ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Spoofing Attack Detection and Localization in Adhoc network using Received Signal Strength (RSS)

Mr. Mukesh Barapatre[1], Prof. Vikrant Chole[2]

Department of CSE, GHRAET, Nagpur (M.S), India[1]

Department of CSE, GHRAET, Nagpur (M.S), India[2]

Abstract: **-** A wireless ad hoc network is formed by a collection of nodes, with no preset infrastructure where each node plays a role of router, It is recognition day by day due to wide use of mobile and handheld devices. Due to dynamic nature of this network, Device identity is perhaps one of the most potential challenges in any network security solution. Wireless networks are unarmed to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities. a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. identity of a node can be confirmed through cryptographic security, traditional security approaches are not always desirable. we propose to use spatial information, a physical property of each node, so hard to falsify or alter fraudulently. and not depend on on cryptographic security, on the beginning for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple node pretend as a same node identity, and (3) localizing multiple adversaries. We propose to use the correlation between a signal's spatial direction and the average received signal gain of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks, It conveys the problem of determining the number of attackers as a multi-class detection problem. Clustering based mechanisms are developed to determine the number of attackers. In this paper enlist the method of spoofing attack detection using spatial correlation between wireless nodes. And cluster based mechanisms to determine the number of attakers in network. We evaluated techniques through two wireless adhoc networks using both an 802.15.4 (ZigBee) network with static and dynamic network wireless network .

Keywords*:* Wireless network security, spoofing , attack detection, localization.

I. INTRODUCTION

A wireless ad hoc network is one of self aligning fastest emerging, technology, due to beginning of cheap, small & more demanding wireless devices. It is being used by most of the users, ranging from military to civilian. Device identity is perhaps one of the most probable challenges in any network security solution. Localizing node is necessary for many higher level network functions such as tracking, monitoring and geometric-based routing and can be used in broad areas . It is easy to attack MAC addresses in IEEE 802.11 wireless network using publicly available tools ,It is possible to implement many 802.11 attacks with easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. example, an attacker can masquerade as a legitimate access point to disrupt network connections such as attacks on access control lists, access point attacks, and Denial-of-Service (DoS) attacks, or to advertise false services to nearby wireless stations,

Therefore, it is important to

- detect the presence of spoofer in wireless network,
- determine the number of attackers, and
- find location of multiple challengers

The traditional approach is to use authentication application to address spoofing attacks. However, authentication requires additional infrastructural overhead and computational power associated with allocating, and maintaining cryptographic keys[6]. Because of the limited power and resources available to the wireless devices and sensor nodes, it is not possible to deploy authentication each time. In addition, key management often require significant human management costs on the network. In this paper,[1][2] we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. For that we propose a scheme for both detecting spoofing attacks, as well as 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 attack detection and localization. Our scheme does not add any workload to the wireless devices. By examining the RSS from each MAC address using cluster algorithm, we have found that the space between the access point in signal space is a good test for effective attack detection. Since we are worried with attackers who have different locations than valid wireless nodes, utilizing spatial information to express spoofing attacks has the unique power to not only recognize the presence of these attacks but also locate adversaries[2][3]. An advantage of using spatial correlation to sense spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves

We focus on static nodes and dynamic node in this work that are common for spoofing scenarios [8].

We addressed spoofing detection in dynamic environments in our work . The works that are closely cor1related to us are [3], [8], [9]. Faria and Cheriton [4] proposed the use of matching rules of signal prints for spoofing detection, Jie Yang et al.[1], Sheng et al. [8] demonstrated the RSS readings and Chen et al. [9] used RSS plus K-means cluster analysis to detect spoofing attacks..

