two wireless nodes are at the same location (i.e., $d_1 = d_2$), the RSS distance in signal space follows a normal distribution with zero mean and $\delta/\sqrt{2}$ standard deviation, whereas the distance follows a normal distribution with $10\gamma \log(d_2/d_1)$ mean and $\delta/\sqrt{2}$ standard deviation if these two nodes are at different locations. The probability density functions (PDFs) of the distance under these two different conditions can be represented as follows:

$$f_{\Delta P}(p \mid \text{same location}) = \frac{1}{\sqrt{\pi}\delta} e^{\frac{-p^2}{\delta^2}} \tag{3}$$

$$f_{\Delta P}(p \mid \text{different location}) = \frac{1}{\sqrt{\pi}\delta} e^{\frac{-\left(p-10\gamma\log\left(\frac{d_2}{d_1}\right)\right)^2}{\delta^2}}. \tag{4}$$

Fig. 2 depicts these two PDFs. The left side of the figure $f_{\Delta P}(p \mid \text{same location})$ describes the RSS distance when two wireless nodes are at the same location, whereas the right side

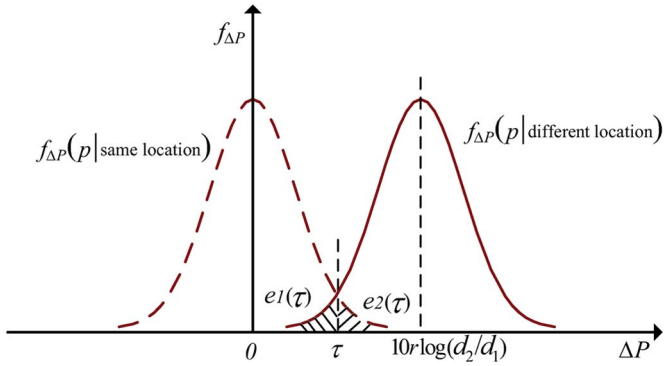


Fig. 2. PDFs of RSS distance in signal space when two wireless nodes are at the same location and at different locations, respectively.

of the figure $f_{\Delta P}(p \mid \text{different location})$ corresponds to the RSS distance when two nodes are at different locations.

Given the threshold τ in the signal space, the probability that we can determine the two nodes are at different locations in 1-D physical space (i.e., detection rate) based on the RSS distance distribution is given by

$$DR = Prob(\Delta P > \tau \mid \text{different locations}) = 1 - \phi\left(\frac{\tau - 10\gamma\log\left(\frac{d_2}{d_1}\right)}{\frac{\sigma}{\sqrt{2}}}\right) \tag{5}$$

and the corresponding false-positive rate is

$$FPR = Prob(\Delta P > \tau \mid \text{same locations}) = 1 - \phi\left(\frac{\tau}{\frac{\sigma}{\sqrt{2}}}\right) \tag{6}$$

where $\phi(\cdot)$ is the CDF of standard normal distribution. In addition, the accuracy of classifying whether these two nodes are at different locations is given by

$$Accuracy = \frac{\phi\left(\frac{\tau}{\frac{\sigma}{\sqrt{2}}}\right) + 1 - \phi\left(\frac{\tau - 10\gamma\log\left(\frac{d_2}{d_1}\right)}{\frac{\sigma}{\sqrt{2}}}\right)}{2}. \tag{7}$$

To analyze the feasibility of using RSS distance in signal space to diagnose whether two nodes are at different locations

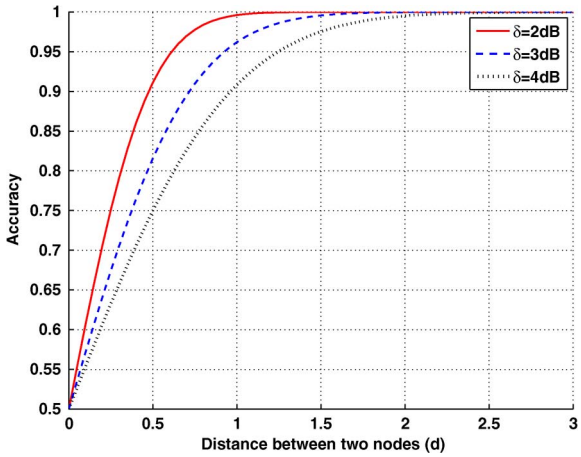


Fig. 3. Detection accuracy for the optimal threshold $\tau = 5\gamma \log(d_2/d_1)$ when the standard deviation of shadowing is 2, 3, and 4 dB, respectively. The path loss exponent is 2.5.

for attack detection, our objective is to select the value of threshold τ that minimizes the average decision errors. In Fig. 2, the probability of erroneously classifying the RSS distance from the same physical location as the RSS distance from different locations is

$$e_1(\tau) = \int_{-\infty}^{\tau} f_{\Delta P}(p \mid \text{different location})\, ds. \tag{8}$$

This is indicated as the shadowing area under the curve of $f_{\Delta P}(p \mid \text{different location})$ to the left of the threshold. Similarly, the probability of erroneously classifying the RSS distance from different locations as the RSS distance from the same location is

$$e_2(\tau) = \int_{\tau}^{+\infty} f_{\Delta P}(p \mid \text{same location})\, ds \tag{9}$$

which is indicated as the shadowing area under the curve of $f_{\Delta P}(p \mid \text{same location})$ to the right of τ. Then, the overall probability of classification error can be obtained as

$$e(\tau) = e_1(\tau) + e_2(\tau). \tag{10}$$

To find the threshold value for which this error is minimal requires differentiating $e(\tau)$ with respect to τ and equating the result to 0, i.e.,

$$f_{\Delta P}(\tau \mid \text{same location}) - f_{\Delta P}(\tau \mid \text{different location}) = 0. \tag{11}$$

This equation is solved for τ to find the optimum threshold. Substituting (3) and (4) into the aforementioned equation yields the optimum threshold, i.e.,

$$\tau = 5\gamma \log\left(\frac{d_2}{d_1}\right). \tag{12}$$

Fig. 3 presents the numerical results of detection accuracy under the optimal threshold $\tau = 5\gamma \log(d_2/d_1)$ when the standard deviation of shadowing is 2, 3, and 4 dB, respectively. In the figure, we observed that the farther away the two nodes are separated, the better the accuracy we have. In addition, we obtained better accuracy with lower standard deviation σ of shadowing. It is encouraging that, under the theoretical analysis, even with a single landmark in 1-D physical space, our approach of utilizing the RSS distance can obtain an accuracy of more than 90% when the two wireless nodes are separated by the distance of $0.5d$ and beyond. When additional landmarks are employed to calculate RSS distance in signal space, we expect to obtain a better accuracy.

We next extend our theoretical model in the 1-D physical space to the 2-D physical space. Suppose that there are n landmarks that monitor the RSS of the wireless nodes. Each RSS vector $\mathbf{s} = \{s_1, s_2, \ldots, s_n\}$ corresponds to a point in an n-dimensional signal space [15]. Then, the RSS distance in n-dimensional signal space is determined by

$$\Delta D = \sqrt{\Delta P_1^2 + \cdots + \Delta P_n^2} \tag{13}$$

where ΔP_i, with $i = 1, 2, \ldots, n$, is the RSS distance at the ith landmark and is given by (2).

Subject to (3), we know that, when these two wireless nodes are at the same location, the distance $(2/\delta^2)\Delta D^2$ in n-dimension signal space follows a chi-square distribution with n degree of freedom [20], i.e.,

$$\frac{2}{\delta^2}\Delta D^2 = \sum_{i=1}^{n} \left(\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}p_i^2}\right)^2 \sim \chi^2_{n,0}. \tag{14}$$

However, when these two wireless nodes are at different locations, $(2/\delta^2)\Delta D^2$ becomes a noncentral chi-square distribution with a noncentrality parameter λ, i.e.,

$$\frac{2}{\delta^2}\Delta D^2 = \sum_{i=1}^{n} \left(\frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}\left(p_i - 10\gamma \log\left(\frac{d_{i2}}{d_{i1}}\right)^2\right)^2}\right)^2 \sim \chi^2_{n,\lambda} \tag{15}$$

where d_{i1} and d_{i2} are the distances from two wireless nodes to the ith landmark, and

$$\lambda = \sum_{i=1}^{n} \left(10\gamma \log\left(\frac{d_{i2}}{d_{i1}}\right)^2\right). \tag{16}$$

Given the threshold τ, the probability that we can determine the two nodes are at different locations in a 2-D physical space with n landmarks (i.e., detection rate) is given by

$$DR = Prob(\Delta D > \tau \mid \text{different locations}) = 1 - \mathcal{F}_{\chi^2_{n,\lambda}}\left(\frac{2}{\delta^2}\tau^2\right) \tag{17}$$

and the corresponding false-positive rate is

$$FPR = Prob(\Delta D > \tau \mid \text{same locations}) = 1 - \mathcal{F}_{\chi^2_{n,0}}\left(\frac{2}{\delta^2}\tau^2\right) \tag{18}$$

where $\mathcal{F}_X(\cdot)$ is the CDF of the random variable X.

