Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

Jie Yang, *Student Member*, *IEEE*, Yingying (Jennifer) Chen, *Senior Member*, *IEEE*, Wade Trappe, *Member*, *IEEE*, and Jerry Cheng

Abstract—Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In this paper, we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, we explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. We evaluated our techniques through two testbeds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90 percent Hit Rate and Precision when determining the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

Index Terms—Wireless network security, spoofing attack, attack detection, localization

1 Introduction

Due to the openness of the wireless transmission medium, adversaries can monitor any transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an *ifconfig* command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames—an attacker can still spoof management or control frames to cause significant impact on networks.

- *J. Yang is with the Department of Computer Science and Engineering, Oakland University, Rochester, Michigan 48309. E-mail: yang@oakland.edu.*
- *Y. Chen is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030. E-mail: yingying.chen@stevens.edu.*
- *W. Trappe is with WINLAB, Rutgers, The State University of New Jersey, Route 1 Tech Center, Room A-102, Technology Centre of New Jersey, 671 Route 1 South, North Brunswick, NJ 08902-3390. E-mail: trappe@winlab.rutgers.edu.*
- *J. Cheng is with the Department of Medicine, Robert Wood Johnson Medical School, University of Medicine & Dentistry of New Jersey, New Brunswick, NJ 08901. E-mail: chengjq@umdnj.edu.*

Manuscript received 7 Nov. 2010; revised 22 July 2011; accepted 7 Mar. 2012; published online 20 Mar. 2012.
Recommended for acceptance by D. Xuan.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2010-11-0663.
Digital Object Identifier no. 10.1109/TPDS.2012.104.

Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial-of-Service (DoS) attacks. A broad survey of possible spoofing attacks can be found in [3], [4]. Moreover, in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly. Therefore, it is important to 1) detect the presence of spoofing attacks, 2) determine the number of attackers, and 3) localize multiple adversaries and eliminate them.

Most existing approaches to address potential spoofing attacks employ cryptographic schemes [5], [6]. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned. In this work, we propose to use received signal strength (RSS)-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since we are concerned with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

We focus on static nodes in this work, which are common for spoofing scenarios [7]. We addressed spoofing detection in mobile environments in our other work [8]. The works that are closely related to us are [3], [7], [9]. Faria and Cheriton [3] proposed the use of matching rules of signalprints for spoofing detection, Sheng et al. [7] modeled the RSS readings using a Gaussian mixture model and Chen et al. [9] used RSS and K-means cluster analysis to detect spoofing attacks. However, none of these approaches have the ability to determine the number of attackers when multiple adversaries use the same identity to launch attacks, which is the basis to further localize multiple adversaries after attack detection. Although Chen et al. [9] studied how to localize adversaries, it can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power levels.

The main contributions of our work are: 1) GADE: a generalized attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries; and 2) IDOL: an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

In GADE, the Partitioning Around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker. We further developed a mechanism called SILENCE for testing Silhouette Plot and System Evolution with minimum distance of clusters, to improve the accuracy of determining the number of attackers. Additionally, when the training data are available, we propose to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. As we demonstrated through our experiments using both an 802.11 network as well as an 802.15.4 network in two real office building environments, GADE is highly effective in spoofing detection with over 90 percent hit rate and precision. Furthermore, using a set of representative localization algorithms, we show that IDOL can achieve similar localization accuracy when localizing adversaries to that of under normal conditions. One key observation is that IDOL can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network.

The rest of the paper is organized as follows. We place our work in the context of related research in Section 2. We provide our theoretical analysis and describe the generalized attack detection model in Section 3. We formulate the problem of determining the number of attackers using multiclass detection and propose our cluster-analysis-based mechanisms in Section 4. In Section 5, we present IDOL, the integrated detection and localization system. Finally, we conclude our work in Section 6.

2 Related Work

The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication [5], [6], [10]. Wu et al. [5] have introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Wool [6] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. An authentication framework for hierarchical, ad hoc sensor networks is proposed in [10]. However, the cryptographic authentication may not be always applicable because of the limited resources on wireless devices, and lacking of a fixed key management infrastructure in the wireless network.

Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorrelates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations, and thus to detect spoofing attacks in wireless networks [11]. Brik et al. [12] focused on building fingerprints of 802.11b WLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. However, there is additional overhead associated with wireless channel response and radiometric signature extraction in wireless networks. Li and Trappe [4] introduced a security layer that used forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks. The MAC sequence number has also been used in [13] to perform spoofing detection. Both the sequence number and the traffic pattern can be manipulated by an adversary as long as the adversary learns the traffic pattern under normal conditions.

The works [3], [7], [14] using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton [3] proposed the use of matching rules of signalprints for spoofing detection. Sheng et al. [7] modeled the RSS readings using a Gaussian mixture model. Sang and Arora [14] proposed to use the node's "spatial signature," including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. However, none of these approaches are capable of determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. Further, they do not have the ability to localize the positions of the adversaries after attack detection.

Turning to studying localization techniques, in spite of its several meter-level accuracy, using RSS [15], [16], [17], [18] is an attractive approach because it can reuse the existing wireless infrastructure and is highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties such as RSS [15], [16], Time Of Arrival (TOA) [19], Time

Difference Of Arrival (TDOA), and direction of arrival (DoA) [20]. Whereas range-free algorithms [21] use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Lateration approaches [19] use distances to landmarks, while angulation uses the angles from landmarks. Scene matching strategies [15] use a function that maps observed radio properties to locations on a preconstructed signal map or database. Further, Chen et al. [22] proposed to perform detection of attacks on wireless localization and Yang et al. [20] proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, we choose a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy.

Our work differs from the previous study in that we use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, our work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

3 Generalized Attack Detection Model

In this section, we describe our Generalized Attack Detection ModEl, which consists of two phases: *attack detection*, which detects the presence of an attack, and *number determination*, which determines the number of adversaries. The number determination phase will be presented in Section 4.

3.1 Theoretical Analysis of the Spatial Correlation of RSS

The challenge in spoofing detection is to devise strategies that use the uniqueness of spatial information, but not using location directly as the attackers' positions are unknown. We propose to study RSS, a property closely correlated with location in physical space and is readily available in the existing wireless networks. 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 the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

We define the RSS value vector as $s = \{s_1, s_2, \ldots s_n\}$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations. Generally, the RSS at the ith landmark from a wireless node is lognormally distributed [23]

$$s_i(d_j)[dBm] = P(d_0)[dBm] - 10\gamma \log\left(\frac{d_j}{d_0}\right) + X_i, \quad (1)$$

where $P(d_0)$ represents the transmitting power of the node at the reference distance d_0, d_j is the distance between the wireless node j and the ith landmark, and γ is the path loss exponent, X_i is the shadow fading which follows zero mean Gaussian distribution with δ standard deviation [23], [24]. For simplicity, we assume the wireless nodes have the same transmission power. We will discuss the issue of using different transmission power levels in Section 3.4. Given two wireless nodes in the physical space, the RSS distance between two nodes in signal space at the ith landmark is given by

$$\Delta s_i = 10\gamma \log\left(\frac{d_2}{d_1}\right) + \Delta X, \quad (2)$$

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

The square of RSS distance in n-dimensional signal space (i.e., at n landmarks) is then determined by

$$\Delta D^2 = \sum_{i=1}^{n} \Delta s_i^2, \quad (3)$$

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

Based on (2) and (3), we know that, when these two wireless nodes are at the same location, the distance $(1/2\delta^2)\Delta D^2$ in n dimension signal space follows a *central Chi-square distribution* $\chi^2(n)$ with n degree of freedom [25]. The probability density functions (PDF) of the random variable $X = \Delta D^2$, which is the square distance in n-dimensional signal space, when two wireless nodes are at the same location can be represented as

$$f_X(x|\text{same location}) = \frac{1}{2^n \delta^n \Gamma(n/2)} e^{-x/4\delta^2} x^{(n/2-1)}, \quad (4)$$

where $x \geq 0$ and $\Gamma(n/2)$ denotes the Gamma function, which has closed-form values at the half-integers.