II. Related Work

There are number of benefits of using wireless Adhoc networks which are based on 802.11 and above standard. Which can be widely used in the military and industrial sectors as well as in education . But, the usage of these access is expected on the basis of availability and confidentiality notion. The 802.11 is capable to maintain the privacy in the data which is to be transmitted. However The 802.11 is susceptible to many attacks at high degree that target to the MAC and its management[5]. Jie Yang, Yingying (Jennifer) Chen and Wade Trappe introduce use of received signal strength(RSS) spatial correlation of wireless nodes to detetect the spoofing attacks[1]. Then, By using Cluster-based mechanisms they determine the number of attackers. Training data sets are discover using the SVM (Support Vector Machines) to further improve the correctness of determining the count of attackers[15]. they build the an IDOL (integrated detection and localization system that can localize the positions of multiple attackers)[1].

A. Overview of RSS

To learn Received Signal Strength (RSS) is a property that are closely associated with position in network space and is freely available in the existing wireless networks[3][4]. The RSS readings at the identical physical space are similar, whereas the RSS readings at dissimilar locations in physical space are distinct. Thus, the RSS readings existent strong spatial correlation characteristics. The Received Signal Strength value array as s = (s1, s2,...sn) where n is the number of landmarks that are watching the RSS of the wireless nodes and know their locations in wireless network grid. Usually, the RSS reading at the ith landmark from a wireless node is dispersed as

$$Si\,(dj)\,[dBm] = P\,(d0)\,[dBm] - 10\Upsilon \log\,(dj/d0) + Xi$$

where P(d0) represents the transmitting power of the node at the local distance d0, ϒ the path loss exponent and, dj is the distance between the wireless node j and the ith landmark, Xi is the shadow fading which is given as input. For simplicity, the nodes have the same transmission power. If the RSS does not match in consecutive RSS values, then the node is said to be malicious[1].

B. Attack Detection Using Cluster Analysis

Spoofing attack detection in wireless adhoc network uses the RSS-based spatial correlation inherited from wireless. RSS readings from a wireless node may oscillate and should grouped together. In precise,the RSS reading belong to same cluster points in n-dimensional signal space from the same physical location over the time,different clusters is formed in signal space for RSS readings from different positions over time. In Fig. 1, represents RSS reading vectors of three different landmarks (n = 3) from two different physical positions. In case of spoofing attack, the legal and the attacker are using the same ID to transfer data packets, and the RSS readings of that ID is the fusion readings measured from each individual node (i.e., spoofing node or victim node). Since in a spoofing attack, the RSS readings from the legal node and the spoofing attackers are mixed together, that suggests we may conduct cluster analysis on the RSS-based spatial correlation to discover the distance in signal space and further detect the occurrence of spoofing attackers in network space. In this work, they use the Partitioning Around Medoids technique to perform clustering analysis in RSS. The PAM Method [18] is a popular descent clustering algorithm. the PAM clustering algo is more robust in the presence of noise and outliers. Thus, the PAM method is more suitable in defining clusters from RSS redings

Thus express spoofing detection as a statistical significance testing problem, the null supposition is

H0 : normal (no spoofing attack).

In testing[1], a test statistic Tis used to calculate whether detected data belong to the null-hypothesis or not.

in attack detection , we partition the RSS vectors from the same node identity into two clusters (i.e., K = 2) doesn't matter how many attackers are use this identity, We then pick the distance between two medoids Dm as the test statistic T in our testing for spoofing detection, Dm = ||Mi _Mj||, where Mi and Mj are the medoids of two clusters.

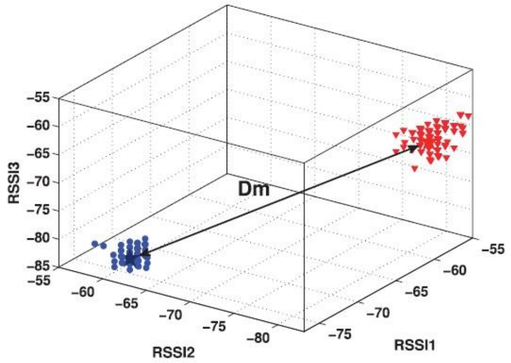


Fig 1 : Illustration of RSS readings from two physical locations.