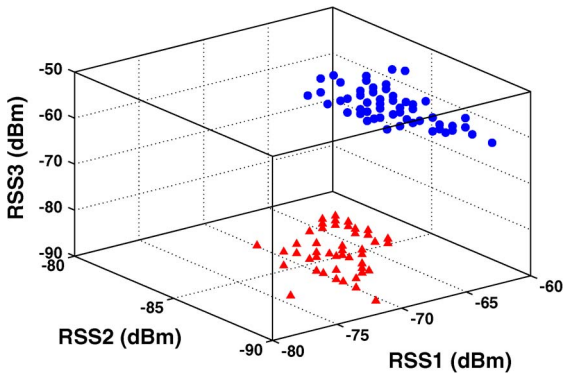


Fig. 4. RSS readings from two physical locations.

C. Test Statistics for Detection of Identity-Based Attacks

The aforementioned analysis provides the theoretical support of using the spatial correlation in RSS inherited from wireless nodes to perform attack detection. It also showed that the RSS readings from a wireless node over time fluctuate under different σ and should cluster together. In particular, the RSS readings from the same physical location over time will belong to the same cluster points in the n-dimensional signal space, whereas the RSS readings from different locations over time should form different clusters in signal space, as shown in Fig. 4, which presents RSS reading vectors of three landmarks (i.e., $n = 3$) from two different physical locations. This observation suggests that we can conduct cluster analysis on top of RSS readings to find out the distance in signal space in practice. Furthermore, we can detect the identity-based attacks based on the observed RSS distance between clusters.

We explore the K-means algorithm, which is one of the most popular iterative descent clustering methods [21]. The squared Euclidean distance is chosen as the dissimilarity measure. If there are M RSS sample readings for a node, the K-means clustering algorithm partitions M sample points into K disjoint subsets S_j with M_j sample points to minimize the sum-of-squares criterion. We have

$$J_{\min} = \sum_{j=1}^{K} \sum_{\mathbf{s_m} \in S_j} \|\mathbf{s_m} - \mu_{\mathbf{j}}\|^2 \tag{19}$$

where $\mathbf{s_m}$ is an RSS vector that represents the mth sample point, and $\mu_{\mathbf{j}}$ is the geometric centroid of the sample points for S_j in signal space. We further choose the distance between two centroids as the test statistic $\mathbf{T}$ for identity-based attack detection. We have

$$D_c = \|\mu_{\mathbf{i}} - \mu_{\mathbf{j}}\| \tag{20}$$

with $i, j \in \{1, 2, \ldots, K\}$.

D. Detection Philosophy

1) Detecting Spoofing Attacks: Under normal conditions, when examining the RSS stream from a node identity, the distance between the centroids from the K-means cluster analysis in signal space should be close to each other, because there is only one cluster from a single physical location. However, under a spoofing attack, there is more than one node at different physical locations, which claim the same node identity. As a result, when examining the RSS stream over time from a node identity, the RSS sample readings from the attacked node (i.e., the original node) will be mixed with RSS readings from at least one different location. Thus, more than one clusters will be formed in the signal space, and the distance between the centroids is larger (i.e., $\mathbf{T^{obs}} > \tau$) as the centroids are derived from the different RSS clusters associated with different locations (the original node plus spoofing nodes) in physical space. When the RSS reading vectors, as shown in Fig. 4, is from one wireless node identity, we observed that two RSS clusters are formed, and the distance between two centroids is large. This result clearly indicates that the RSS readings come from two different physical locations and thus declares the presence of a spoofing attack. Furthermore, based on our analysis in Section III-B, the farther the attacker is from the original node, the more the likelihood that their RSS patterns significantly differ, and the higher the accuracy that the detector can achieve.

2) Detecting Sybil Attacks: Similarly, the basic idea behind using the K-means cluster analysis to detect Sybil attacks relies on the RSS correlation in the physical locations of nodes. When examining the RSS readings from two nodes with different identities over time, we can apply the K-means cluster analysis to the *mixture* of these two RSS streams. Under normal conditions without a Sybil attack, the observed value of the test statistic $\mathbf{T^{obs}}$ (i.e., D_c^{obs}) should be large, because there are two different RSS clusters from two physical locations, whereas when a Sybil attack is present, the $\mathbf{T^{obs}}$ is small and satisfies $\mathbf{T^{obs}} < \tau$, because the RSS readings originated in one physical location (i.e., the location of a Sybil node), and thus, there is only one cluster in the signal space.

IV. Metrics

In this section, we present our metrics for evaluating the performance of our attack detector by using spatial correlation of RSS based on the K-means cluster analysis in real experiments.

Detection Rate and False-Positive Rate: An identity-based attack will cause the significance test to reject $\mathcal{H}_0$. We are thus interested in the statistical characterization of the attack-detection attempts over all the possible attacks on the floor. The detection rate is defined as the percentage of attack attempts that are determined to be under attack. Note that, when the attack is present, the detection rate corresponds to the probability of detection P_d, whereas under normal (nonattack) conditions, it corresponds to the probability of declaring a false positive P_{fa}. The detection rate and false-positive rate vary under different thresholds.

ROC Curve: To evaluate an attack detection scheme, we want to study both the false-positive rate P_{fa} and the probability of detection P_d. The ROC curve is a plot of attack detection accuracy compared to the false-positive rate. It can be obtained by varying the detection thresholds. The ROC curve provides a direct means of measuring the tradeoff between false positives and correct detections.

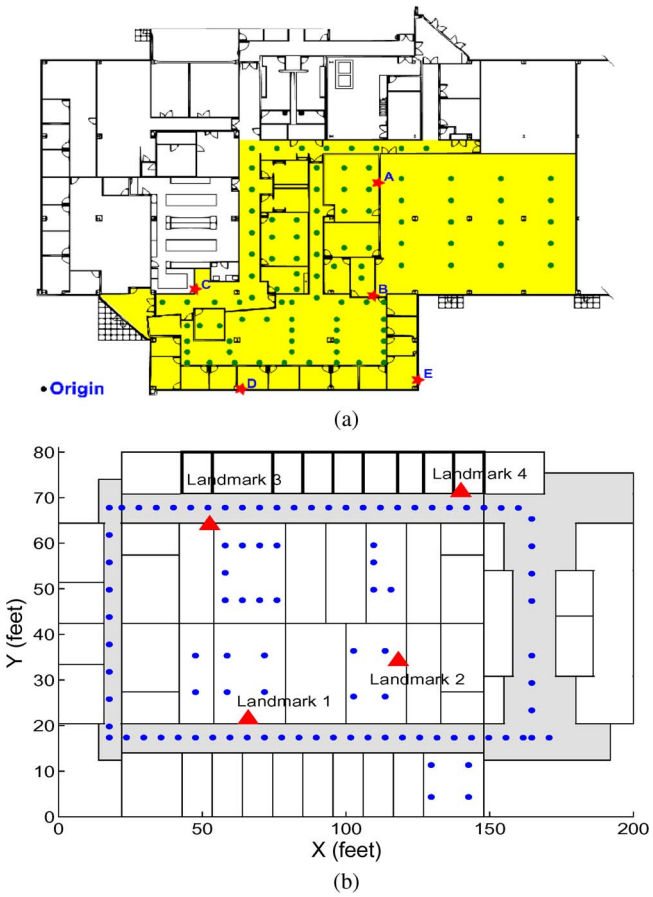


Fig. 5. Landmark setups and testing locations in two networks within two office buildings. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

Distance Between Wireless Nodes: In a spoofing attack, when a spoofing node is close to an original node, the resulting test statistic D_c^{obs} will not be large and may affect the decision of attack detection, whereas in a Sybil attack, when two wireless nodes are close to each other, a small test statistic D_c^{obs} will be obtained. This condition may mislead our attack detector to determine the presence of a Sybil attack. Hence, we are interested in studying how the distance between two nodes affects the performance of our attack detector.

V. Experimental Methodology

To evaluate the effectiveness of our mechanisms in detecting identity-based attacks, we conducted experiments using two networks: 1) an IEEE 802.11 (WiFi) network at the Wireless Information Network Laboratory (WINLAB) and 2) an IEEE 802.15.4 (ZigBee) network in the Department of Computer Science, Rutgers, The State University of New Jersey. The size of these two floors are 219 $\times$ 169 ft and 200 $\times$ 80 ft, respectively. Fig. 5(a) shows the 802.11 network, with five landmarks shown in red stars, which are deployed to maximize signal strength coverage in the yellow-shaded experimental area. Meanwhile, the 802.15.4 network is presented in Fig. 5(b), with four landmarks distributed in a squared setup to achieve optimal landmark placement [17], as shown in red triangles.

The small dots in floor maps are the locations used for testing. For the 802.11 network, there are 101 locations, and we collected 300 packet-level RSS samples at each location, whereas for the 802.15.4 network, there are 94 locations, and 300 packet-level RSS samples are collected at each location.

