International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 99-104

DETECTION & LOCALIZATION OF SPOOFING ATTACK IN WI-FI NETWORK

Abhilasha Singh, Varsha Wahane (Asst. Proffesor)
Information Technology
Terna College of Engineering
Nerul, Navi-Mumbai, India
Singh.abhilasha09@gmail.com
Information Technology
Terna College of Engineering
Nerul, Navi-Mumbai, India
varshasim@gmail.com

***Abstract*—Wi-Fi is a networking technology that uses high frequency radio waves to provide high speed internet and network connections. The main function of wi-fi is to provide communication and sharing with the help of internet. Spoofing attack is a situation where some party masquerades as legitimate user by falsifying data and thereby gaining illegitimate advantage. Therefore it is necessary to detect spoofing attack and eliminate them. But the main problem arises when more than one attacker is taking the same node identity. In this case it becomes necessary to find the attackers and localize them. In our paper, we are detecting spoofing attacks as well as localizing adversaries for situations where multiple attackers are taking same node identity to launch spoofing attack.**

Keywords—Wi-Fi, Spoofing attack, Masqurades, Attackers, localization

I. INTRODUCTION

WiFi is a local area wireless computer networking technology which is used to network electronic devices [12]. It is also defined as wireless local area network. Many electronic devices uses WiFi like personal computers, smart phones, gaming consoles, digital audio players, tablet computers [12].

Wifi is less secure than wired network, mainly because the intruder does not need a physical connection. And as more wireless and sensor networks are deployed, they become the tempting target of attackers. Due to the openness of wireless and sensor networks, spoofing attack is very easy to launch. Spoofing attack means forging someone's identity mostly of legitimate users and therby gaining access of privileged data. Spoofing attack is a very serious attack as it leads to identity compromise as well as series of other attacks such as evil twin access point attack and even denial of service attack.

In order to secure its connection, WiFi has adopted various encryption technology. Cryptography is one of the oldest and most used encryption method for authentication. However due to various overheads like infrastructural and computational power associated with key distribution and maintenance, it is not always possible for wireless devices to deploy it for authentication. Mainly because of limited memory and storage space, it becomes hard to do the authentication if some overhead is included and in cryptography we know that various management infrastructural overheads are there. Other algorithm such as SEKM was also utilized. SEKM uses public key encryption method, but again as it depends on key, overheads depending on key distribution is there. K-Cluster analysis was also used for determining the presence of spoofing attack and finds the number of attackers. It does not include any overheads but if multiple adversaries are posing as single node, then in such case it is unable to determine the exact number of attackers. We have utilized spacial correlation on RSS (Received Signal Strength), a physical property that is associated with every node and hard to falsify. The x-y coordinates are calculated for every node for 300 samples using Dynamic triangular location method. And the RSS value for these nodes is calculated using Grey Prediction method. Grey prediction is used to predict the tendency of RSSI at run-time stage and present analysis of predicted RSSI when mobile user is moving. Grey prediction is able to reduce the fluctuation of RSSI when sensors are moving [13]. The location coordinates with grey prediction achieve smaller mean distance error.

II. PRESENT THEORIES AND PRACTICES

Spoofing attack must be detected on time as it makes the network vulnerable to various attacks like traffic injection attacks, access control lists attack, rogue access point attacks, and eventually Denial-of- Service (DoS) attacks [1]. Large-scale network also becomes target of multiple adversaries masquerading as the same identity and work together to launch malicious attacks such as network resource utilization attack and denial-of-service attack.

Because of this it becomes important to detect spoofing attack, determine number of attackers and localize them.

To detect spoofing attacks, cryptography is the most used approach. As it is known that cryptography relies on reliable key distribution and so there exists the overheads of the management and distribution of this key. Because of its infrastructural, computational, and management overhead, it is not always desirable to use it in sensor network, as the sensors have very low memory and space. In addition, cryptographic methods are susceptible to node compromise, which is a serious threat to sensor network as the entire network can be scanned. In this work, we propose to use 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. Using spacial correlation to detect spoofing attack also have the advantage that it adds no extra overhead to the wireless sensor network.

Our main focus in this work is on static nodes in-order to detect spoofing attack. Most of the existing approaches are unable to determine the number of spoofers if multiple nodes are using same node identity to launch attacks, which is why we are further doing the localization of nodes. The approach to localize the attackers however, is unable to localize the attackers if they are using different transmission power levels.