III. Proposed Work

The proposed system effort is inspired from amending the limitations of earlier systems. In specific, the new system proposes a scheme in which the nodes are static as well as dynamic ad hoc network node. A reputation-based trust management scheme is designed to enable fast detection of attacker nodes. The main idea of the scheme is to detect Spoofers in wireless ad hoc network using Radio Signal Strength (RSS) ,

The proposed System are a GENERALIZED ATTACK DETECTION AND LOCALIZATION

MODEL(GADLM) that can used to detect spoofing attacks as well as determine the number of attacker using cluster analysis methods based on RSS-based spatial information among normal devices and attackers; and localization system that can both detect attacks as well as find the positions of multiple spoofers even when the node vary their transmission power levels. In GADLM, the Partitioning Around Medoids and k means cluster analysis method is used to perform attack detection.We formulate the problem of defining the number of attackers as a multiclass detection problem. We then used cluster-based methods to determine the number of attacker.

We developed mechanism for System Evolution with minimum distance of clusters, to improve the correctness of detection of the number of attackers. Additionally,,if the training data are available, we try to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.we demonstrated through our experiments using both an 802.15.4 (ZigBee Static) network as well as an 802.15.4 (ZigBee Dynamic) network simulator, for simulation of network we use ns2 (network simulator) GADLM is highly effective in spoofing detection with over 80-90 percent hit rate and precision. Furthermore, we can achieve similar localization accuracy.

A. Genralized Attack Detection and Localization

In GADLM, we use RSS readings of node for cluster analysis method which is used to perform attack detection in wireless ad hoc network. We develop the system for determining the number of attackers using cluster-based mechanism.

-To identify the locations of multiple adversaries even when the challengers differ their transmission power levels. The main contribution of the paper is organized areas follows:

- To successfully detect the presence of spoofing attack
- To compute the number of attackers

-To recognize the position of multiple challengers in the network

- To deliver solution to detect adversaries in the network where in there is no additional cost or modification to the wireless devices themselves
- To remove or overcome traditional approach of authentication key management
- To remove overhead from the network devices .

In GADLM, we present our integrated system that can find spoofing attacks, count the number of attackers, and locate the spoofers. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

B. Spoofing Attack Detection

In this [1][2], Spoofing Attack detection is discovered. Received Signal Strength (RSS) is a property that are closely associated with position in network space and is freely available in the existing wireless networks.

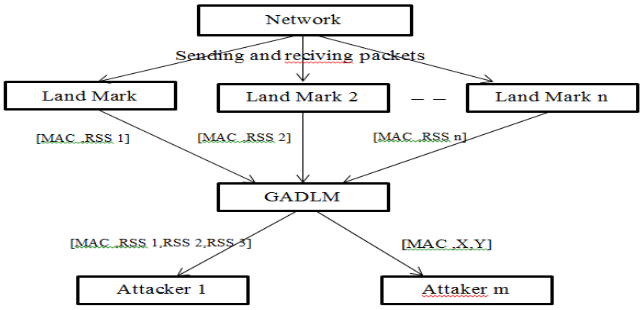


Fig.2 Genralized Attack Detection and Localization system architecture

The Received Signal Strength value array as s = (s1, s2,...sn) where n is the number of landmarks that are watching the RSS of the wireless nodes and know their locations in wireless network grid. Usually, the RSS reading at the ith landmark from a wireless node is dispersed as

$$Si\ (dj)\ [dBm] = P\ (d0)\ [dBm] - 10\Upsilon \log\ (dj/d0) + Xi$$

where P(d0) represents the transmitting power of the node at the local distance d0, ϒ the path loss exponent and, dj is the distance between the wireless node j and the ith landmark, Xi is the shadow fading which is given as input[1]. For simplicity, the nodes have the same transmission power in static network. If the RSS does not match in consecutive RSS values, then the node is said to be malicious.

