Cluster-Based Intrusion Detection Technique for Wireless Networks

Mr. P.Sundara Vadivel
Assistant Professor Computer Science and Engineering, Department of Computer Science, Bharath Niketan Engineering College,
Email:sundar.be2005@rediffmail.com

Mr. J. Senthil Kumar
Assistant Professor Information Technology, Department of Computer Science, Bharath Niketan Engineering College,
Email: ssasenthils@gmail.com

Mr. M.Sudharsanan
Department of Computer Science, Bharath Niketan Engineering College
Email: m.sudharsanan@gmail.com

Abstract - Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. In this paper we propose a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks. 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 test beds using both an 802.11 (Wi-Fi) network and an 802.15.4 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.

Keywords: *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 the 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. Spoofing attacks can further facilitate a variety of traffic injection attacks, 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. 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 detect the presence of spoofing attacks, Determine the number of attackers, and Localize multiple adversaries and eliminate them. Most existing approaches to address potential spoofing attacks employ cryptographic schemes. 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.

2. Related Work

The traditional approach to prevent attacks is to use cryptographic-based authentication. Wu et al. 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 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. However, the crypto-graphic 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 decor relates 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. Brik et al. 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 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 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 using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton proposed the use of matching rules of signal prints for spoofing detection. Sheng et al. modeled the RSS readings using a Gaussian mixture model. Sang and Arora 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 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 land-marks using the measurement of various physical properties such as RSS, Time Of Arrival (TOA), Time Difference Of Arrival (TDOA), and direction of arrival (DoA). Whereas range-free algorithms use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Literation approaches 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 reconstructed signal map or database. Further, Chen et al. proposed to perform detection of attacks on wireless localization and Yang et al. proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, I 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 I use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Further-more, 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

Generalized Attack Detection Model (GADE), consists of two phases: attack detection, which detects the presence of an attack, and number determination, which determines the number of adversaries.

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 transmitters Physical location and is governed by the distance to the landmarks. 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 ass={s1…s2..sn} 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 lognormal distributed we next study the detection power of our approach by using the RSS-based spatial correlation. Presents the numerical results of receiver operating characteristic (ROC) Curves based 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 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 no centrality parameter , which is represented by the distance between two wireless nodes together with the landmark

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 which presents RSS reading vectors of three landmarks 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.

The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method, 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

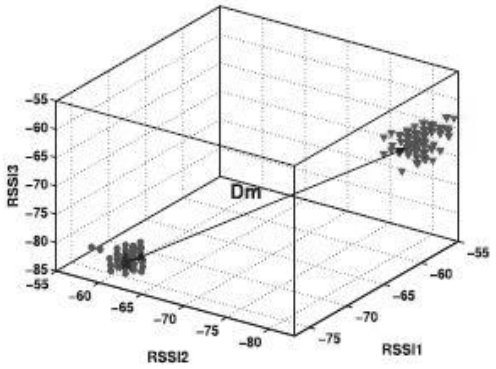

Illustration of RSS readings from two physical locations.

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 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 _ 169 ft and 200 ft _ 80 ft, respectively. 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 . We note that the deployment of landmarks has important impact on the detection performance, which is similar to the wireless localization . Each landmark is a Linux machine equipped with a Atheros mini PCI 802.11 wireless card and a T mote Sky mote so as to measure the RSS readings from both Wi-Fi 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 teststhrough all the possible combinations of testing points for cases of two, three, and four attackers masquerading as a single node identity. In

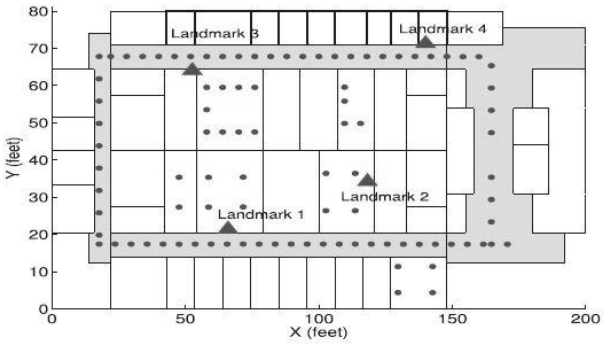

Fig 3.3 Cluster Formation

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.

4. Determining the number of attackers

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. Since it is not known that how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS readings

4.1 Results of Attack Detection

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. shows the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. 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.

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 . We varied transmission power for an attacker from 30 m We found that in all cases Dm is larger than normal Conditions 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.

4.3 Performance of Detection

To evaluate the effectiveness of using cluster analysis for attack detection, Fig. 6 presents the Receiver Operating Characteristic curves using as a test statistic to perform attack detection for both the 802.11 and the 802.15.4 networks. 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

5. IDOL: Integrated detection and localization framework

Integrated systems that can detect spoofing attacks, determine the number of attackers, and localize multiple adversaries.

5.1 Algorithms

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

5.2 RADAR-gridded.

The RADAR-Gridded algorithm is a scene-matching localization algorithm extended. 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 . 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 s. ABP then computes the probability of the wireless device being at each tile Li, with i =.1……L, on the floor using

Bayes' rule:

$$P(Li|s) = P(s|Li) * p(Li) / P(s)$$

Normalizes the probability and returns the most likely tiles/grids up to its confidence α

5.3Bayesian networks:

BN localization is a multi-literation algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex is the RSS reading from the I landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the landmark. The value of follows a signal propagation model,

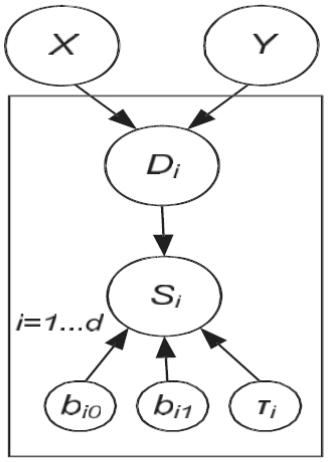

Fig 5.3 Bayesian vertex x and y

where are the parameters specific to the landmark.