III. PROPOSED SYSTEM

In the proposed system, we are using a different approach. We utilize the physical properties associated with wireless transmissions to detect spoofing. In our work we are proposing a system which will detect spoofing attack and will localize multiple adversaries performing the attack based on their location. In our approach we are using the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. No extra overhead is added to wireless sensor nodes by our approach.

A. Spoofing Attack Detection

We use RSS reading of the nodes for cluster analysis. The Received Signal Strength value array as $s = (s_1,s_2,...s_n)$ 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 given in [14]

$$Si\ (dj)\ [d\text{Bm}] = P\ (d0)\ [d\text{Bm}] - 10\Upsilon \log\ (dj/d0) + Xi$$

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 [14].

In-order to detect spoofing attack, we are using PAM (Partitioning Around Medoids), it divides the RSSI value of a single node into two clusters and takes the medoids of both the cluster. The distance between two medoids D_M serves as test statics.

The basic idea behind PAM that we are utilizing is that the RSSI value taken from a single node N denotes the physical location of that node only. So if it is divided into two cluster and the difference of medoids are taken, then this difference must be very low. This holds true under normal condition, but if another node or a number of nodes which are at different physical location are taking the node identity of N, then this difference between medoids will be large.

So, if value of DM is small, no spoofing attack has taken place. But if the value is large, it means more than one node is taking the same node identity, launching the spoofing attack.

B. SILENCE Mechanism

SILENCE is using Silhouette Plot and System Evolution with minimum distance of clusters, to improve the accuracy of determining the number of attackers [1].

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 [1]. The SILENCE mechanism uses the advantage of both method to evaluate the no. of attackers with increased accuracy.

C. Support Vector Machine

We are using the training data collected during the offline training phase, to train the SVM which will further improve the performance of determining the number of spoofing attackers. SVM has the advantage of combining the characterics of various available statistical method, such as System Evolution and SILENCE, to detect the number of attackers. We are using Support Vector Machines (SVM) to increase the accuracy in determining 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.

D. Localization

We present our integrated system that detect spoofing attack, determine the number of attackers and localize multiple adversaries. There are a number of algorithms for localization out of which we are using Area based probability.

It uses interpolated signal mapping.

IV. EXPERIMENTAL RESULTS

We are using MATLAB as implementation platform for our approach, due to its network based features. In real time, wi-fi devices send the signals to the system via wi-fi medium, which is then analyzed by the network. This same thing can be done by MATLAB, just the difference is that instead of using hardware, we are designing the wi-fi model using MATLAB software.

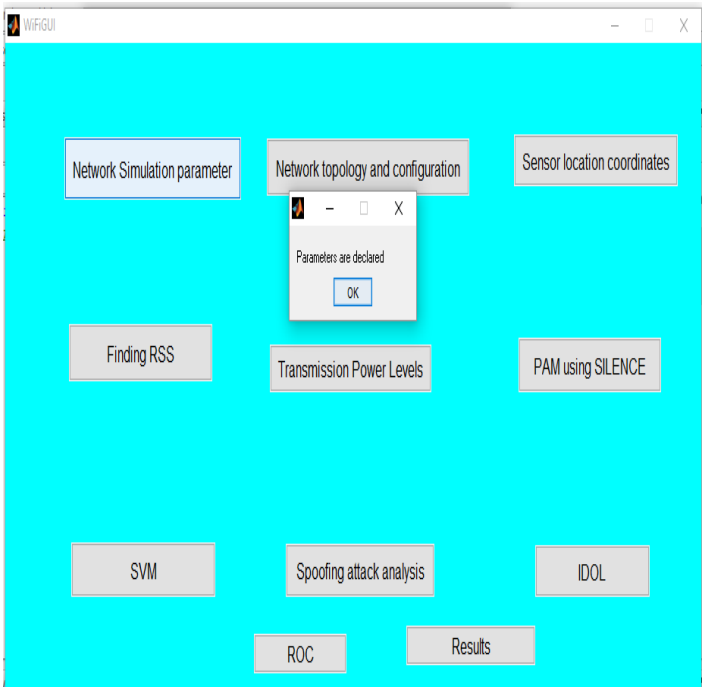

Fig.1 Wi-Fi GUI

In Fig.1, by clicking the "network simulation parameter", all the parameters are triggered. Here we are using 25 nodes and 300 samples. For Wi-Fi, we are using 1000.0e6 Hz frequency. Initially the RSSI value is initialized to 0 and the probability range is taken between 0 & 1 with the difference is 0.003.After the text edit has been completed, the paper is ready