In addition, we built a real-time localization system to localize the positions of attackers. We use the leave-one-out method in localization algorithms, which means that we choose one location as the testing node, whereas the rest of the locations are chosen as training data. For the 802.11 network, the size of the training data is 100 locations, whereas for the 802.15.4 network, the size of the training data is 73 locations. The detailed description of our localization system is presented in Section VIII.

To test our approach's ability to detect identity-based attacks, for spoofing attacks, we randomly chose a point pair on the floor and treated one point as the position of the original node and the other point as the position of the spoofing node, whereas for Sybil attacks, we randomly chose a location, split the collected RSS samples, and applied with multiple node identities.

We ran the identity-based attack detection test through all the possible combinations of point pairs on the floor by using all the testing locations in both networks. There are a total of 5050 pairs for the 802.11 network and 4371 pairs for the 802.15.4 network. The experimental results will be presented in the following sections for the attack detector and the attack localizer.

VI. Experimental Evaluation of Detecting Spoofing Attacks

In this section, we focus on detecting spoofing attacks. We first describe how we can determine the threshold of test statistics and detect attacks when adversaries use different transmission power levels. The experimental results are then presented to evaluate the effectiveness of detecting spoofing attacks.

A. Determining the Threshold of Test Statistics

Based on the analysis in Section III-B, it is important to choose the appropriate threshold τ, which will allow the attack detector to be robust to false detections. The thresholds define the critical region for the significance testing. In our experiments, the threshold is obtained through empirical training of the K-means algorithm. Fig. 6 shows the results of the CDF of the D_c in signal space for both the 802.11 and 802.15.4 networks. We found that the curve of D_c greatly shifted to the right under spoofing attacks, which is in line with our analytical results in Section III-B, thereby suggesting that using D_c as a test statistic is an effective way of detecting spoofing attacks. We will examine the performance of the attack detector under various τ.

B. Detecting Attacks Using Different Transmission Power Levels

If an attacker sends packets at a transmission power level that is different from the original node with the same identity, there will be two distinct RSS clusters in signal space. The

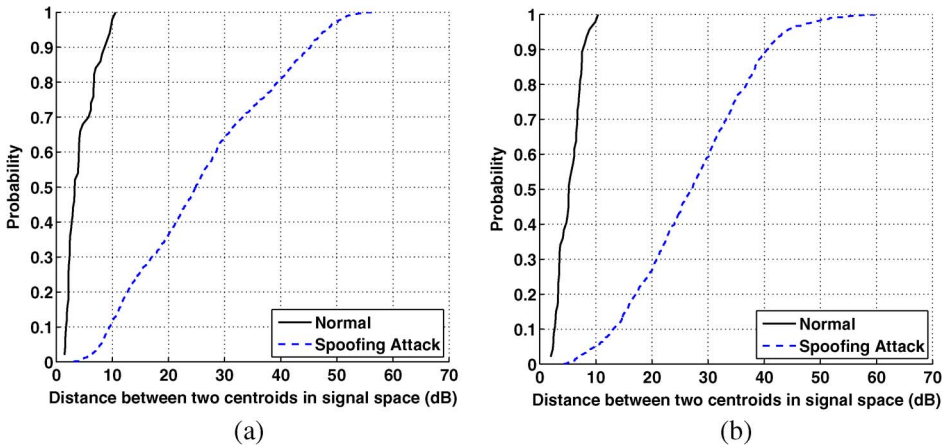


Fig. 6. Spoofing attack detection: CDF of the test statistic D_c in the signal space. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

TABLE I
SPOOFING ATTACK DETECTION: DETECTION RATE AND FALSE-POSITIVE RATE IN TWO NETWORKS

Network, Threshold	Detection Rate	False Positive Rate
802.11, τ = 8.2dB	0.9653	0.0990
802.11, τ = 9.1dB	0.9500	0.0495
802.11, τ = 10.6dB	0.9263	0
802.15.4, τ = 8.2dB	0.9806	0.0957
802.15.4, τ = 10dB	0.9664	0.0426
802.15.4, τ = 11dB	0.9577	0

spoofing attack will thus be detected based on the test statistics of D_c, obtained from the RSS clusters. Therefore, our K-means detector is robust when an attacker launches a spoofing attack from different transmission power levels.

C. Detection Results

In this section, we present the evaluation of the effectiveness of the attack detector in detecting spoofing attacks.

1) Effectiveness of Attack Detector: Table I presents the detection rate and false-positive rate for both the 802.11 and 802.15.4 networks under different threshold settings. The corresponding ROC curves are displayed in Fig. 7. The results are encouraging, showing that for false-positive rates less than 5%, the detection rates are more than 95%. Even when the false-positive rate goes to zero, the detection rate is still more than 92% for both the 802.11 and 802.15.4 networks.

Table II presents the detection rate and false-positive rate for the 802.11 network when the spoofing attacker varies its transmission power level to launch attacks. In our experiments, the attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB of transmission power. Compared with Table I, Table II shows that we can achieve a higher detection rate when the attacker uses different transmission power levels. Thus, our attack detector can effectively detect the spoofing attacks that are launched by using different transmission power levels.

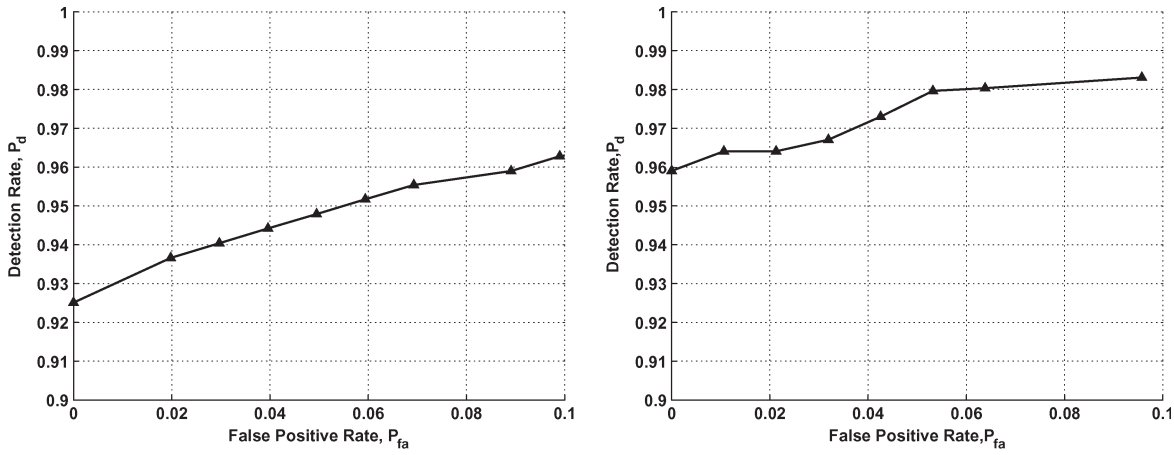
2) Impact of the Distance Between the Spoofing Node and the Original Node: Our analytical results in Section III-B show that the distance between the spoofing node and the original node will affect the detection accuracy. We further study how likely a spoofing node can be detected by our attack detector when it is at varying distances from the original node in physical space. Fig. 8 presents the detection rate as a function of the distance between the spoofing node P_{spoof} and the original node P_{org}. We found that the farther away P_{spoof} is from P_{org}, the higher the detection rate becomes. For the 802.11 network, the detection rate goes to more than 90% when P_{spoof} is about 23 ft away from P_{org} under τ equal to 8 dB. On the other hand, for the 802.15.4 network, the detection rate is more than 90% when the distance between P_{spoof} and P_{org} is about 20 ft by setting threshold τ to 9 dB. This result is in line with the average localization-estimation errors using RSS [15], which are about 15 ft. When the nodes are less than 15 ft apart, they have a high likelihood of generating similar RSS readings, and thus, the spoofing-detection rate falls below 90% but is still greater than 55%. However, when P_{spoof} moves closer to P_{org}, the attacker also increases the probability to expose itself. The detection rate goes to 100% when the spoofing node is about 45–50 ft away from the original node.

VII. EXPERIMENTAL EVALUATION OF DETECTING SYBIL ATTACKS

In this section, we first describe how we can determine the threshold of test statistics for detecting Sybil attacks and then develop the DoT mechanism to handle attacks launched by Sybil nodes that use different transmission power levels to create different identities. Finally, the experimental results are presented to evaluate the effectiveness of detecting Sybil attacks that use our attack detector.

