Securing Wireless Networks against Multiple Spoofing Attacks

Shridevi A Desai, *Student, TJIT*, Shilpa MV, *Asst.Professor, TJIT*

***Abstract*—Wireless spoofing attacks can significantly impact the performance of networks as they are easy to launch. Though we can use cryptographic authentication for verifying the identity of the node, conventional securities approaches are not desirable because of their overhead requirements. In this paper we propose to use physical properties associated with the node which is hard to falsify and reliant on cryptography, as the bases for detecting spoofing attacks, determining the number of attackers when there are multiple adversaries attacking as the same node entity. We propose to use the unique key generated using hashing algorithm for wireless nodes to detect the spoofing attacks. Cluster based mechanisms are used to determine the number of attackers. Our detection results using a representative set of algorithms provides a strong evidence of high accuracy of localizing multiple adversaries.**

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

1 Introduction

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network.

The traditional approach to address spoofing 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 addition, key management often incurs significant human management costs on the network. In this paper, we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, we propose a scheme for both detecting spoofing attacks, as well as

localizing the positions of the adversaries performing the attacks.Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.

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: 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.

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. 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. 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.

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. Finally, we conclude our work in Section 5.

2 LITERATURE SURVEY

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, adhoc 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.

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. 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. Whereas range-free algorithm 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 use a function that maps observed radio properties to locations on a preconstructed signal map or database. Further, Chen et al 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 (GADE)

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 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 ¼ 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 determining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias [27].

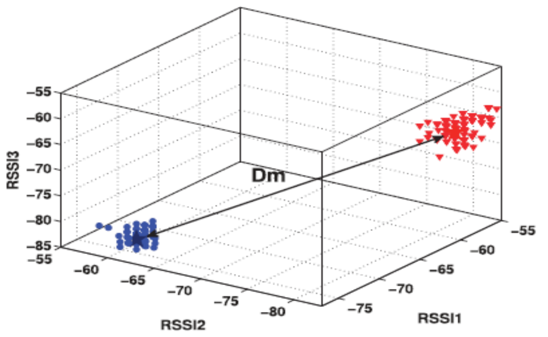


Fig.1 Illustration of RSS readings from two physical locations

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 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 Dm as the test statistic T in our significance testing for spoofing detection,

$$D_m = \|M_i - M_j\|$$

where Mi and Mj are the medoids of two clusters. Under normal conditions, the test statistic Dm 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 Dm will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space.

3.2 Results of Attack Detection

3.2.1 Impact of Threshold and Sampling Number

The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a threshold _ enables the attack detector to be robust to false detections. Fig. 5 shows the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. We observed that the curve of Dm shifted greatly to the right under spoofing attacks. Thus, when Dm > _,we can declare the presence of a spoofing attack. The short lines across the CDF lines are the averaged variances of Dm 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 _ 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 Dm is, the more robust the detection mechanism can be. Therefore, there is a tradeoff between the 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.

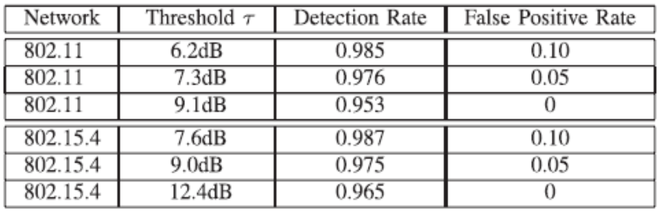
3.2.2 Handling Different Transmission Power Levels

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., Dm 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 Dm is larger than normal conditions. Fig. 5b presents an example of the Cumulative Distribution Function of the Dm 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 Dm under the different transmission power level shifts to the right indicating larger Dm values. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

3.2.3 Performance of Detection

To evaluate the effectiveness of using cluster analysis for attack detection, Fig. 6 presents the Receiver Operating Characteristic curves of using Dm 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 _ 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.

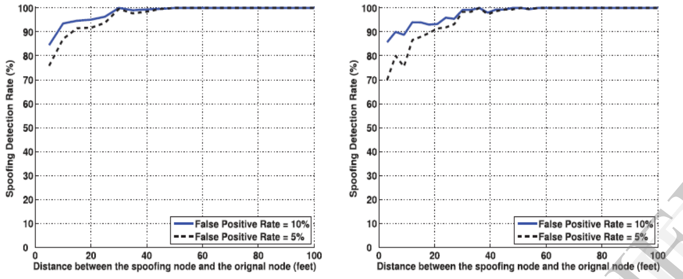
Table 1
Detection Rate and False Positive Rate in Two Networks



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

3.2.4 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. 2 presents the detection rate as a function of the distance between the spoofing node Pspoof and the original node Porg. We found that the further away Pspoof is from Porg, 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 Pspoof is about 15 feet away from Porg when the false positive rate is 5 percent. While for the 802.15.4 network



(a) 802.11 network (b) 802.15.4 network

Fig.2 The detection rate as a function of the distance between the spoofing node and the original node.

the detection rate is above 90 percent when the distance between Pspoof and Porg 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 Pspoof moves closer to Porg, 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 ci=3, we define Pi as the positive class of ci and all other classes (i.e., all other number of attackers) as negative class Ni

$$P_i = c_i,$$

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

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

$$HR_i = \frac{N_{true}}{P_i}$$

Where Ntrue is the true positive detection of class ci. Let Nfalse be the false detection of the class ci out of the negative class Ni that do not have i number of attackers. We then define the false positive rate FPi for a specific number of attackers of class ci as FPi=Ntrue/Ni. Then, the Precision is defined as

$$Precision_i = \frac{N_{true}}{N_{true} + N_{false}}$$

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]

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

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 *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*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 System Evolution

4.2.1 Attacker Number Determination

The System Evolution is a new method to analyze cluster structures and estimate the number of clusters . 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 $E_m(K)$ 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=M_a/2 parts. Then, the number of sample points in the border region is defined as n_a=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

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

and the Merging Energy as

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

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 $Xs_i,s_j€\{a_i\}\{b_j\}$, 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 $E_p(k) \geq E_m(K)$ alternatively. The algorithm stops when it reaches a equilibrium state $K_{optimal}$, at which the optimal number of clusters is found in the data set: $K_{optimal}$=k, if $E_p(k)>E_m(k)$ and $E_p(k+1)<E_m(k+1)$.

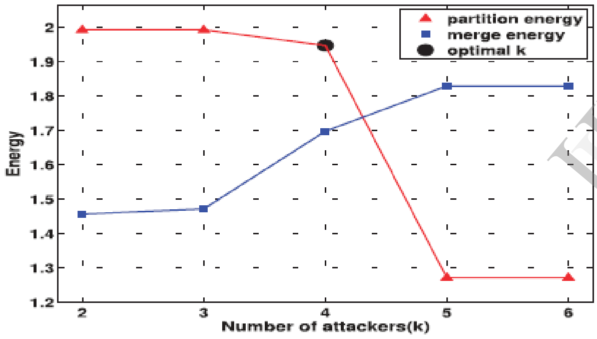


Fig 3.Detection of four advarsaries masquerading the same node

Fig. 3 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 $E_p(4) > E_m(5)$ and $E_p(5) < E_m(5)$ indicating that there are four adversaries in the network using the same identity to perform spoofing attacks.

5 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 wireless networks. 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. 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.

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.

REFERENCES

[1] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. USENIX Security

[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 RFBased 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.