However, when these two wireless nodes are at different locations, $(1/2\delta^2)\Delta D^2$ becomes a *noncentral chi-square distribution* $\chi^2(n, \lambda)$ with n degree of freedom and a noncentrality parameter λ, where

$$\lambda = \sum_{i=1}^{n} \left(10\gamma \log\left(\frac{d_{i2}}{d_{i1}}\right)\right)^2, \quad (5)$$

and d_{ij}, with $i = 1, 2, \ldots n,\ j = 1, 2$, is the distance from jth wireless nodes to the ith landmark. The PDF of the random variable $X = \Delta D^2$ when two wireless node are at the different locations can be represented as

$$f_X(x|\text{diff. locations}) = \frac{1}{4\delta^2} e^{-\frac{\lambda+x}{4\delta^2}} \left(\frac{x}{\lambda}\right)^{\frac{n-2}{4}} I_{\frac{n-2}{2}}\left(\frac{\sqrt{\lambda x}}{2\delta^2}\right), \quad (6)$$

where $I_\alpha(z)$ is a modified Bessel function of the first kind [25].

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

$$DR = P(x > \tau|\text{diff. locations}) = 1 - \mathcal{F}_{\chi^2(n,\lambda/2\delta^2)}\left(\frac{\tau}{2\delta^2}\right), \quad (7)$$

and the corresponding false positive rate is

$$FPR = P(x > \tau|\text{same locations}) = 1 - \mathcal{F}_{\chi^2(n)}\left(\frac{\tau}{2\delta^2}\right), \quad (8)$$

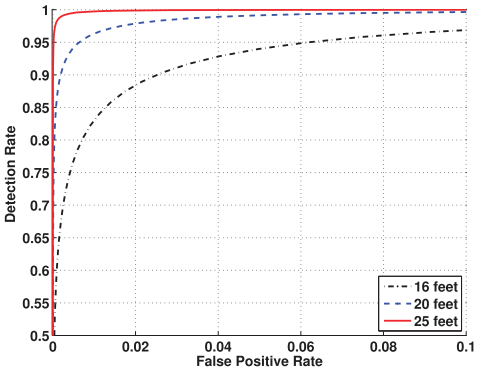


Fig. 1. The ROC curves when the distance between two wireless devices is 16, 20, and 25 feet, respectively. The standard deviation of shadowing is 2 dB. The path loss exponent is 2.5.

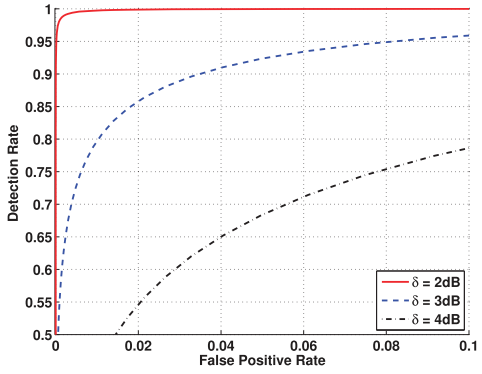


Fig. 2. The ROC curves when the standard deviation of shadowing is 2, 3, and 4 dB, respectively. The distance between two devices is 25 feet.

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

From (7) and (8), for a specified detection rate DR, the threshold of test can be obtained as

$$\tau = 2\delta^2 \mathcal{F}^{-1}_{\chi^2(n,\lambda/2\delta^2)}(1 - DR), \tag{9}$$

and the false positive rate can be represented in terms of the detection rate

$$FPR = 1 - \mathcal{F}_{\chi^2(n)}\left(\mathcal{F}^{-1}_{\chi^2(n,\lambda/2\delta^2)}(1 - DR)\right). \tag{10}$$

From (7), we can see that the detection rate DR increases with λ, which can be represented by the distance between two wireless nodes together with the landmarks. Moreover, for a specified detection rate DR, (10) shows that the false positive rate FPR increases with the standard deviation of shadowing δ.

We next study the detection power of our approach by using the RSS-based spatial correlation. Fig. 1 presents the numerical results of receiver operating characteristic (ROC) curves based on (7) and (8) when randomly placing two wireless devices in a 100 by 100 feet square area. There are four landmarks deployed at the four corners of the square area. The physical distance between two wireless devices is 16, 20, and 25 feet, respectively. The path loss exponent γ is set to 2.5 and the standard deviation of shadowing is 2 dB. From the figure, we observed that the ROC curves shift to the upper left when increasing the distance between two devices. This indicates that the farther away the two nodes are separated, the better detection performance that our method can achieve. This is because the detection performance is proportional to the noncentrality parameter λ, which is represented by the distance between two wireless nodes together with the landmarks.

We further investigate the detection performance of our approach under RSS variations. In this study, we fixed the distance between two wireless devices as 25 feet. The obtained ROC curves when the standard deviation of shadowing is set to 2, 3, and 4 dB, respectively, is shown in Fig. 2. From the figure, it can be seen that we can obtain better detection performance with lower standard deviation of shadowing δ. A larger standard deviation of shadowing causes the two distributions, i.e., noncentral chi-square and central chi-square, to get closer to one another. Consequently, the smaller standard deviation of shadowing δ results in a better detection performance.

3.2 Attack Detection Using Cluster Analysis

The above analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that the RSS readings from a wireless node may fluctuate and should cluster together. In particular, the RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. We illustrated this important observation in Fig. 3, which presents RSS reading vectors of three landmarks (i.e., $n = 3$) from two different physical locations. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

In this work, we utilize the Partitioning Around Medoids Method to perform clustering analysis in RSS. The PAM Method [26] is a popular iterative descent clustering algorithm. Compared to the popular K-means method [9], the PAM method is more robust in the presence of noise and outliers. Thus, the PAM method is more suitable in

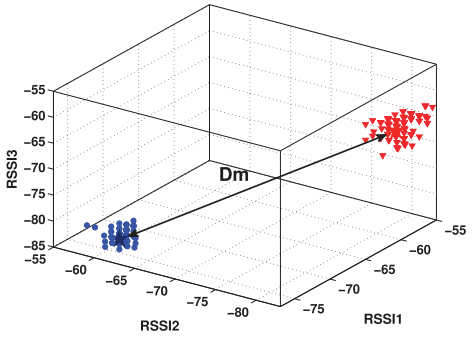


Fig. 3. Illustration of RSS readings from two physical locations.

determining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias [27].

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

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

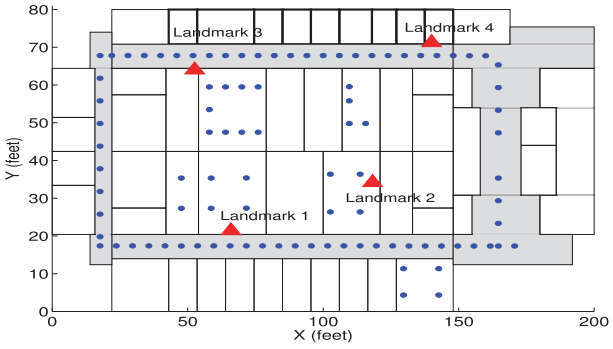
In significance testing, a test statistic $\mathbf{T}$ is used to evaluate whether observed data belong to the null-hypothesis or not. In particular, in our attack detection phase, we partition the RSS vectors from the same node identity into two clusters (i.e., $K = 2$) no matter how many attackers are using this identity, since our objective in this phase is to detect the presence of attacks. We then choose the distance between two medoids D_m as the test statistic T in our significance testing for spoofing detection, $D_m = \|\mathbf{M_i} - \mathbf{M_j}\|$, where M_i and M_j are the medoids of two clusters. Under normal conditions, the test statistic D_m should be small since there is basically only one cluster from a single physical location. However, under a spoofing attack, there is more than one node at different physical locations claiming the same node identity. As a result, more than one clusters will be formed in the signal space and D_m will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space.

3.3 Evaluation Strategy

To test the performance of our attack detection approach, we evaluate our approach in real office building environments. We conducted experiments in two office buildings: one is the Wireless Information Network Laboratory (WINLAB) using an 802.11 (WiFi) network and the other is the Computer Science Department at Rutgers University using an 802.15.4 (ZigBee) network as presented in Fig. 4. The wireless devices we consider here are a Dell laptop running Linux and equipped with an Orinoco silver card (for the 802.11 network) and a Tmote Sky mote (for the 802.15.4 network). The size of these two floors are 219 ft $\times$ 169 ft and 200 ft $\times$ 80 ft, respectively. Fig. 4a shows five landmarks in red stars in the 802.11 networks to maximize the coverage, whereas there are four landmarks deployed as red triangles in the 802.15.4 network to achieve optimal landmark placement [17], shown in Fig. 4b. We note that the deployment of landmarks has important impact on the detection performance, which is similar to the wireless localization [17]. Each landmark is a Linux machine equipped with a Atheros miniPCI 802.11 wireless card and a Tmote Sky mote so as to measure the RSS readings from both WiFi and Zigbee networks.