A. Determining the Threshold of Test Statistics

Similar to detecting spoofing attacks, the thresholds define the critical region for the significance testing. In detecting Sybil attacks, we show how we determine the thresholds through empirical training for our attack detector. During the offline phase, we collected the RSS readings across a set of locations over the experimental area and obtained the distance between two centroids in signal space for each node. We then use the distribution of the training information to determine the



(a) (b)

Fig. 7. Spoofing-attack detection: ROC curves over all the testing points across the experimental floor. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

TABLE II
SPOOFING-ATTACK DETECTION WHEN THE ATTACKER VARIES ITS TRANSMISSION POWER LEVEL: DETECTION RATE AND FALSE-POSITIVE RATE WHEN THE ATTACKER USES 10-dB TRANSMISSION POWER LEVEL, WHEREAS THE ORIGINAL NODE USES 15 dB

Network, Threshold	Detection Rate	False Positive Rate
802.11, τ = 8.2dB	0.9838	0.0990
802.11, τ = 9.1dB	0.9756	0.0495
802.11, τ = 10.6dB	0.9630	0

threshold τ. At runtime, based on the RSS sample readings for each node pair (i.e., the mixture of two RSS streams from different identities), we can calculate the observed value D_c^{obs}. Our condition for declaring the presence of a Sybil attack is

$$D_c^{\text{obs}} < \tau. \tag{21}$$

Fig. 9 presents the CDF of the D_c in signal space for both the 802.11 and 802.15.4 networks. We found that the value of D_c is small under Sybil attacks, whereas the value of D_c is large under normal situations. This observation clearly indicates that using D_c as a test statistic is effective for detecting Sybil attacks.

B. DoT Mechanism

An adversary may vary the transmission power levels to create different identities to trick the system. In our analysis, different signal strength clusters will then be formed in the signal space due to different transmission power levels used, although they are from the same physical location.

We examine the pass loss part of the signal propagation that models the received power as a function of the distance to the landmark. We have

$$P(d)\ [\text{dBm}] = P(d_0)\ [\text{dBm}] - 10\gamma \log\left(\frac{d}{d_0}\right) \tag{22}$$

where $P(d_0)$ represents the transmitting power of a node at the reference distance d_0, d is the distance between the transmitting node and the landmark, and γ is the path-loss exponent. Furthermore, we can express the difference of the received power between two landmarks i and j as

$$P_i(d) - P_j(d) = 10\gamma_i \log\left(\frac{d_i}{d_0}\right) - 10\gamma_j \log\left(\frac{d_j}{d_0}\right). \tag{23}$$

Based on (23), we found that the difference of the corresponding received power between two different landmarks is independent of the transmission power. Hence, when a Sybil node that resides at a physical location varies its transmission power to create different identities, the difference of the RSS readings between two different landmarks from forged identities is a constant, because the RSS readings are obtained from a single physical location.

We thus developed the DoT mechanism, which utilizes the difference of the centroid vectors in signal space obtained from cluster analysis and further applies the difference on the obtained difference of the centroids to detect Sybil attacks that are launched by using different power levels. We use an example to illustrate how DoT helps detect the presence of a Sybil attack. When there are four landmarks deployed in the area of interest, we study the input RSS streams from two node identities and denote the two centroid vectors that are returned from the K-means algorithm as $\mu_{\mathbf{1}} = \{\mu_1^1, \mu_1^2, \mu_1^3, \mu_1^4\}$ and $\mu_{\mathbf{2}} = \{\mu_2^1, \mu_2^2, \mu_2^3, \mu_2^4\}$. DoT then calculates the difference of the difference between the corresponding centroid components from landmark 1 to the others as follows:

$$\begin{cases} e_{12} = \left(\mu_1^1 - \mu_1^2\right) - \left(\mu_2^1 - \mu_2^2\right) \\ e_{13} = \left(\mu_1^1 - \mu_1^3\right) - \left(\mu_2^1 - \mu_2^3\right) \\ e_{14} = \left(\mu_1^1 - \mu_1^4\right) - \left(\mu_2^1 - \mu_2^4\right). \end{cases} \tag{24}$$

Due to random noise, environmental bias, and multipath effects, the difference e fluctuates around zero. We define a confidence level α. Assuming that the centroid from each landmark is independent, when $\prod_{i\neq j, i, j=1}^{K} e_{ij} < 1 - \alpha$, with $K = \binom{N}{2}$, DoT concludes the presence of a Sybil attack, and the two node identities under study is, in fact, one physical node. Empirically, we found that choosing three independent equations out of K is enough to perform attack detection.

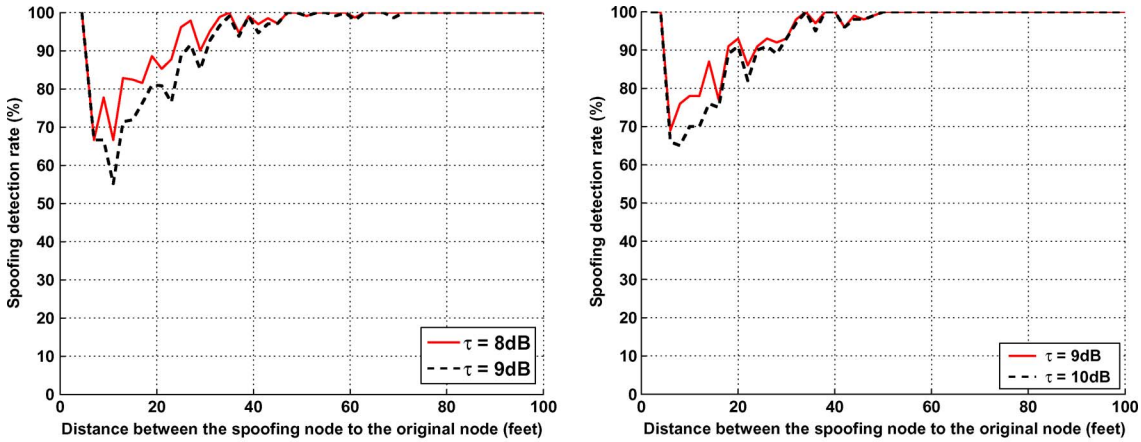


Fig. 8. Spoofing-attack detection: Detection rate as a function of the distance between the spoofing and original nodes. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

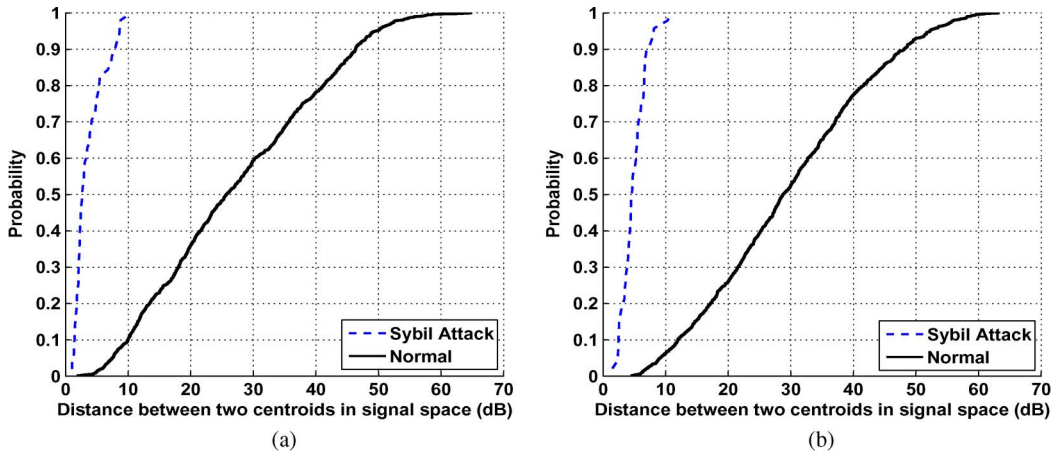


Fig. 9. Sybil-attack detection: CDF of the test statistic D_c in the signal space. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

TABLE III
SYBIL-ATTACK DETECTION: DETECTION RATE AND FALSE-POSITIVE RATE IN TWO NETWORKS

Network, Threshold	Detection Rate	False Positive Rate
802.11, τ = 10.6dB	1.0000	0.0736
802.11, τ = 9.1dB	0.9505	0.0485
802.11, τ = 8.2dB	0.9010	0.0346
802.15.4, τ = 10.9dB	1.0000	0.0409
802.15.4, τ = 9.1dB	0.9574	0.0269
802.15.4, τ = 7.9dB	0.9043	0.0173

C. Detection Results

In this section, we present the evaluation of the effectiveness of the attack detector in detecting Sybil attacks.

1) Effectiveness of Attack Detector: Table III presents the detection rate and false-positive rate for both the 802.11 and 802.15.4 networks under different threshold (τ) settings. The corresponding ROC curves are displayed in Fig. 10. We found that the attack detector can achieve a detection rate of more than 95% with less than a 10% false-positive rate. Even when the detection rate reaches 100%, the false-positive rate is only 7.4% for the 802.11 network and 4.1% for the 802.15.4 network, respectively. In addition, in Table III, we observed that the similar thresholds are achieved for both networks under detection rates of 90%, 95%, and 100%. These results indicate that our attack detector is generic across different networks and is highly effective in performing attack detection.

2) Evaluation of DoT: Fig. 11 presents the ROC curve by using DoT under the situation that an adversary varies the transmission power level from 10 dB to 15 dB to launch a Sybil attack. We observed that DoT can achieve a 100% detection rate when the corresponding false-positive rate is about 9.5%. This result is encouraging, because it shows that our attack-detection approach is robust to detect adversaries that use different transmission power levels to launch Sybil attacks.