6. PROPOSED MODULES:

- Handling Different Transmission
- Performance of detection
- The Number of Attackers
- Attacker Number Determination
- The silence mechanism

6.1HANDLING DIFFERENT TRANSMISSIONS

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.

6.2 PERFORMANCE OF DETECTIONS

The cluster analysis for attack detection, 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. 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.

6.3 THE NUMBER OF ATTACKERS

The 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.

6.4 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 among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is calculated as the average distance between elements in the border region of the twin clusters.

6.5 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. 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. Support Vector Machines-Based Mechanism 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.

7. SCREEN SHOT

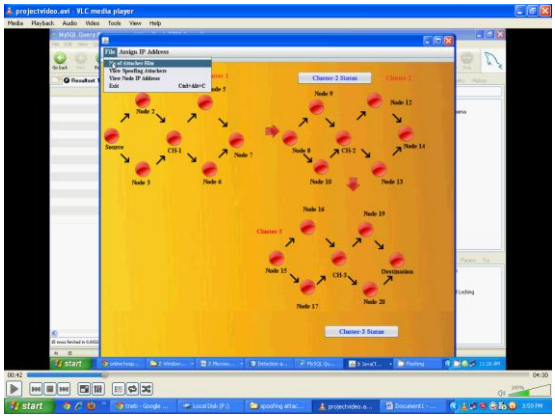

Fig7.1(Research is going on process)

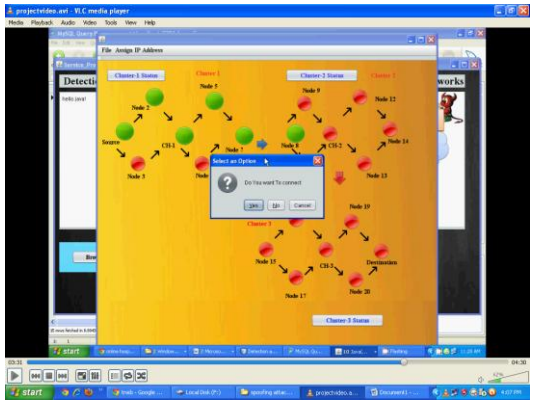

Fig7.2 (Research is going on process)

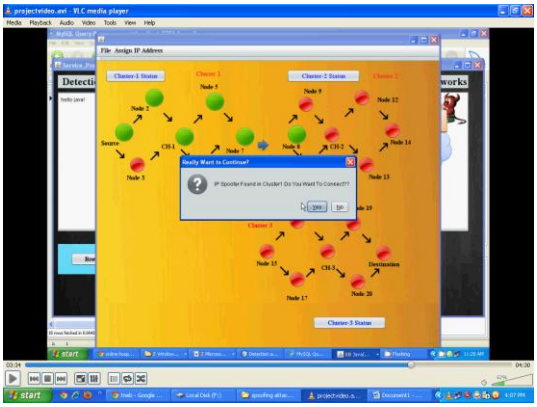

Fig7.3 (Research is going on process)

8. CONCLUSION AND FUTURE WORK

In this proposed work, we utilize the Received Signal Strength (RSS) -based spatial co-relation. RSS is associated with wireless nodes as its physical property which is hard to falsify and not reliant on cryptography as basis for detecting spoofing attacks in wireless networks. We provided the theoretical analysis of using RSS-based spatial co-relation readings with GADE so as to detect the spoofing attack in the system. The Multiclass Detection problem, SILENCE mechanism proposed to detect number of adversaries in the network. Also further SVM is proposed to improve the accuracy in detecting number of adversaries. Then enhanced IDOL model is proposed to localize the attackers in the system. This integrated model utilizes number of attackers from SILENCE mechanism and then using RADAR Gridded algorithm can find actual location and position of such spoofing attackers in the wireless networks. To test the proposed system we conducted experiments, such results from experiments also showed that this proposed technique reliant on RSS is more accurate and secure than existing one.

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

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

[21] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. CourierDover, 1965.

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

[23] 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.

[24] 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.

AUTHORS

Mr.P. Sundara Vadivel received his B.E. degree in Computer science Engg in 2005 from Madurai Kama Raj University and M.E. degree in Computer Science and Engineering in 2009 from Anna Universityi, He is currently working as Assistant Professor in the Department of Computer Science and Engineering at Bharath Niketan Engineering College . His areas of interest are Mobile computing, operating systems and Computer networks. Currently he is doing research on Mobile Computing and Spatial Queries He has published many papers in national and International journals.He is the lifetime member of ISTE and IEEE.

Mr.J.Senthil kumar received his B.E. degree in Computer science Engg in 2008 from Karpagam College Of Engineering and M.E. degree in Computer Science and Engineering in 2011 from Karpagam University, He is currently working as Assistant Professor in the Department of Information technology at Bharath Niketan Engineering College. His areas of interest are Mobile computing, operating systems and Computer Networks. Currently he is doing research on Mobile Computing and Spatial Queries He has published many papers in national and International journals. He is the lifetime member of ISTE and IEEE.

Mr.M.Sudharsanan **r**eceived his B.E. degree in Computer science En gg from Bharath niketan engineering collge and post graduate degree in Software Engineering from Anna University Chennai, India. His areas of interest are Ethical hacking, Mobile computing, operating systems and Computer Networks. He has presented many papers in national and international conferences in various fields. As part of this paper, he is working on developing

communication protocols for wireless network security—protocols optimized for wireless and mobility that can support file and database access. . He is also investigating operating systems support for mobile hosts .He is a member of ISTE