The small dots in the floor maps are the locations used for testing. There are 101 locations for the 802.11 network and 94 locations for the 802.15.4 network. At each location, 300 packet-level RSS samples are collected separately during the daytime when there were people walking around. Further, to evaluate the robustness of our approach in handling attacks using different transmission power levels, we collected packets at varying transmission power levels from 30 mW (15 dBm) to 1 mW (0 dBm) for the 802.11 network. We randomly chose point combinations on the floor and treated one point as the position of the original node, and the rest as the positions of the spoofing nodes. Then, we ran tests

(a) 802.11 network



(b) 802.15.4 network

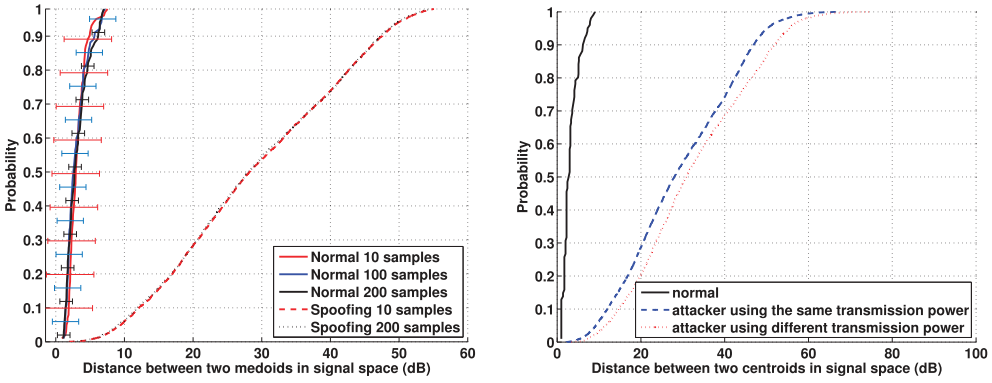
Fig. 4. Landmark setups and testing locations in two networks within two office buildings.

through all the possible combinations of testing points for cases of two, three, and four attackers masquerading as a single node identity. In addition, we built an integrated system to both detect attacks as well as localize the positions of adversaries. We use the leave-one-out method in localization algorithms, which means we choose one location as the testing node whereas the rest of the locations as training data till all the locations have been tested. The experimental results will be presented in the following sections, respectively.

3.4 Results of Attack Detection

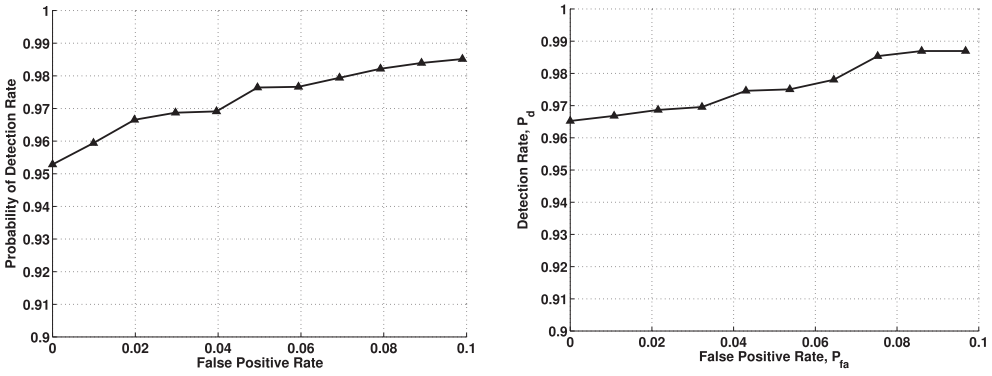
3.4.1 *Impact of Threshold and Sampling Number*

The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a threshold τ enables the attack detector to be robust to false detections. Fig. 5 shows the Cumulative Distribution Function of D_m in signal space under both normal conditions as well as with spoofing attacks. We observed that the curve of D_m shifted greatly to the right under spoofing attacks. Thus, when $D_m > \tau$, we can declare the presence of a spoofing attack. The short lines across the CDF lines are the averaged variances of D_m under different sampling numbers. We observed that the CDF curves of different sampling numbers are almost mixed together, which indicate that for a given threshold τ similar detection rate will be achieved under different sampling numbers. However, the averaged variance decreases with the increasing number of samples—the short-term RSS samples are not as stable as the long-term RSS samples. The more stable the D_m is, the more robust the detection mechanism can be. Therefore, there is a tradeoff between the



(a) Sampling number study (b) Different transmission power

Fig. 5. 802.11 network: cumulative distribution function of distance between medoids D_m in signal space.



(a) 802.11 network (b) 802.15.4 network

Fig. 6. Receiver operating characteristic curves when using the PAM method to perform attack detection.

number of RSS samples needed to perform spoofing detection and the time the system can declare the presence of an attack. For this study, we use 200 RSS samples, which has a variance of 0.84 dB^2.

3.4.2 Handling Different Transmission Power Levels

If a spoofing attacker sends packets at a different transmission power level from the original node, based on our cluster analysis there will be two distinct RSS clusters in signal space (i.e., D_m will be large). We varied transmission power for an attacker from 30 mW (15 dBm) to 1 mW (0 dBm). We found that in all cases D_m is larger than normal conditions. Fig. 5b presents an example of the Cumulative Distribution Function of the D_m for the 802.11 network when the spoofing attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB transmission power level. We observed that the curve of D_m under the different transmission power level shifts to the right indicating larger D_m values. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

3.4.3 Performance of Detection

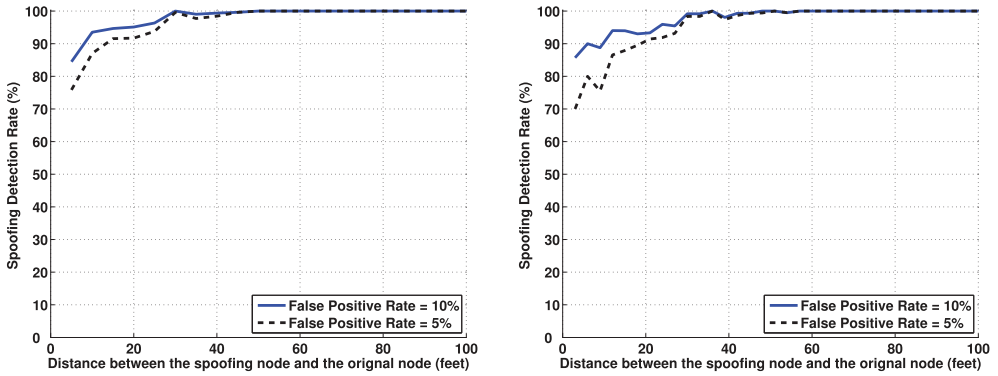
To evaluate the effectiveness of using cluster analysis for attack detection, Fig. 6 presents the Receiver Operating Characteristic curves of using D_m as a test statistic to perform attack detection for both the 802.11 and the 802.15.4 networks. Table 1 presents the detection rate and false positive rate for both networks under different threshold settings. The results are encouraging, showing that for false positive rates less than 10 percent, the detection rate are above 98 percent when the threshold τ is around 8 dB. Even when the false positive rate goes to zero, the detection rate is still more than 95 percent for both networks.

3.4.4 Impact of Distance between the Spoofing Node and the Original Node

We further study how likely a spoofing device can be detected by our attack detector when it is at various distances from the original node in physical space. Fig. 7 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 further away P_{spoof} is from P_{org}, the higher the detection rate becomes. This observation is consistent with our theoretical analysis presented in Section 3.1. In particular, for the 802.11 network, the detection rate goes to over 90 percent when P_{spoof} is about 15 feet away from P_{org} when the false positive rate is 5 percent. While for the

TABLE 1
Spoofing Attack Detection: Detection Rate and False Positive Rate in Two Networks

Network	Threshold τ	Detection Rate	False Positive Rate
802.11	6.2dB	0.985	0.10
802.11	7.3dB	0.976	0.05
802.11	9.1dB	0.953	0
802.15.4	7.6dB	0.987	0.10
802.15.4	9.0dB	0.975	0.05
802.15.4	12.4dB	0.965	0



(a) 802.11 network (b) 802.15.4 network

Fig. 7. The detection rate as a function of the distance between the spoofing node and the original node.