3) Impact of Distance Between Wireless Nodes: We further study how the Sybil attack detection rate and the false-positive rate are affected by the distance between two wireless nodes in a network. We define a distance threshold $D_{\min}$, which is the minimum distance between two nodes within one experimental setting. Fig. 12 shows the ROC curves under different thresholds of $D_{\min}$ for both the 802.11 and 802.15.4 networks. We note that each ROC curve is generated by using those distances between two nodes larger than the corresponding $D_{\min}$ in an

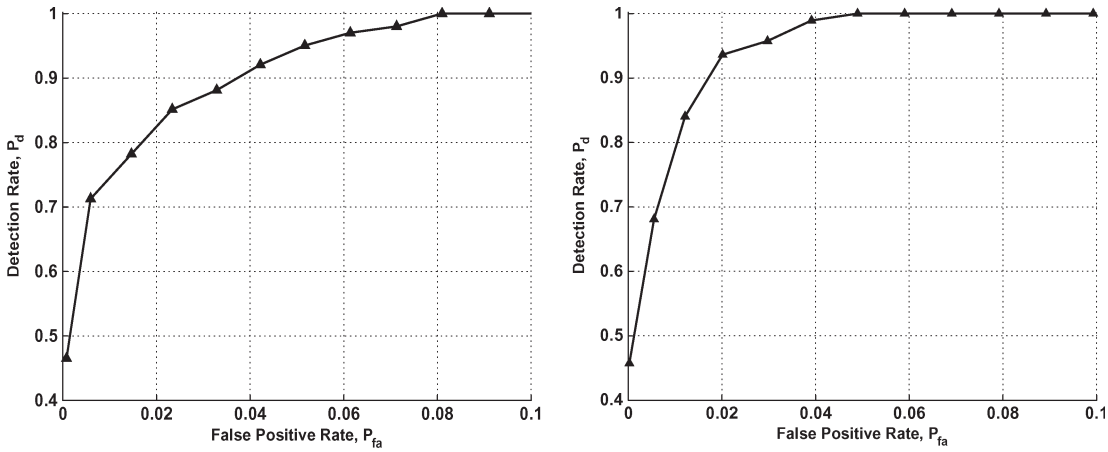


Fig. 10. Sybil-attack detection. ROC curves over all the testing points across the experimental floor: (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

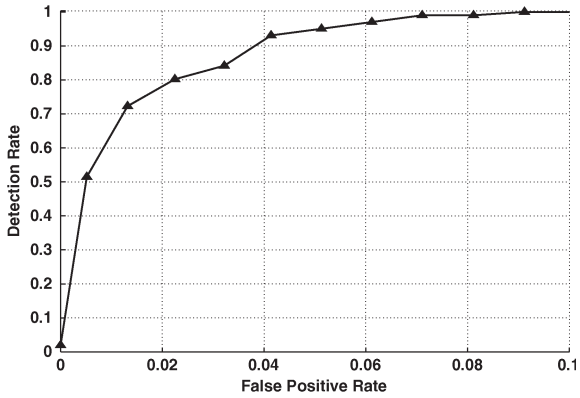


Fig. 11. DoT: ROC curve when an adversary varies transmission power levels to launch a Sybil attack.

experimental setting. We found that the ROC curves shift to the upper left when we increase the threshold $D_{\min}$. This result indicates that the farther away two nodes are from each other, the higher the detection rate, and the lower the false-positive rate achieved.

If two wireless nodes are close to each other, the resulting test statistic D_c^{obs} will be small and may be less than the threshold (i.e., $D_c^{\text{obs}} < \tau$). Consequently, the attack detector will claim a false positive (i.e., declaring the presence of a Sybil attack). Thus, we further examine how likely the false-positive rate of our detector can be reduced by varying the node distance threshold $D_{\min}$. Fig. 13 presents the false-positive rate as a function of $D_{\min}$ under different detection rates for both the 802.11 and 802.15.4 networks. First, the curves of false-positive rate show that a higher detection rate usually results in a higher false-positive rate, which is in line with our observation when using ROC curves. Second, the results indicate that the false-positive rate decreases as the $D_{\min}$ increases. For instance, by examining the curve under a detection rate of 95%, the false-positive rate decreases from 3.66% to 0.85% in the 802.11 network and from 2.53% to 0.49% in the 802.15.4 network, respectively, when $D_{\min}$ increases from 10 ft to 30 ft. In addition, we observed that the detector can achieve a 100% detection rate with a 0% false-positive rate when $D_{\min}$ reaches 68 ft in the 802.11 network and 56 ft in the 802.15.4 network, respectively.

VIII. Localizing Adversaries

If an identity-based attack is determined to be present by the attack detector, we want to localize the adversaries and to eliminate the attackers from the network. In this section, we present a real-time localization system that can be used to locate the positions of the attackers. We then describe the localization algorithms for estimating the adversaries' position. The experimental results are presented to evaluate the effectiveness of our approach.

A. Localization System

We have developed a general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy-to-plug-in localization algorithms. It is built around four logical components: 1) Transmitter; 2) Landmark; 3) Server; and 4) Solver. The system architecture is shown in Fig. 14.

Transmitter: Any device that transmits packets can be localized. Oftentimes, the application code does not need to be altered on a sensor node to localize it.

Landmark: The Landmark component listens to the packet traffic and extracts the RSS reading for each transmitter. It then forwards the RSS information to the Server component. The Landmark component is stateless and is usually deployed on each landmark or AP with known locations.

Server: A centralized server collects RSS information from all the Landmark components. The identity-based detection is performed at the Server component. The Server component summarizes RSS information such as averaging or clustering and then forwards the information to the Solver component for localization estimation.

Solver: The Solver component takes the input from the Server component, performs the localization task by utilizing the localization algorithms that are plugged in, and returns the localization results back to the Server component. There are

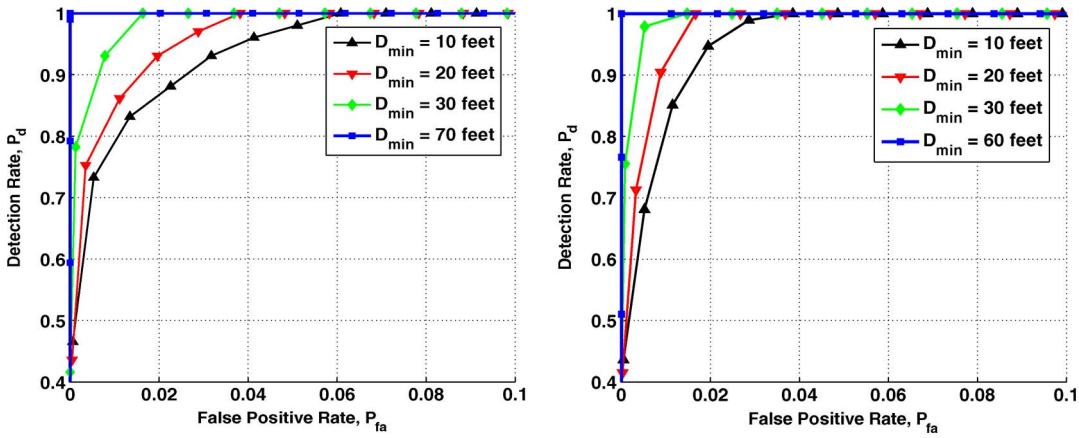


Fig. 12. Sybil-attack detection: ROC curves when varying the node distance threshold $D_{\min}$. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

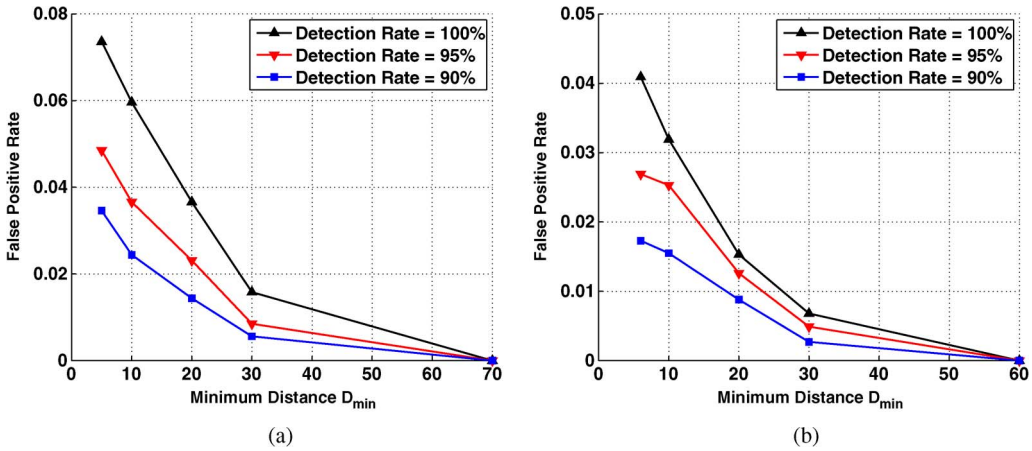


Fig. 13. Sybil-attack detection: False-positive rate as a function of the node distance threshold $D_{\min}$. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

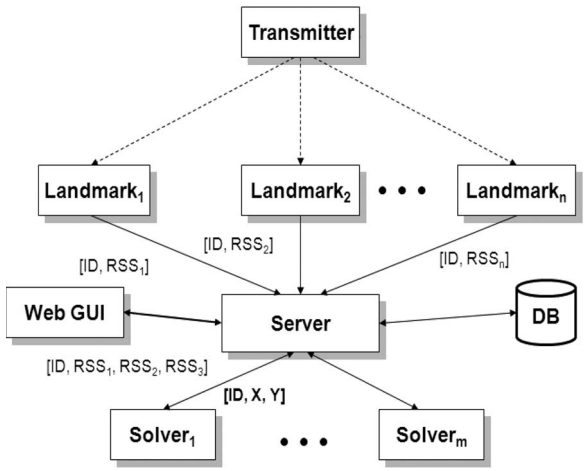


Fig. 14. Localization system architecture.

multiple Solver instances available, and each Solver instance can simultaneously localize multiple transmitters.