The old-style localization methodologies are based on averaged RSS from each node characteristics inputs to estimate the position of a node. But, in wireless spoofing attacks, the received signal strength (RSS) of a node identity may be mixed with RSS readings of both the unique node as well as spoofing nodes from dissimilar physical locations(i.e. , dynamic network) due to moving nodes in adhoc network. The old method of averaging RSS readings cannot distinguish RSS readings from different physical locations and thus is not realistic for localizing adversaries in dynamic topology. Different from outdated localization methods, our detection and localization system utilizes the RSS medoids returned from cluster analysis as inputs to localization algorithms to estimate the positions of opponents in dynamic network. Handling adversaries using different transmission power levels. An adversary may vary the transmission power levels when executing spoofing attacks so that the localization system cannot compute its location accurately.

C. Handling challengers using different transmission power levels.

An competitor may change the transmission power levels when executing spoofing attacks so that the localization system cannot detect its location perfectly with the help of neigbour discovery algorithms. Jie Yang, Yingying (Jennifer) Chen and Wade Trappe[1] introduce the pass loss equation that models the received power as a function of the distance to node and landmark:

$$P(d)[dBm] = P(d0)[dBm] - 10\Upsilon \log10(d/d0)$$

where *d* is the distance between the transmitting node and the access points(landmark), P(*d0*) represents the transmitting power of a node at the local distance *d0*, and ϒ is the path loss exponent.in Advance, we can express the difference of the received power between two landmarks i and landmark j as

P(*di*) – P(*dj*) = 10ϒilog10(*di/do*) -10ϒjlog10(*dj/do*).

Based on, we notice that the difference of the received power among two different landmarks is free of the transmission power levels. Thus, when an adversary located at a physical location differs its transmission power to achieve a spoofing attack, the change of the RSS readings between two different landmarks from the challenger is a constant meanwhile the RSS readings are achieved from a single physical location.

D. Localization

In order to calculate the overview of GADLM for localizing adversaries,we have chosen a representative localization algorithms we use nearest neighbor matching in signal space[15], Given an observed RSS reading with an unknown location, nearest neighbor search the x, y of the nearest neighbor in the signal map to the one to localize, where “nearest” is well-defined as the euclidean distance of RSS readings of node in an N-dimensional signal space, where N is the number of access point (landmarks). In this module, all 28 the nodes are computing the neighbor nodes with their transmission range with the help of landmarks. Then it gives the position of node i.e., its position to all of its neighbors. It happens for all the nodes at regular intervals. Andlast it give the position of spoofing node in 2 dimentional space (i.e., in x, y axis).

IV. SYSTEM IMPLEMENTATION

A. Simulation Enviroment

For the network simulation of proposed work we use the latest version of NS-2 has been used, **network simulator** is a name for series of distinct event network simulators, like ns-1, ns-2 and ns-3. All of them are network simulator, largely used in research[4] and teaching. ns-2 is open source software publicly available under the GNU GPLv2 license for research, development, and use[20].

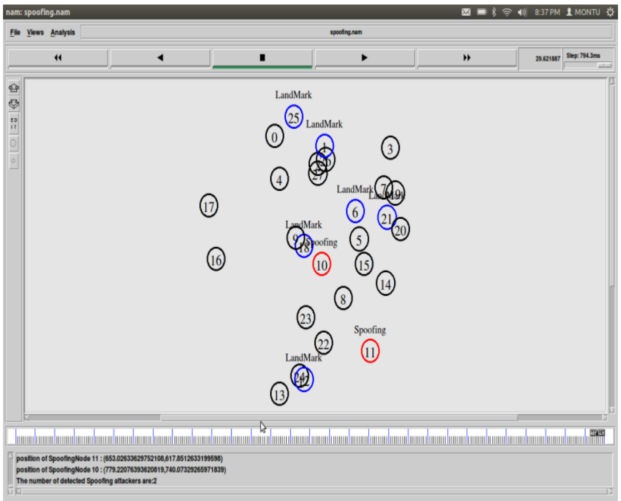
B . Simulation Parameters

For Simulation we have to set no of parameter according to network ,There are number of simulation parameters which can be varied, change in value of different performance metrics[20], which can be shown in below table.