802.15.4 network, the detection rate is above 90 percent when the distance between P_{spoof} and P_{org} is about 20 feet by setting the false positive to 5 percent. This is in line with the average localization estimation errors using RSS [28] which are about 15 feet. When the nodes are less than 15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90 percent, but still greater than 70 percent. However, when P_{spoof} moves closer to P_{org}, the attacker also increases the probability to expose itself. The detection rate goes to 100 percent when the spoofing node is about 45-50 feet away from the original node.

4 Determining the Number of Attackers

4.1 Problem Formulation

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multiclass detection problem and is similar to determining how many clusters exist in the RSS readings. If C is the set of all classes, i.e., all possible combination of number of attackers. For instance, $C = \{1, 2, 3, 4\}$. For a class of specific number of attackers c_i, e.g., $c_i = 3$, we define P_i as the positive class of c_i and all other classes (i.e., all other number of attackers) as negative class N_i

$$P_i = c_i, \tag{11}$$

$$N_i = \bigcup_{j \neq i} c_j \in C. \tag{12}$$

Further, we are interested in the statistical characterization of the percentage that the number of attackers can be accurately determined over all possible testing attempts with mixed number of attackers. Associated with a specific number of attackers, i, we define the Hit Rate HR_i as $HR_i = \frac{N_{true}}{P_i}$ where N_{true} is the true positive detection of class c_i. Let N_{false} be the false detection of the class c_i out of the negative class N_i that do not have i number of attackers. We then define the false positive rate FP_i for a specific number of attackers of class c_i as $FP_i = \frac{N_{false}}{N_i}$. Then, the Precision is defined as

$$Precision_i = \frac{N_{true}}{N_{true} + N_{false}}. \tag{13}$$

F-measure. F-measure is originated from information retrieval and measures the accuracy of a test by considering both the Hit Rate and the Precision [29]

$$F\text{-}measure_i = \frac{2}{\frac{1}{Precision_i} + \frac{1}{HitRate_i}}. \tag{14}$$

Multiclass ROC graph. We further use the multiclass ROC graph to measure the effectiveness of our mechanisms. Particularly, we use two methods [30]: $class - reference\ based$ and $benefit - error\ \ based$. The class-reference-based formulation produces C different ROC curves when handling C classes based on P_i and N_i. Further, in the C-class detection problem, the traditional 2×2 confusion matrix, including True Positives, False Positives, False Negatives, and True Negatives, becomes an $C \times C$ matrix, which contains the C benefits (true positives) and $C^2 - C$ possible errors (false positives). The benefit-error-based method is based on the $C \times C$ matrix. For example, when $C = 3$ with possible number of attackers of $\{2, 3, 4\}$, the benefits are 3 and the possible errors are 6.

4.2 Silhouette Plot

4.2.1 Attacker Number Determination

A Silhouette Plot is a graphical representation of a cluster [31]. To determine the number of attackers, we construct Silhouettes in the following way: the RSS sample points $\mathbf{S} = \{\mathbf{s_1}, \ldots, \mathbf{s_N}\}$ (with N as the total number of samples) are the data set and we let $C = (c_1, \ldots, c_K)$ be its clustering into K clusters, as shown in Fig. 8. Let $d(\mathbf{s}_k, \mathbf{s}_l)$ be the distance between $\mathbf{s}_k$ and $\mathbf{s}_l$. Let $c_j = \{\mathbf{s}_1^j, \ldots, \mathbf{s}_{mj}^j\}$ be the jth cluster, $j = 1, \ldots, K$, where $m_j = |c_j|$.

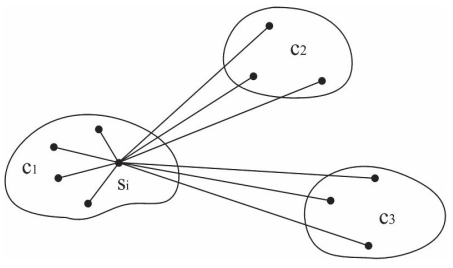


Fig. 8. Illustration of the construction of Silhouettes, $K = 3, j = 1$.

TABLE 2
Silhouette Plot: Hit Rate, Precision, and F-Measure of Determining the Number of Attackers

Number of Attackers	2	3	4
802.11 network, Hit Rate	99.59%	89.81%	80.52%
802.11 network, Precision	91.85%	87.29%	99.33%
802.11 network, F-measure	95.56%	88.53%	88.94%
802.15.4 network, Hit Rate	99.46%	91.05%	83.77%
802.15.4 network, Precision	93.22%	85.71%	99.67%
802.15.4 network, F-measure	96.24%	88.30%	91.03%

The average distance a_i^j between the ith RSS vector in the cluster c_j and the other RSS vectors in the same cluster is thus given by

$$a_i^j = \frac{1}{m_j - 1} \sum_{\substack{k=1 \\ k \neq i}}^{m_j} d\left(\mathbf{s}_i^j, \mathbf{s}_k^j\right), \quad i = 1, \ldots, m_j. \tag{15}$$

Further, the minimum average distance between the ith RSS vector in the cluster c_j and all the RSS vectors clustered in the clusters c_k, $k = 1, \ldots, K, k \neq j$ is given by

$$b_i^j = \min_{\substack{n=1,\ldots K \\ n \neq j}} \left\{ \frac{1}{m_n} \sum_{k=1}^{m_n} d\left(\mathbf{s}_i^j, \mathbf{s}_k^n\right) \right\}, \quad i = 1, ..., m_j. \tag{16}$$

Then, the silhouette width of the ith RSS vector in the cluster c_j is defined as

$$w_i^j = \frac{b_i^j - a_i^j}{\max\left\{a_i^j, b_i^j\right\}}. \tag{17}$$

From (17), it follows that $-1 \leq w_i^j \leq 1$. We can now define the silhouette of the cluster c_j

$$W_j = \frac{1}{m_j} \sum_{i=1}^{m_j} w_i^j. \tag{18}$$

Hence, the global Silhouette index for partition p that partitions the data set into K clusters is given by

$$W(K)_p = \frac{1}{K} \sum_{j=1}^{K} w_j. \tag{19}$$

Finally, we define Silhouette Coefficient SC to determine the number of attackers

$$SC = \max_K W(K)_p. \tag{20}$$

SC is used for the selection of the "best" value of the cluster number K (i.e., the optimal number of attackers) by choosing the K to make $W(K)$ as high as possible across all partitions. Since the objective of constructing silhouettes is to obtain SC, we note that there are no adjustable parameters in this detection scheme.

4.2.2 Experimental Evaluation

Table 2 presents experimental values of Hit Rate, Precision, and F-measure when the attacker number $i = \{2, 3, 4\}$ for both the 802.11 and the 802.15.4 networks. We observed that the performance of Silhouette Plot in both networks are qualitatively the same. We found that when the number of attackers equals to 2, i.e., two attackers masquerading the same identity in the network, the Silhouette Plot achieves both the highest Hit Rate, above 99 percent, and the highest F-measure value, over 95 percent. Further, the case of four attackers achieves the highest Precision above 99 percent, which indicates that the detection of the number of attackers is more accurate; however, the Hit Rate decreases to about 80 percent. Moreover, the Precision of the case of three attackers is lower than the cases of two and four attackers. This is because the cases of two attackers and four attackers are likely to be mistakenly determined as the case of three attackers. In general, our observation indicates that the Hit Rate decreases as the number of attackers increases. However, when the number of attackers increases, the adversaries also increase the probability to expose themselves. In the rest of our study, we will only present the results up to four attackers that masquerade the same node identity simultaneously.