During the localization process, the following steps will take place:

1) A Transmitter sends a packet. Some numbers of Landmarks observe the packet and record the RSS.
2) Each Landmark forwards the observed RSS from the transmitter to the Server.
3) The Server collects the complete RSS vector for the transmitter and sends the information to a Solver instance for location estimation.
4) The Solver instance performs localization and returns the coordinates of the transmitter back to the Server.

If there is a need to localize hundreds of transmitters at the same time, the server can perform load balancing among different solver instances. This centralized localization solution also makes enforcing contracts and privacy policies more tractable.

B. Attack Localizer

When our detector has identified an attack for a node identity, the centroids returned by the K-means clustering analysis in signal space can be used by the Server and sent to the Solver for location estimation. In particular, in spoofing attacks, the returned positions should be the location estimate for the original node and the spoofing nodes in physical space. Fig. 15 shows an example of the relationship among the original node P_{org}, the location estimation of the original node L_{org}, the spoofing node P_{spoof}, and the localized spoofing node position L_{spoof}.

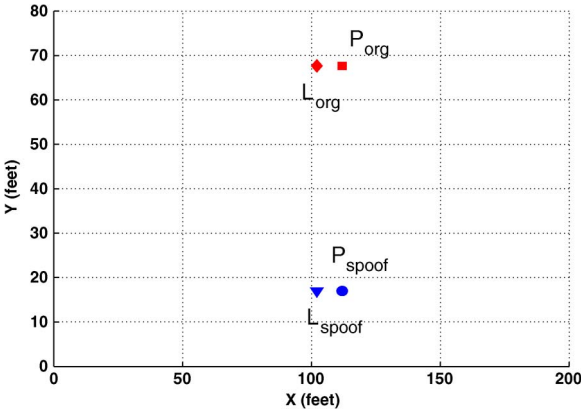


Fig. 15. Relationships among the original node, the spoofing node, and their location estimation returned by the localization system.

To show the generality of our localization system in locating the adversarial nodes, we have chosen two representative localization algorithms that use signal strength from point- and area-based algorithms.

RADAR: Point-based methods return an estimated point as a localization result. One primary example of a point-based method is the RADAR scheme [13]. In RADAR, during the offline phase, a mobile transmitter with known position periodically broadcasts beacons, and the RSS readings are measured at a set of landmarks. Collecting together the averaged RSS readings from each of the landmarks for a set of known locations provides a radio map. At runtime, localization is performed by measuring a transmitter's RSS at each landmark, and the vector of RSS values is compared with the radio map. The record in the radio map whose signal strength vector is closest, in the Euclidean sense, to the observed RSS vector is declared to correspond to the location of the transmitter. In this paper, instead of using the averaged RSS in the traditional approach, we use the RSS centroids obtained from the K-means clustering algorithm as the observed RSS vector for localizing a node.

Area-Based Probability (ABP): Area-based algorithms return the most likely area in which the true location resides. Compared with point-based methods, one major advantage of area-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. ABP returns an area, i.e., a set of tiles on the floor, bounded by a probability that the transmitter is within the returned area [17]. ABP assumes that the distribution of RSS for each landmark follows a Gaussian distribution. The Gaussian random variable from each landmark is independent. ABP then computes the probability that the transmitter is at each tile L_i on the floor by using Bayes' rule, i.e.,

$$P(L_i \mid \mathbf{s}) = \frac{P(\mathbf{s} \mid L_i) \times P(L_i)}{P(\mathbf{s})}. \tag{25}$$

Given that the transmitter resides at exactly one tile, satisfying $\sum_{i=1}^{L} P(L_i \mid \mathbf{s}) = 1$, ABP normalizes the probability and returns the most likely tiles up to its confidence α.

Both RADAR and ABP are employed in our experiments to localize the positions of the attackers.

C. Experimental Evaluation

1) Localization Metrics: To evaluate the effectiveness of our localization system in finding the locations of the attackers, we are interested in the following performance metrics.

Localization error CDF. We obtain the CDF of the location-estimation error from all the localization attempts of adversaries. For area-based algorithms, we also report CDFs of the minimum and maximum errors. For a given localization attempt, these are points in the returned area that are closest to and furthest from the true location.

Relationship between the true and estimated distances. For spoofing attacks, the relationship between the true distance of the spoofing node to the original node $\|P_{\text{org}} - P_{\text{spoof}}\|$ and the distance of the location estimate of the spoofing node to that of the original node $\|L_{\text{org}} - L_{\text{spoof}}\|$ evaluates how accurate our attack localizer can report the positions of both the original node and the attackers.

2) Experimental Results: We first present the statistical characterization of the location-estimation errors. Fig. 16 presents the localization error CDF of the original nodes and the spoofing nodes for both RADAR and ABP in the 802.11 and 802.15.4 networks. For the area-based algorithm, we present the median tile error $ABP - med$ and the minimum and maximum tile errors $ABP - min$ and $ABP - max$, respectively. We found that the location-estimation errors from using the RSS centroids in signal space are about the same as using averaged RSS as the input for localization algorithms [15]. Furthermore, we observed that the localization performance in the 802.11 network is similar to that in the 802.15.4 network. Due to space limitations, we did not present the localization results of Sybil nodes. We note that we observed similar localization performance when localizing Sybil nodes.

More importantly, we observed that the localization performance of the original nodes is qualitatively the same as that of the spoofing nodes. This result is very encouraging, because the similar performance is strong evidence that using the centroids from the K-means cluster analysis is effective in both identifying the identity-based attacks and localizing the attackers.

In spoofing attacks, the challenge in localizing the positions of spoofing nodes arises, because the system does not know the positions of either the original or the spoofing node. Thus, we would like to examine how accurate the localization system can estimate the distance between P_{org} and P_{spoofing}. Fig. 17 displays the relationship between $\|L_{\text{org}} - L_{\text{spoofing}}\|$ and $\|P_{\text{org}} - P_{\text{spoofing}}\|$ across different localization algorithms and networks. The blue dots represent the cases of the detected spoofing attacks, whereas the red crosses indicate the spoofing attacks have not been detected by the K-means attack detector. Comparing with Fig. 8, i.e., the detection rate as a function of the distance between P_{org} and P_{spoofing}, the results of the undetected spoofing attack cases represented by the red crosses are in line with the results in Fig. 8. The spoofing attacks are 100% detected when $\|P_{\text{org}} - P_{\text{spoofing}}\|$ is equal to or is greater than about 50 ft.

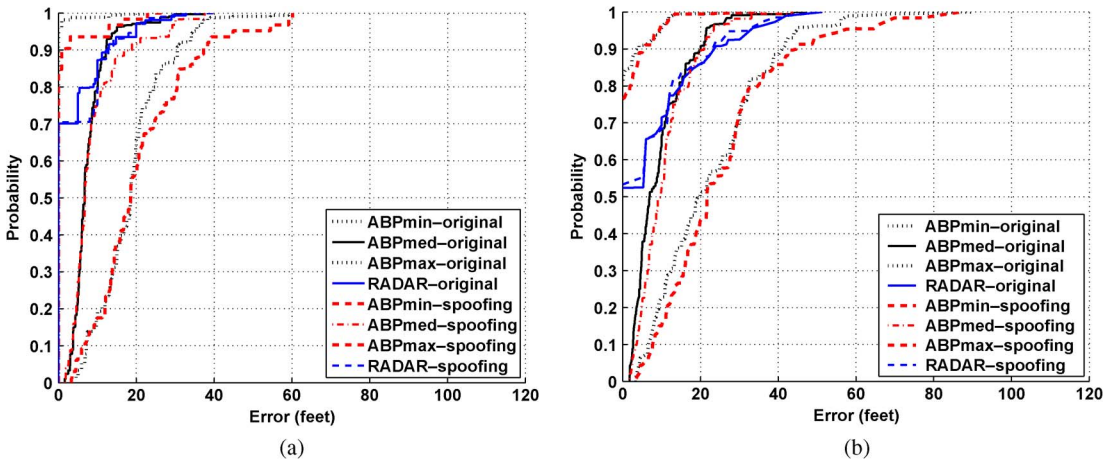


Fig. 16. Localization error CDF across localization algorithms and networks when localizing both original and spoofing nodes in spoofing attacks. (a) IEEE 802.11 network. (b) IEEE 802.15.4 network.