TABLE I Simulation Parameter

Sr. No.	Parameter	Value
1	Simulator	NS-2 (Version 2.35)
2	Channel type	Channel/Wireless Channel
3	Radio Propagation Model	Propagation/TwoRay Ground
4	Network interface type	Phy/WirelessPhy/ 802_15_4
5	MAC Type	Mac/802_15_4
6	Interface queueType	Queue/DropTail/ PriQueue
7	Traffic Type	CBR
8	Antenna	Antenna/ OmniAntenna
9	Maximum packet	100
10	Area (M*M)	1000*800
11	Simulation Time	30.0 Sec
12	No of Nodes	28
13	Routing Protocol	AODV

Performance of GADLM System in wireless ad hoc can be realized by running the simulation, the fig 3. Show the output of wireless adhoc network (ZigBee) there are 28 node in the network grid which is set in1000*800m, and moving randomly each node is capable of transmitting data and forming network. Genralized Attack detection and Localization model illustrate the random no of landmark which are used to initiate the transmission and calculate the RSS reading for each neighboring nodes .then it return the count of spoofing node in network and location of node .

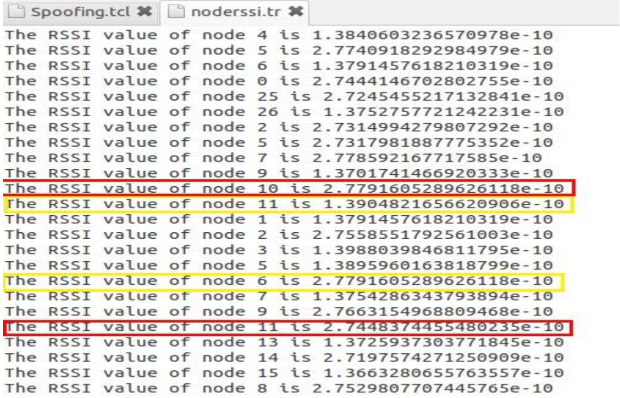


```
position of SpoofingNode 11 : (653.02633629752108,617.8512633199598)
position of SpoofingNode 10 : (779.22076393620819,740.07329265971839)
The number of detected Spoofing attackers are:2
```

Fig.3. Ns2 Simulation Result for wireless adhoc network.

RSS reading of node is calculate through landmarks, which provides the data for k-mean clustering algorithm which is used to detect no of spoofing node,and the by using localization system find out the position of spoofing node.the RSS ID of node is calculate from that data we can easily find out the possible spoofers which can be illustrate in following fig. 4.

Performance of System in wireless environment can be realized by computable study of values of different metrics used to compute performance of system which are as follows.



```
The RSSI value of node 4 is 1.3840603236570978e-10
The RSSI value of node 5 is 2.7740918292984979e-10
The RSSI value of node 6 is 1.3791457618210319e-10
The RSSI value of node 0 is 2.7444146702802755e-10
The RSSI value of node 25 is 2.7245455217132841e-10
The RSSI value of node 26 is 1.3752757721242231e-10
The RSSI value of node 2 is 2.7314994279807292e-10
The RSSI value of node 5 is 2.7317981887775352e-10
The RSSI value of node 7 is 2.778592167717585e-10
The RSSI value of node 9 is 1.3701741466920333e-10
The RSSI value of node 10 is 2.7791605289626118e-10
The RSSI value of node 11 is 1.3904821656620906e-10
The RSSI value of node 1 is 1.3791457618210319e-10
The RSSI value of node 2 is 2.7558551792561003e-10
The RSSI value of node 3 is 1.3988039846811795e-10
The RSSI value of node 5 is 1.3895960163818799e-10
The RSSI value of node 6 is 2.7791605289626118e-10
The RSSI value of node 7 is 1.3754286343793894e-10
The RSSI value of node 9 is 2.7663154968809468e-10
The RSSI value of node 11 is 2.7448374455480235e-10
The RSSI value of node 13 is 1.3725937303771845e-10
The RSSI value of node 14 is 2.7197574271250909e-10
The RSSI value of node 15 is 1.3663280655763557e-10
The RSSI value of node 8 is 2.7529807707445765e-10
```