4.3 System Evolution

4.3.1 Attacker Number Determination

The System Evolution is a new method to analyze cluster structures and estimate the number of clusters [32]. The System Evolution method uses the *twin-cluster* model, which are the two closest clusters (e.g., clusters a and b) among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy $E_p(K)$ denotes the border distance between the twin clusters, whereas the Merging Energy $E_m(K)$ is calculated as the average distance between elements in the border region of the twin clusters. The border region includes a number of sample points chosen from clusters a and b that are closer to its twin cluster than any other points within its own cluster. For instance, if cluster a contains total M_a sample points, in the twin-cluster model, a will be partitioned into $D_a = \frac{\sqrt{M_a}}{2}$ parts. Then, the number of sample points in the border region is defined as $n_a = \frac{M_a}{D_a}$. The same rule is carried out for its twin cluster b. Thus, we compute the Partition Energy $E_p(K)$ as

$$E_p(K) = \frac{1}{n_a + n_b} \left\{ \sum_{i=1}^{n_a} \min_{j=1,\ldots n_b} D\left(a_i, b_j\right) + \sum_{j=1}^{n_b} \min_{i=1,\ldots n_a} D\left(a_i, b_j\right) \right\}, \tag{21}$$

and the Merging Energy $E_m(K)$ as

$$E_m(K) = \frac{1}{\binom{n_a+n_b}{2}} \sum_{i=1}^{(n_a+n_b-1)} \sum_{j=i+1}^{(n_a+n_b)} D\left(\mathbf{s}_i, \mathbf{s_j}\right), \tag{22}$$

where $D(a_i, b_j)$ is the euclidean/Pearson distance between the elements a_i and b_j in clusters a and b, respectively. And $X\mathbf{s}_i, \mathbf{s}_j \in \{a_i\} \bigcup \{b_j\}$, which are the elements in the border region of the twin clusters.

The basic idea behind using the System Evolution method to determine the number of attackers is that all the rest of clusters are separated if the twin clusters are separable. Starting from the initial state with $K = 2$, the algorithm works with PAM by changing the number of clusters in a data set through the partitioning process $E_p(K) > E_m(K)$ and the merging process $E_m(K) \geq E_p(K)$ alternatively. The algorithm stops when it reaches a equilibrium state $K_{optimal}$, at which the optimal number of

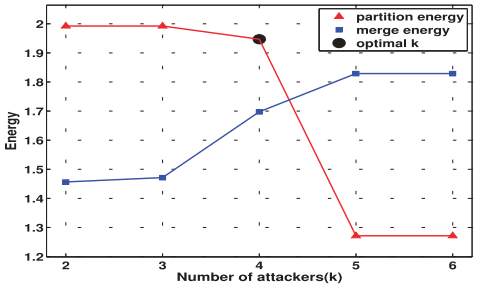


Fig. 9. System evolution: detection of four adversaries masquerading the same node identity.

clusters is found in the data set: $K_{optimal} = K$, if $E_p(K) > E_m(K)$ and $E_p(K+1) \leq E_m(K+1)$.

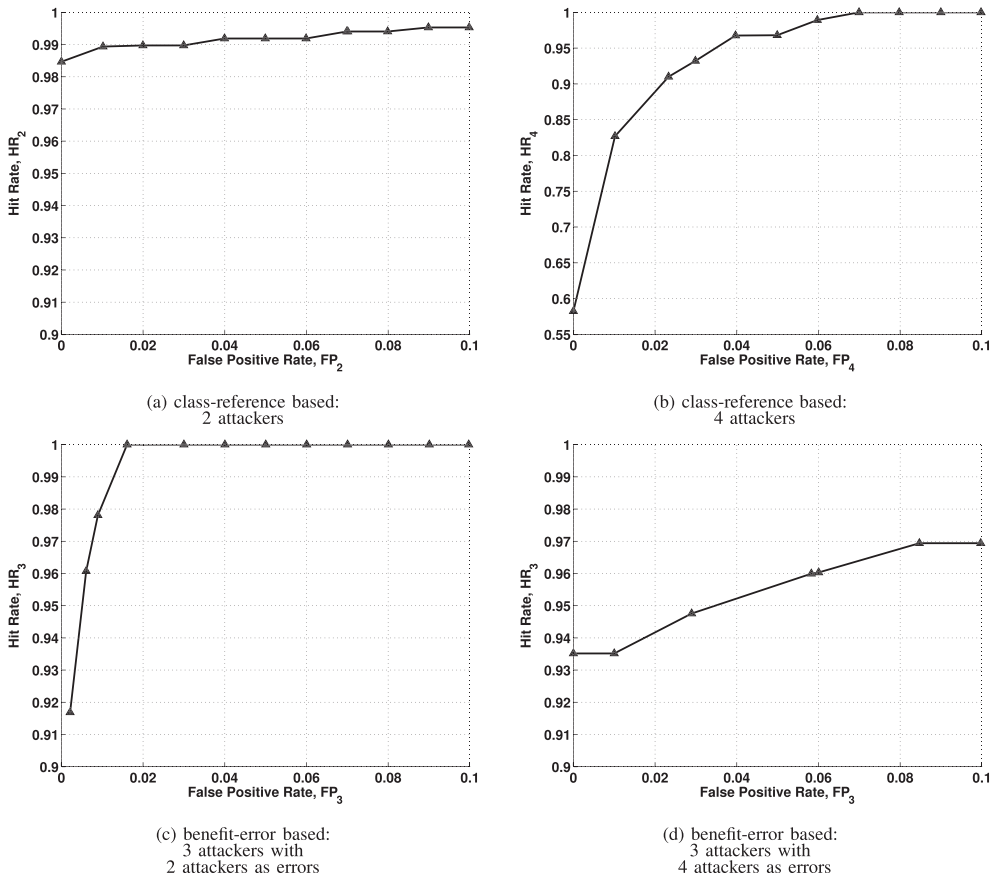
Fig. 9 presents an example of using the System Evolution method to determine the number of attackers in the 802.11 network. It shows the energy calculation versus the number of clusters. The $K_{optimal}$ is obtained when $K = 4$ with $E_p(4) > E_m(4)$ and $E_p(5) < E_m(5)$ indicating that there are four adversaries in the network using the same identity to perform spoofing attacks.

4.3.2 Experimental Evaluation

In this section, we show our study of System Evolution using multiclass ROC graphs. We perform threshold τ' testing on $E_p(K) - E_m(K)$. We can then obtain the number of attackers $K_{optimal}$ based on: $K_{optimal} = K$, if $E_p(K) - E_m(K) > \tau'$ and $E_p(K+1) - E_m(K+1) \leq \tau'$. Fig. 10 presents the multiclass ROC graphs using both the class-reference-based method (i.e., the cases of two and four attackers) and the benefit-error-based method (i.e., the case of three attackers) by varying the threshold τ'. Because of the overall higher Hit Rate under the 802.15.4 network, we only present the results of the 802.11 network in Fig. 10. By using the class-reference-based method, in Figs. 10a and 10b, we observed better performance of Hit Rate under the case of two attackers than the case of four attackers when the False Positive Rate decreases. Turning to examine the ROC graphs of the case of three attackers by using the benefit-error-based method as shown in Figs. 10c and 10d, we found that bounded by less than 10 percent False Positive Rate, the Hit Rate is lower when treating four attackers as errors than treating two attackers as errors. This indicates that the probability of misclassifying three attackers as four attackers is higher than that of misclassifying three attackers as two attackers.

4.4 The SILENCE Mechanism

The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters [32]. However, we observed that for both Silhouette Plot and System Evolution methods, the Hit Rate decreases as the number of attackers increases, although the Precision increases. This is because the clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions



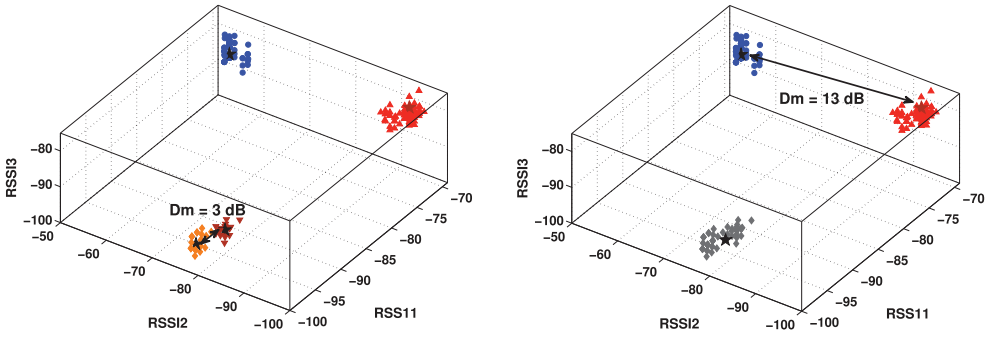
(a) class-reference based: 2 attackers

(b) class-reference based: 4 attackers

(c) benefit-error based: 3 attackers with 2 attackers as errors

(d) benefit-error based: 3 attackers with 4 attackers as errors

Fig. 10. System evolution in 802.11 network: multiclass receiver operating characteristic graphs of hit rate versus false positive.