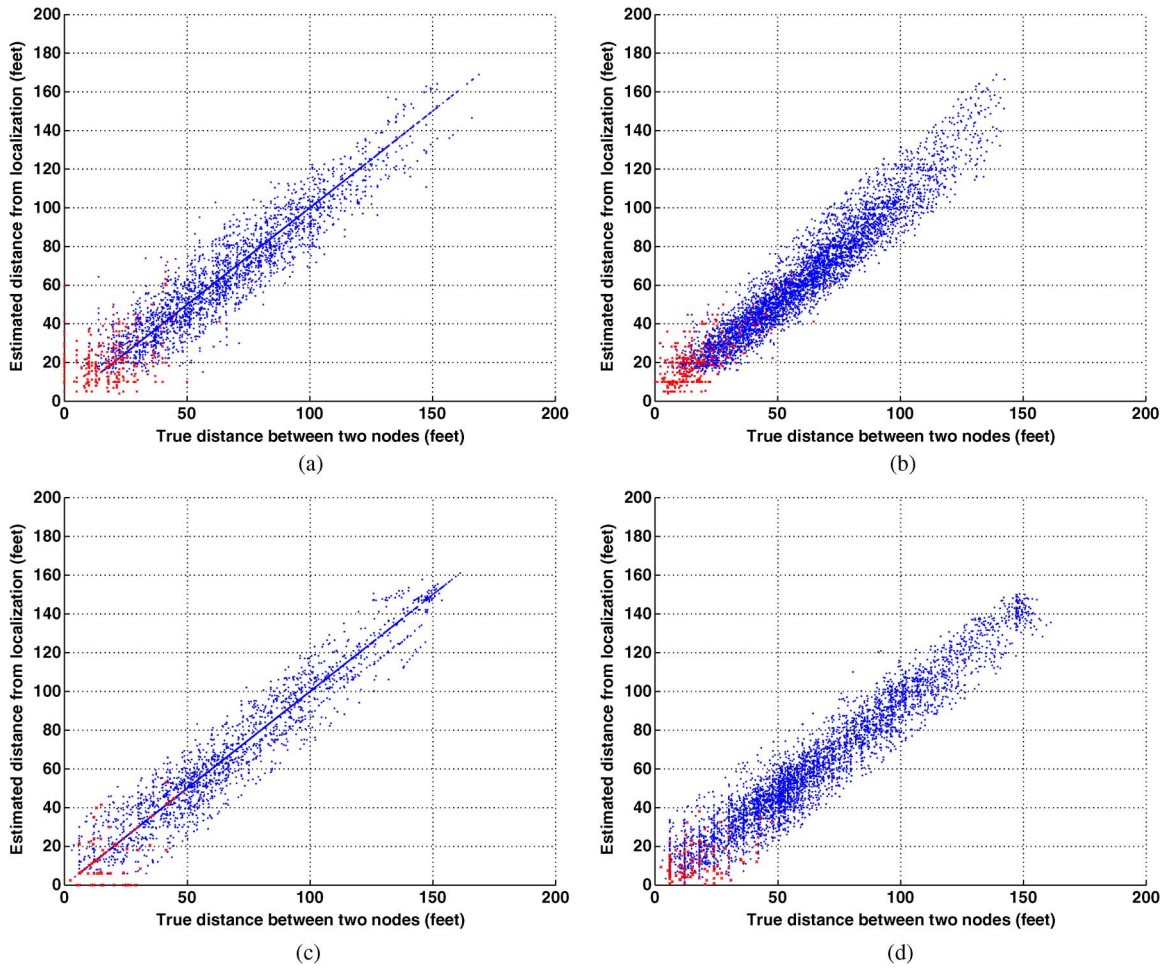


Fig. 17. Relationship between the true distance and the estimated distance for the original and spoofing nodes across localization algorithms and networks in spoofing attacks. (a) IEEE 802.11: RADAR, $\tau = 10$ dB. (b) IEEE 802.11: ABP, $\tau = 10$ dB. (c) IEEE 802.15.4: RADAR, $\tau = 9$ dB. (d) IEEE 802.15.4: ABP, $\tau = 9$ dB.

Furthermore, the relationship between $\|L_{\text{org}} - L_{\text{spoof}}\|$ and $\|P_{\text{org}} - P_{\text{spoof}}\|$ is along the 45° straight line. This result means that $\|L_{\text{org}} - L_{\text{spoof}}\|$ is directly proportional to $\|P_{\text{org}} - P_{\text{spoof}}\|$ and indicates that our localization system is highly effective for localizing the attackers. At a fixed distance value of $\|P_{\text{org}} - P_{\text{spoof}}\|$, the values of $\|L_{\text{org}} - L_{\text{spoof}}\|$ fluctuate around the true distance value. The fluctuation reflects the localization errors of both P_{org} and P_{spoof}. The larger the $\|P_{\text{org}} - P_{\text{spoof}}\|$ is, the smaller the fluctuation of $\|L_{\text{org}} - L_{\text{spoof}}\|$ becomes, at about 10-ft maximum. This result means that, if the spoofing node is farther away from the original node, it is extremely likely that the K-means attack detector can

detect it. In addition, our attack localizer can find the attacker's position and estimate the distance from the original node to the spoofing node at a maximum error of about 10–20 ft.

IX. Related Work

There has been active research that addresses identity-based attacks. We cannot cover the entire body of works in this section. Rather, we give a short overview of traditional approaches and several new methods. We then describe the related research in localization.

Detection of Spoofing Attacks: The traditional security approach to cope with identity fraud is to use cryptographic authentication. An authentication framework for hierarchical *ad hoc* sensor networks is proposed in [22], and a hop-by-hop authentication protocol is presented in [23]. The work in [24] has introduced a secure and efficient key management (SEKM) framework. The authors of [25] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. In addition, binding approaches are employed by cryptographically generated addresses (CGA) to defend against the network identity spoofing [26].

It is not always desirable to use authentication due to limited resources on nodes and infrastructural overhead involved; therefore, new approaches have recently been proposed to detect spoofing attacks that use physical properties associated with wireless transmission. The work in [27] has introduced a security layer that is separate from conventional network-authentication methods. The authors of [28] utilized properties of the wireless channel at the physical layer to support high-level security objectives. The most closely related works to our paper are [4] and [29], in which one work proposed the use of matching rules of signal prints for spoofing detection, whereas the other work modeled the RSS readings using a Gaussian mixture model. However, they did not address how they can localize attackers.

Detection of Sybil Attacks: Employing cryptographic-related methods [30]–[32] are the traditional approaches to prevent Sybil attacks. To address the issues of computational constraints on wireless and sensor nodes, [1] proposed schemes based on symmetric key cryptography to satisfy the resource requirements, and [33] used unique random pairwise key establishment schemes based on t-degree polynomials.

Furthermore, radio resource testing and registration approaches are two methods that deviate from the conventional security approaches. However, the radio-resource testing [32] process may consume much battery power, whereas registration alone cannot prevent Sybil attacks, because a malicious attacker may get multiple identities by nontechnical means such as stealing. In addition, [9] employed RSS to detect wireless Sybil attacks. However, it did not study how the Sybil nodes can be localized.

Wireless Localization: The localization techniques can be categorized along several dimensions. Based on localization infrastructure, [34] used infrared methods, and [35] employed ultrasound to perform localization. Both of them need to deploy specialized infrastructure for localization. On the other hand, in spite of its several-meter-level accuracy [12], using RSS [13], [17], the work in [36] is an attractive approach, because it can reuse the existing wireless infrastructure.

Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks by using the measurement of various physical properties [37] such as RSS [13], [15], time of arrival (TOA) [38], and time difference of arrival (TDOA) [35]. Range-free algorithms [39]–[41] use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy for mapping a node to a location. Lateration approaches [38], [41], [42] use distances to landmarks, whereas angulation uses the angles from landmarks. Fingerprint-matching strategies [13]–[15] use a function that maps observed radio properties to locations on a preconstructed radio map. Finally, another dimension of classification extends to aggregate [39] or singular algorithms.

Our paper differs from the aforementioned research in several ways. First, there is little work that can detect both spoofing and Sybil attacks using the same set of techniques. Furthermore, our approach is robust to attackers that use different transmission power levels to launch attacks. Finally, much of the aforementioned work focuses on attack detection only, whereas our paper can perform both attack detection and localize the adversaries' positions.

X. Conclusion

In this paper, we have proposed a method for detecting identity-based attacks, including spoofing and Sybil attacks, and localizing the adversaries in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, our RSS-based approach does not add additional overhead to the wireless devices and sensor nodes. We formulated the identity-based detection problem as a statistical-significance-testing problem. We then provided theoretical analysis of exploiting the spatial correlation of RSS inherited from wireless nodes for attack detection. We further utilized the K-means cluster analysis to derive the test statistic. Our attack detector is robust to detect attacks that are launched by adversaries that use different transmission power levels. In addition, we have built a real-time localization system and integrated our K-means attack detector into the system to locate the positions of the attackers and, as a result, to eliminate the adversaries from the network.