Fig.4. RSS Reading of node,red indicate the Spoofing RSS ID from yellow node.

- Average end-to-end delay

It is average time taken by packets to move from source to destination across a adhoc network. This consist of all possible delays caused queuing at the interface queue ,route discovery latency, and retransmission time taken at the MAC, propagation and transfer times.The lower value means the better performance of the protocol [13].

End to end delay = ∑ (arrive time - send time)

- Packet Loss

It is the number of packets fallen by nodes due to numerous reasons. The lower value of the packet lost means the better performance of the system.

Packet lost = No of packet send – No of packet received.

- Network Throughput

The number of packets sent from source to destination per unit of timeis called Throughput .

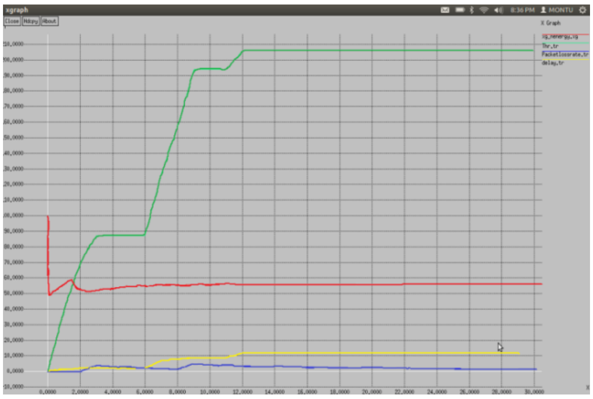


Fig. 5. Throughput Packetloss rate,end to end delay,energy graph of GADLM

From above graph we can say that value of throughput is increasing linearly from starting for network as well as PDR values for System is low as possible and constant after some time.similarly energy and packet loss is minimum through out the simulation.

V. Conclution

This scheme offered to use received signal strength(RSS)-based spatial correlation a physical property of each wireless device that is hard to forge and not dependent on cryptography as the source for noticing spoofing attacks in wireless networks. It provided theoretical analysis of using the RSS received signal strength readings for attack detection, inherited from wireless nodes. The method can both detects the existence of attacks as well as define the number of challengers, spoofing the same node identity that can locate any number of attackers.

VI. Future Work

Our future work will primarily concentrate on to analyze & study system on the context of wireless environment and to estimate deviation in its performance after put on our detection & Localization mechanism by bearing in mind other performance metrics also...\

References

[1] Jie Yang, Yingying (Jennifer) Chen and Wade Trappe, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE Transection on parallel and distributed system, Vol.24, NO. 1, January 2013.

[2] Bellardo and S. Savage ,“ 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, Proc. USENIX Security Symp., pp. 15- 28, August 2003

[3] 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

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

[5] 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

[6] 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.

[7] 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.

[8] 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.

[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] 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.

[11] 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

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

[13] 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.

[14] 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.

[15] 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.

[16] K. Wang, “Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data,” Technical Report NO. 2007

[17] N. Cristianini and J. Shawe-Taylor, An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods. Cambridge Univ. Press, 2000.

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

[19] P. Bahl and V.N. Padmanabhan, “RADAR: An in-Building RFBased User Location and Tracking System,” Proc. IEEE INFOCOM, 2000.

[20] NS-2, The ns Manual (formally known as NS Documentation) available at http: //www. isi.edu/nsnam/ ns/do