(a) Silhouette Plot (b) System Evolution

Fig. 11. Illustration of the minimum cluster distance using cluster analysis methods under the case of three attackers.

and fake RSS clusters caused by outliers and variations of the signal strength. Fig. 11 illustrates such a situation where there are three attackers masquerading the same identity. Silhouette Plot returns the number of attackers $K_{sp} = 4$ as shown in Fig. 11a. We found that the minimum distance between two clusters in Silhouette Plot is very small because two clusters are actually from a single physical location. Further, Fig. 11b shows that System Evolution returns the number of attackers $K_{se} = 3$, the correct number of attackers, and the minimum distance between two clusters is large indicating that the clusters are from different physical locations.

Based on this observation, we developed *SILENCE*, testing SILhouette Plot and System EvolutioN with minimum distanCE of cluster, which evaluates the minimum distance between clusters on top of the pure cluster analysis to improve the accuracy of determining the number of attackers. The number of attackers K in SILENCE is thus determined by

$$K = \begin{cases} K_{sp} & \text{if } \mathrm{K}_{sp} = \mathrm{K}_{se}; \\ K_{sp} & \text{if } \min\left(\mathrm{D}_m^{obs}\right)_{\mathrm{K}_{sp}} > \min\left(\mathrm{D}_m^{obs}\right)_{\mathrm{K}_{se}}; \\ K_{se} & \text{if } \min\left(\mathrm{D}_m^{obs}\right)_{\mathrm{K}_{sp}} < \min\left(\mathrm{D}_m^{obs}\right)_{\mathrm{K}_{se}}, \end{cases} \tag{23}$$

where D_m^{obs} is the observed value of D_m between two clusters. SILENCE takes the advantage of both Silhouette Plot and System Evolution and further makes the judgment by checking the minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers. Hence, when applying SILENCE to the case shown in Fig. 11, SILENCE returns $K = 3$ as the number of attackers, which is the true positive in this example.

4.4.1 Experimental Evaluation

The effectiveness of using SILENCE to determine the number of attackers is presented in Table 3. And Fig. 12 presents the comparison of Hit Rate and F-measure of SILENCE to those of Silhouette Plot and System Evolution methods. The key observation is that there is a significant increase of Hit Rate for all the cases of the number of attackers under study. In particular, for the 802.11 network, the Hit Rate has increased from $89 \sim 92$ percent in Silhouette Plot and System Evolution to 98 percent using SILENCE for the case of three attackers and from 80-82 to 90 percent for the four attackers case. Whereas for the 802.15.4 network, the Hit Rate has increased from around 91-95 to 96 percent in SILENCE for the case of three attackers and from 84 to 88 percent for the four attackers case. Further, we observed that SILENCE has better performance over all the two, three, and four attackers in terms of F-measure. The overall improvement of F-measure is from 91 to 96 percent for 802.11 network, and from 92-93 to 95 percent for 802.15.4 network. Further, comparing with Silhouette Plot and System Evolution, the computational cost of SILENCE does not increase much. We experienced that SILENCE can determine the number of attackers within 1 second for each experimental run. These results demonstrate that SILENCE, a mechanism that combines minimum distance testing and cluster analysis together to perform multiclass attacker detection, is more effective than using techniques based on cluster analysis alone.

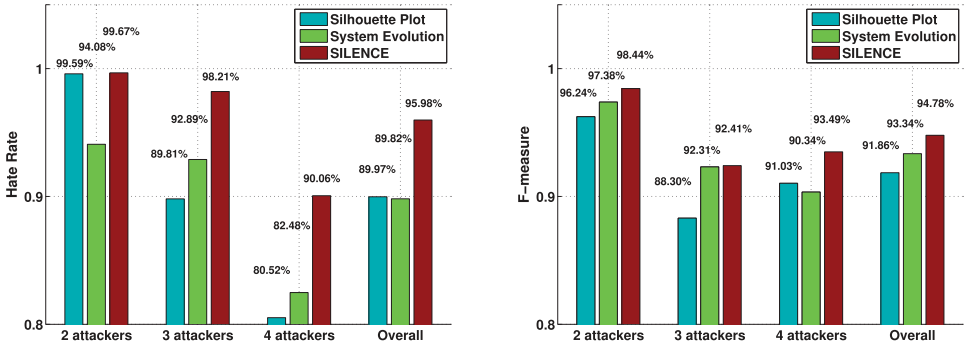
4.5 Support Vector Machines-Based Mechanism

Provided the training data collected during the offline training phase, we can further improve the performance of determining the number of spoofing attackers. In addition, given several statistic methods available to detect the number of attackers, such as *System Evolution* and *SILENCE*, we can combine the characteristics of these methods to achieve a higher detection rate. In this section, we explore using Support Vector Machines to classify the number of the spoofing attackers. The advantage of using SVM is that it can combine the intermediate results (i.e., features) from different statistic methods to build a model based on training data to accurately predict the number of attackers.

Particularly, SVM is a set of kernel-based learning methods for data classification, which involves a training phase and a testing phase [33]. Each data instance in the training set consists of a target value (i.e., class label) and several attributes (i.e., features). For example, for spoofing

TABLE 3
SILENCE: Hit Rate, Precision, and F-Measure

Number of Attackers	2	3	4
802.11 network, Hit Rate	99.67%	98.21%	90.06%
802.11 network, Precision	98.86%	91.42%	99.72%
802.11 network, F-measure	99.27%	94.69%	94.64%
802.15.4 network, Hit Rate	99.93%	96.04%	87.80%
802.15.4 network, Precision	96.99%	89.04%	99.96%
802.15.4 network, F-measure	98.44%	92.41%	93.49%



(d) 802.11: F-measure (d) 802.15.4: F-measure

Fig. 12. Hit Rate and F-measure comparison of SILENCE to methods using cluster analysis alone such as Silhouette and System Evolution.

detection, we can use a target value of "+1" to label the result if there are two attackers and a value of "−1" to label the result if the number of attackers is not 2. Furthermore, the features can be the difference of the partition energy and merge energy from System Evolution, or the minimum distance between two clusters from SILENCE, or the combination of them. The goal of SVM is to produce a model from the training set to predict the target value of data instances (i.e., the testing data).

The training data set can be obtained through regular network monitoring activities. Given a training set of instance-label pairs $(x_i; y_i); i = 1, \ldots l$, where $x_i \in R^n$ is the n dimension features and $y_i \in [+1, -1]$ is the label, the support vector machines require the solution of the following optimization problem [33]:

$$\begin{aligned} \min_{\mathbf{w},b,\xi} \quad & \frac{1}{2}\mathbf{w}^T\mathbf{w} + \mathcal{C}\sum_{i=1}^{l}\xi_i \\ \text{Subject to} \quad & y_i(\mathbf{w}^T\phi(x_i) + b) \geq 1 - \xi_i, \\ & \xi_i \geq 0. \end{aligned} \tag{24}$$

Its dual is

$$\begin{aligned} \min_{\alpha} \quad & \frac{1}{2}\alpha^T Q\alpha - \mathbf{e}^T\alpha \\ \text{Subject to} \quad & \mathbf{y}^T\alpha = 0, \\ & 0 \leq \alpha_i \leq C, \quad i = 1, \ldots, l, \end{aligned} \tag{25}$$

where $\mathbf{e}$ is the vector of all ones, Q is an l by l positive semidefinite matrix, $Q_{ij} = y_i y_j K(x_i, x_j)$, and $K(x_i, x_j) \equiv \phi(x_i)^T\phi(x_j)$ is called the kernel function. $\mathcal{C} > 0$ is the penalty parameter of the error term. The training vectors x_i are mapped into a higher dimensional space by the function ϕ. SVM then finds a linear separating hyperplane with the maximal margin in that higher dimensional space. Though several kernels are being proposed by researchers, we use the simple linear kernel for our testing [34]

$$K(x_i, x_j) = x_i^T x_j. \tag{26}$$

Furthermore, given a new instance x', the decision function on its label y' is given by

$$y' = \operatorname{sgn}\left(\sum_{i=1}^{l} y_i\alpha_i K(x_i, x') + b\right). \tag{27}$$

Since the classification of the number of attackers is a multiclass problem, the original binary SVM classifier needs to be extended to a multiclass classifier. In the literature, there are many approaches which can be used to combine the original binary SVM classifier to k-class classifiers [35], such as *one-against-all* and *one-against-one*. In our testing, we use the *one-against-one* method because it has shorter training time and better performance than *one-against-all* [36].