We studied the effectiveness and generality of our attack detector and attacker localizer in both the 802.11 and 802.15.4 networks in two real office building environments. The performance of the K-means attack detector is evaluated in terms of detection rates and ROC curves. Our attack detector has achieved high detection rates, i.e., more than 95%, and low false-positive rates, i.e., less than 5%. Moreover, our DoT mechanism is highly effective in detecting a Sybil attack that uses different transmission power levels.

When locating the positions of the attackers, we have utilized both the point- and area-based algorithms in our real-time localization system. We found that the performance of the system, when localizing the adversaries that use the results of the K-means cluster analysis, are about the same as localizing

under normal conditions. In particular, in spoofing attacks, the distance between the spoofing node and the original node can be estimated with a median error of 10 ft. Our method is generic across different localization algorithms and networks. Therefore, our experimental results provide strong evidence of the effectiveness of our approach in detecting identity-based attacks and localizing the positions of the adversaries.

REFERENCES

[1] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil attacks in sensor networks," in *Proc. 25th IEEE ICDCSW*, Jun. 2005, pp. 185–191.

[2] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, 1999, pp. 173–186.

[3] A. Banerjea, "A taxonomy of dispersity routing schemes for fault-tolerant real-time channels," in *Proc. ECMAST*, May 1999, vol. 26, pp. 129–148.

[4] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC-layer spoofing using received signal strength," in *Proc. IEE INFOCOM*, Apr. 2008, pp. 1768–1776.

[5] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Security Symp.*, 2003, pp. 15–28.

[6] W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," *IEEE Wireless Commun.*, vol. 9, no. 6, pp. 44–51, Dec. 2002.

[7] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2004, pp. 634–638.

[8] J. R. Douceur, "The Sybil attack," in *Proc. 1st IPTPS*, Mar. 2002, pp. 251–260.

[9] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. Int. Workshop Adv. Experimental Activities Wireless Netw. Syst.*, 2006, pp. 564–570.

[10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *ACM Wireless Netw. J.*, vol. 8, no. 5, pp. 481–494, Sep. 2002.

[11] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 2, pp. 221–262, May 2006.

[12] A. Krishnakumar and P. Krishnan, "On the accuracy of signal-strength-based location estimation techniques," in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 642–650.

[13] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE INFOCOM*, Mar. 2000, pp. 775–784.

[14] M. Youssef, A. Agrawal, and A. U. Shankar, "WLAN location determination via clustering and probability distributions," in *Proc. 1st IEEE PerCom*, Mar. 2003, pp. 143–150.

[15] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, "The robustness of localization algorithms to signal-strength attacks: A comparative study," in *Proc. DCOSS*, Jun. 2006, pp. 546–563.

[16] T. Roos, P. Myllymaki, H. Tirri, P. Misikangas, and J. Sievanen, "A probabilistic approach to WLAN user location estimation," *Int. J. Wireless Inf. Netw.*, vol. 9, no. 3, pp. 155–164, Jul. 2002.

[17] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, "A practical approach to landmark deployment for indoor localization," in *Proc. 3rd IEEE SECON*, Sep. 2006, pp. 365–373.

[18] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A survey of various propagation models for mobile communication," *IEEE Antennas Propag. Mag.*, vol. 45, no. 3, pp. 51–82, Jun. 2003.

[19] A. Goldsmith, *Wireless Communications*. New York: Cambridge Univ. Press, 2005.

[20] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1965.

[21] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning, Data Mining Inference, and Prediction*. New York: Springer-Verlag, 2001.

[22] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *Proc. ACM WiSe*, 2003, pp. 79–87.

[23] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A lightweight hop-by-hop authentication protocol for ad hoc networks," in *Proc. IEEE MWN*, 2003, pp. 749–755.

[24] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in *Proc. 19th IEEE IPDPS*, 2005, p. 288a.

[25] A. Wool, "Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation," *Wireless Netw.*, vol. 11, no. 6, pp. 677–686, Nov. 2005.

[26] T. Aura, "Cryptographically Generated Addresses (CGA)," RFC 3972, IETF, 2005.

[27] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in *Proc. 3rd IEEE SECON*, Sep. 2006, pp. 50–59.

[28] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. ACM WiSe*, 2006, pp. 30–42.

[29] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signal prints," in *Proc. ACM WiSe*, Sep. 2006, pp. 43–52.

[30] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM CCS*, Nov. 2002, pp. 41–47.

[31] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[32] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in *Proc. 3rd IPSN*, Apr. 2004, pp. 259–268.

[33] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM CCS*, Oct. 2003, pp. 52–61.

[34] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active-badge location system," *ACM Trans. Inf. Syst.*, vol. 10, no. 1, pp. 91–102, Jan. 1992.

[35] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location support system," in *Proc. ACM MobiCom*, Aug. 2000, pp. 32–43.

[36] J. Yang and Y. Chen, "A theoretical analysis of wireless localization using RF-based fingerprint matching," in *Proc. 4th SMTPS*, Apr. 2008, pp. 1–6.

[37] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[38] P. Enge and P. Misra, *Global Positioning System: Signals, Measurements, and Performance*. Lincoln, MA: Ganga-Jamuna, 2001.

[39] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz, "Localization from mere connectivity," in *Proc. 4th ACM MobiHoc*, Jun. 2003, pp. 201–212.

[40] T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes in large-scale sensor networks," in *Proc. 9th ACM MobiCom*, 2003, pp. 81–95.

[41] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," in *Proc. IEEE GLOBECOM*, 2001, pp. 2926–2931.

[42] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: A quantitative comparison," *Comput. Netw.*, vol. 43, no. 4, pp. 499–518, Nov. 2003.

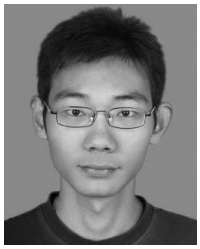
[43] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. 4th IEEE SECON*, May 2007, pp. 193–202.

[44] J. Yang, Y. Chen, and W. Trappe, "Detecting Sybil attacks in wireless and sensor networks using cluster analysis," in *Proc. 4th IEEE Int. Workshop Wireless Sensor Netw. Security*, Sep. 2008, pp. 834–839.

Yingying Chen (M'08) received the Ph.D. degree in computer science from Rutgers, The State University of New Jersey, Piscataway.

She is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ. Prior to joining Stevens Institute of Technology, she was with Bell Laboratories and the Optical Networking Group, Lucent Technologies, Holmdel, NJ. Her research interests include wireless and system security and privacy, wireless networking, and distributed systems. She is a Coauthor of *Securing Emerging Wireless Systems* and has extensively published in journal papers and conference proceedings.

Dr. Chen was the recipient of the National Science Foundation CAREER Award, the IEEE Outstanding Contribution Award from the IEEE New Jersey Coast Section from 2005 to 2009, the Best Technological Innovation Award from the International TinyOS Technology Exchange in 2006, and the Best Paper Award at the 2009 International Conference on Wireless On-Demand Network Systems and Services.



Jie Yang (S'08) received the B.E. degree in automatic control from the Beijing Institute of Technology, Beijing, China, in 2004. From 2005 to 2007, he was under the Ph.D. program with the Department of Automatic Control, Beijing Institute of Technology. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ.

His research interests include the areas of information security and privacy, wireless localization, and location-based services.

Wade Trappe (M'03) received the B.A. degree in mathematics from the University of Texas at Austin, in 1994 and the Ph.D. degree in applied mathematics and scientific computing from the University of Maryland, College Park, in 2002.

He is currently an Associate Director with the Wireless Information Network Laboratory and an Associate Professor with the Department of Electrical and Computer Engineering, Rutgers, The State University of New Jersey, Piscataway. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects that involve security and privacy for sensor networks, physical-layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new radio frequency identification technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks and mechanisms for jamming detection and defense for wireless networks and has investigated privacy-enhancing routing methods for wireless networks. He has published more than 100 papers, including two papers in media security and one paper on the localization of cognitive radios (for which he received the Best Paper Awards) and several wireless security papers in premier conference proceedings. His experience in network security and wireless systems spans 12 years, and he is a Coauthor of the popular textbook *Introduction to Cryptography With Coding Theory* and four other books on wireless systems and multimedia security.

Dr. Trappe is a member of the IEEE Signal Processing Society, the IEEE Communications Society, and the Association for Computing Machinery.

Richard P. Martin (M'10) received the B.A. degree from Rutgers, The State University of New Jersey, Piscataway, and the M.S. and Ph.D. degrees in computer science from the University of California, Berkeley.

He is currently an Associate Professor of computer science with Rutgers, The State University of New Jersey, where he is a Member of the Wireless Network Information Laboratory. His research interests include wireless device localization and human factors in dependable computing.

Dr. Martin received of the Best Paper Award at the 2004 IEEE Conference on Sensor and Ad Hoc Communication Networks and a Faculty Early Career Development (CAREER) Award from the U.S. National Science Foundation (NSF). He has served as an Investigator on grants from the Defense Advanced Research Projects Agency, the NSF, and IBM.