4.5.1 Experimental Evaluation

To validate the effectiveness of the SVM-based mechanism for determining the number of attackers, we randomly choose half of the data as training data, whereas the rest of data for testing. The features we used are the combination of the difference of partition energy and merge energy from System Evolution and the minimum distance between two clusters from SILENCE. Specifically, we used a feature set with 10 dimensions, five dimensions from the difference of partition energy and merge energy obtained from *System Evolution*, and the other five from the minimum distance between clusters. For example, the signal strength data have been partitioned multiple cluster sets (e.g., two, three, four, five, and six clusters, respectively). For each partition, we obtain one difference of partition energy and merge energy using *System Evolution* and one minimum distance between clusters. To evaluate the computational cost of the SVM-based method, we implemented SVM on the laptop equipped with 1 GHz CPU. We found that the online detection time using the SVM-based method is less than 1 ms.

Table 4 shows experimental results of using SVM-based mechanism when the attacker number $i = \{2, 3, 4\}$ for both the 802.11 and 802.15.4 networks. We observed that the performance of SVM in both networks are similar. We found that when the number of attackers equals to 2, the SVM-based

TABLE 4
SVM: Hit Rate, Precision, and F-Measure of Determining the Number of Attackers

Number of Attackers	2	3	4
802.11 network, Hit Rate	99.96%	99.07%	94.83%
802.11 network, Precision	99.10%	95.65%	99.92%
802.11 network, F-measure	99.52%	97.33%	97.31%
802.15.4 network, Hit Rate	99.99%	96.49%	92.41%
802.15.4 network, Precision	97.44%	92.86%	99.99%
802.15.4 network, F-measure	98.70%	94.64%	96.06%

method achieves the highest Hit Rate (above 99 percent) and the highest F-measure value, over 98 percent. Moreover, the case of four attackers achieves the highest Precision, above 99 percent, which indicates that the detection of the number of attackers is highly accurate; however, the Hit Rate decreases to about 90 percent.

By comparing the results of SVM to those of Silhouette Plot, System Evolution and SILENCE methods, we found that there is a significant increase of Hit Rate, Precision and F-measure for all the cases of the number of attackers under study. This is due to the facts that the SVM-based mechanism uses the training data to build a prediction model and it also takes the advantage of the combined features from two statistic methods. These results demonstrate that SVM-based mechanism, a classification approach that combines training data and different statistic features is more effective in performing multiclass attacker detection when multiple attackers are present in the system.

5 IDOL: Integrated Detection and Localization Framework

In this section, we present our integrated system that can both detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

5.1 Framework

The traditional localization approaches are based on averaged RSS from each node identity inputs to estimate the position of a node. However, in wireless spoofing attacks, the RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations. The traditional method of averaging RSS readings cannot differentiate RSS readings from different locations and thus is not feasible for localizing adversaries.

Different from traditional localization approaches, our integrated detection and localization system utilizes the RSS medoids returned from SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return positions from our system includes the location estimate of the original node and the attackers in the physical space.

Handling adversaries using different transmission power levels. An adversary may vary the transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately. We examine the pass loss equation that models the received power as a function of the distance to the landmark:

$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right), \qquad (28)$$

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. Further, we can express the difference of the received power between two landmarks, i and j, as

$$P(d_i) - P(d_j) = 10\gamma_i \log_{10}\left(\frac{d_i}{d_0}\right) - 10\gamma_j \log_{10}\left(\frac{d_j}{d_0}\right). \qquad (29)$$

Based on (29), we found that the difference of the corresponding received power between two different landmarks is independent of the transmission power levels. Thus, when an adversary residing at a physical location varies its transmission power to perform a spoofing attack, the difference of the RSS readings between two different landmarks from the adversary is a constant since the RSS readings are obtained from a single physical location. We can then utilize the difference of the medoids vectors in signal space obtained from SILENCE to localize adversaries.

5.2 Algorithms

In order to evaluate the generality of IDOL for localizing adversaries, we have chosen a set of representative localization algorithms ranging from nearest neighbor matching in signal space (RADAR [15]), to probability-based (Area-Based Probability (ABP) [16]), and to multilateration (Bayesian Networks (BN) [37]).

RADAR-gridded. The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from [15]. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR returns the x, y of the nearest neighbor in the signal map to the one to localize, where "nearest" is defined as the euclidean distance of RSS points in an N-dimensional signal space, where N is the number of landmarks.

Area-based probability. ABP also utilizes an interpolated signal map [16]. Further, the experimental area is divided into a regular grid of equal-sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector $\mathbf{s}$. ABP then computes the probability of the wireless device being at each tile L_i, with $i = 1 \ldots L$, on the floor using Bayes' rule:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})}. \qquad (30)$$

Given that the wireless node must be at exactly one tile satisfying $\sum_{i=1}^{L} P(L_i|\mathbf{s}) = 1$, ABP normalizes the probability and returns the most likely tiles/grids up to its confidence α.

Bayesian networks. BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization [37]. Fig. 13 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex s_i is the RSS reading from the ith landmark; and the vertex D_i represents the euclidean distance between the location specified by X and Y and the ith landmark. The value of s_i follows a signal propagation model $s_i = b_{0i} + b_{1i} \log D_i$, where b_{0i}, b_{1i} are the parameters specific to the ith landmark. The distance

$$D_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$$

in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a

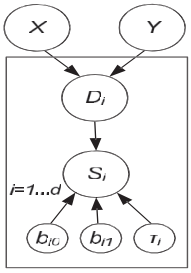


Fig. 13. Bayesian graphical model in our study.

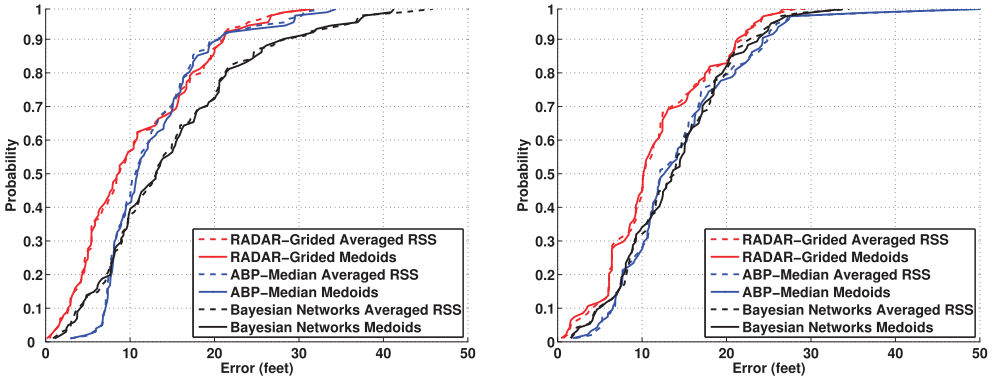
Gaussian distribution around the above propagation model, with variance τ_i: $s_i \sim N(b_{0i} + b_{1i} \log D_i, \tau_i)$. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

5.3 Experimental Evaluation

Fig. 14 presents the localization error CDF when using the returned RSS medoids from SILENCE and the averaged RSS, respectively, for RADAR-Gridded, ABP, and Bayesian Networks in two networks. We observed similar localization performance when using the returned RSS medoids to the traditional approaches using averaged RSS. Further, Fig. 15 presents the CDF of localization error of RADAR-Gridded and ABP when adversaries using different transmission power levels. To evaluate the performance of our approach by using the difference of returned medoids, three cases are presented in Fig. 15: 1) Adversaries used the same transmission power levels as the original node and the returned medoids are used; 2) Adversaries changed their transmission power level from 15 to 10 dB and the returned medoids are used; and 3) Adversaries changed their transmission power level from 15 to 10 dB and the difference of returned medoids are used. The key observation from Fig. 15 is that the performance of using the difference of returned medoids in handling adversaries using different transmission power levels is comparable to the results when adversaries used the same transmission power levels as the original node. Further, the localization performance is much worse than the traditional approaches if the difference of returned medoids is not used when localizing adversaries using different transmission power levels, shown as the case 2 above. In particular, when using our approach, we can achieve the median error of 13 feet for both RADAR-Gridded and ABP in case 3, a 40-50 percent performance improvement, comparing to the median errors of 20 and 19 feet for RADAR-Gridded and ABP, respectively, in case 2. Thus, IDOL is highly effective in localizing multiple adversaries with or without changing their transmission power levels.

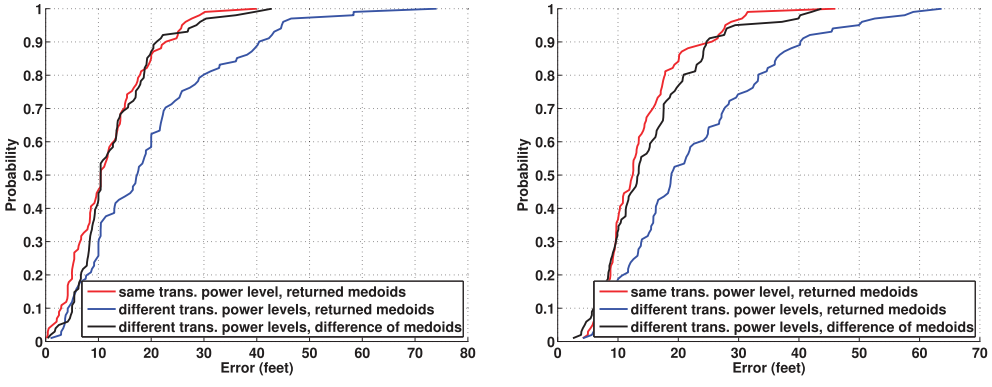
6 Conclusion

In this work, we proposed to use received signal strength-based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in



(a) 802.11 network (b) 802.15.4 network

Fig. 14. Comparison of localization errors between using medoids from cluster analysis and using averaged RSS.



(a) RADAR-Grided (b) ABP-Median

Fig. 15. Localization errors when adversaries using different transmission power levels.

wireless networks. We provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. We derived the test statistic based on the cluster analysis of RSS readings. Our approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. We developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution, that use cluster analysis alone. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system.

To validate our approach, we conducted experiments on two testbeds through both an 802.11network (WiFi) and an 802.15.4 (ZigBee) network in two real office building environments. We found that our detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98 percent and determining the number of adversaries, achieving over 90 percent hit rates and precision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

ACKNOWLEDGMENTS

This work is supported in part by the US National Science Foundation (NSF) Grants CNS-0954020, CCF-1018270. This work was done while J. Yang was at Stevens Institute of Technology.

REFERENCES

[1] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *Proc. USENIX Security Symp.,* pp. 15-28, 2003.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," *Proc. IEEE Wireless Comm. and Networking Conf.,* 2004.

[3] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," *Proc. ACM Workshop Wireless Security (WiSe),* Sept. 2006.

[4] Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks," *Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON),* 2006.

[5] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," *Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS),* 2005.

[6] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," *ACM/Springer Wireless Networks,* vol. 11, no. 6, pp. 677-686, 2005.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," *Proc. IEEE INFOCOM,* Apr. 2008.

[8] J. Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments," *Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),* 2009.

[9] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," *Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),* May 2007.

[10] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," *Proc. ACM Workshop Wireless Security (WiSe),* pp. 79-87, 2003.

[11] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," *Proc. IEEE Int'l Conf. Comm. (ICC),* pp. 4646-4651, June 2007.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," *Proc. 14th ACM Int'l Conf. Mobile Computing and Networking,* pp. 116-127, 2008.

[13] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," *Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection,* pp. 309-329, 2006.

[14] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," *Proc. IEEE INFOCOM,* pp. 2137-2145, 2008.

[15] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF-Based User Location and Tracking System," *Proc. IEEE INFOCOM,* 2000.

[16] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," *Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON),* Oct. 2004.

[17] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," *Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON),* Sept. 2006.

[18] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," *Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS),* Apr. 2008.

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

[20] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," *Proc. IEEE INFOCOM,* pp. 2396-2400, 2007.

[21] T. He, C. Huang, B. Blum, J.A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," *Proc. MobiCom '03,* 2003.

[22] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," *Proc. IEEE INFOCOM,* Apr. 2007.

[23] A. Goldsmith, *Wireless Communications: Principles and Practice.* Cambridge Univ. Press, 2005.

[24] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication," *IEEE Antennas and Propagation Magazine,* vol. 45, no. 3, pp. 51-82, June 2003.

[25] M. Abramowitz and I.A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables.* Courier Dover, 1965.

[26] L. Kaufman and P.J. Rousseeuw, *Finding Groups in Data: An Introduction to Cluster Analysis.* Wiley Series in Probability and Statistics, 1990.

[27] G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic, "Models and Solutions for Radio Irregularity in Wireless Sensor Networks," *ACM Trans. Sensor Networks,* vol. 2, pp. 221-262, 2006.

[28] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R.P. Martin, "The Robustness of Localization Algorithms to Signal Strength Attacks: A Comparative Study," *Proc. Int'l Conf. Distributed Computing in Sensor Systems (DCOSS),* pp. 546-563, June 2006.

[29] C. van Rijsbergen, *Information Retrieval,* second ed. Butterworths, 1979.

[30] T. Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters,* vol. 27, pp. 861-874, 2006.

[31] P. Rousseeuw, "Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis," *J. Computational and Applied Math.,* vol. 20, no. 1, pp. 53-65, Nov. 1987.

[32] K. Wang, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China, 2007.

[33] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods.* Cambridge Univ. Press, 2000.
[34] C.-C. Chang and C.-J. Lin, *LIBSVM: A Library for Support Vector Machines,* Software, http://www.csie.ntu.edu.tw/cjlin/libsvm, 2001.
[35] V. Franc and V. Hlavác, "Multi-Class Support Vector Machine," *Proc. Int'l Conf. Pattern Recognition (ICPR),* vol. 16, pp. 236-239, 2002.
[36] C. Hsu and C. Lin, "A Comparison of Methods for Multiclass Support Vector Machines," *IEEE Trans. Neural Networks,* vol. 13, no. 2, pp. 415-425, Mar. 2002.
[37] D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S. Krishnakumar, "Bayesian Indoor Positioning Systems," *Proc. IEEE INFOCOM,* pp. 324-331, Mar. 2005.

Jie Yang received the PhD degree in computer engineering from Stevens Institute of Technology in 2011. He is currently an assistant professor in the Department of Computer Science and Engineering at Oakland University. He was a postdoctoral fellow in the Data Analysis and Information Security (DAISY) Laboratory at Stevens Institute of Technology. His research interests include cyber security and privacy, mobile and pervasive computing, wireless localization systems, and mobile social networks. He is the recipient of the Best Paper Award from ACM International Conference on Mobile Computing and Networking (MobiCom) 2011 and the Outstanding Research Award in 2009 from Stevens Institute of Technology. His research has received wide press coverage including *MIT Technology Review*, *The Wall Street Journal*, CNET News, and Yahoo News. He is a student member of the IEEE.

Yingying (Jennifer) Chen received the PhD degree in computer science from Rutgers University. She is currently an associate professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests include cyber security and privacy, wireless and sensor networks, mobile social networks and pervasive computing. She has coauthored the book *Securing Emerging Wireless Systems* and published extensively in journal and conference papers. Prior to joining Stevens Institute of Technology, she was with Alcatel-Lucent. She received the IEEE Outstanding Contribution Award from IEEE New Jersey Coast Section each year 2005-2009. She is the recipient of the US National Science Foundation (NSF) CAREER award. She is the recipient of Google Research Award 2010 and the Best Paper Award from ACM International Conference on Mobile Computing and Networking (MobiCom) 2011. She is also the recipient of the Best Paper Award from the International Conference on Wireless On-demand Network Systems and Services (WONS) 2009, as well as the Best Technological Innovation Award from the International TinyOS Technology Exchange 2006. She is a senior member of the IEEE.

Wade Trappe received the BA degree in mathematics from the University of Texas at Austin in 1994 and the PhD 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. He is a member of the IEEE, the IEEE Signal Processing Society, the IEEE Communications Society, and the Association for Computing Machinery.

Jerry Cheng received the PhD degree in statistics from Rutgers University. He is currently an assistant professor in Robert Wood Johnson Medical School at the University of Medicine and Dentistry of New Jersey (UMDNJ). His research interests include data mining and learning, statistical modeling and data analysis, clustering analysis and algorithms, statistical applications in engineering, and biostatistics. Prior to the current position, he was a postdoctoral research scholar with the Department of Statistics at Columbia University.