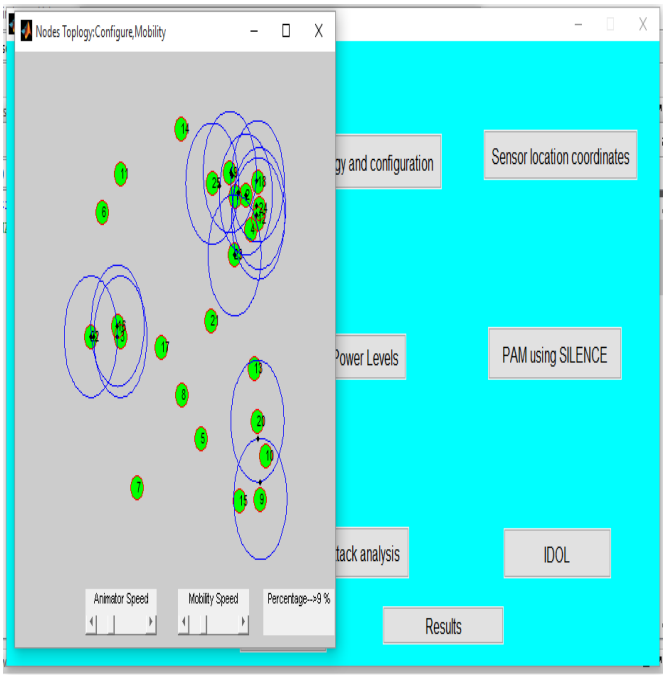

Fig.2 Network Topology

After the parameters are declared and the event is triggered, the network is created and 25 nodes perform Random way point movement. With the help of Animator Speed & Mobility Speed, we can control the speed of node movements. As the nodes are random way point, its minimum distance and maximum distance between two consecutive nodes are taken as 20 & 120. The node movement is denoted in fig.2.

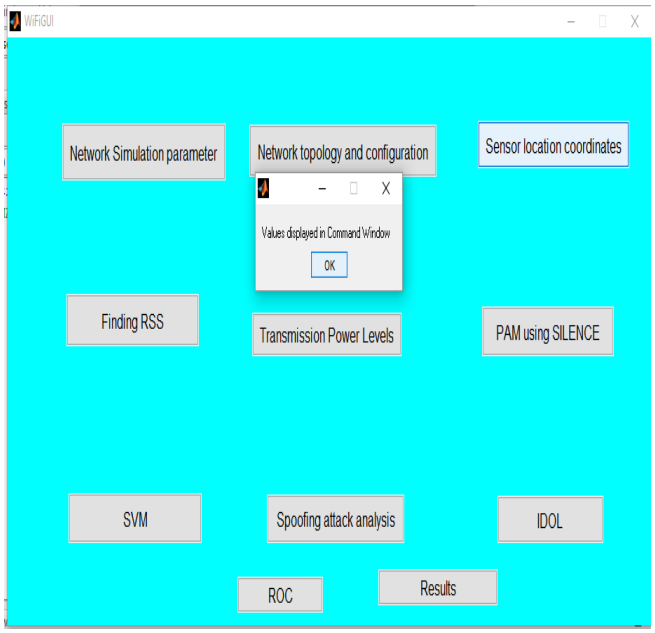

Fig.3 sensor location coordinates

As the nodes are moving in the Zigbee network, the location of each nodes are calculated using Dynamic Triangular Location method and is given in fig.4. At least three sensor nodes are required by DTN to estimate the location of mobile user. Worst RSSI measured by a sensor node will be discarded by DTN and other sensor nodes are used to estimate the location. A node which receives the strongest RSSI is chosen by DTN and taken as master node, and assume the mobile user's location in mapping circle of master node. The mapping circle in is the estimation distance d1 between the master node and mobile user. DTN finds the angle Θ on mapping circle by using a cost function to pick one that best matches the observed distance. Following steps are comprised in DTN:

1.To generate the mapping circle: best possible location of mobile user $(x1+d1\cos\Theta, y1+d1\sin\Theta)$ found by DTN on the mapping circle by using the possible distances (d2Θ, d3Θ) between the mobile user and slave nodes.

2. The distance of mobile user estimation: A error between the estimation distances (d2 and d3) and possible distances (d2Θ,d3Θ) is found by the DTN.

3. The coordinate of mobile approximation: A cost function at each angle Θ is calculated by DTN and Θ increase one degree at each time. DTN search the minimum cost function, and Θ of minimum cost function is estimation angle on mapping circle. The angle Θ on the mapping circle is the estimation location D of mobile user. At-last we shift the local coordinate D and find the global coordinate of mobile user $(x1+d1\cos\Theta, y1+d1\sin\Theta)$.

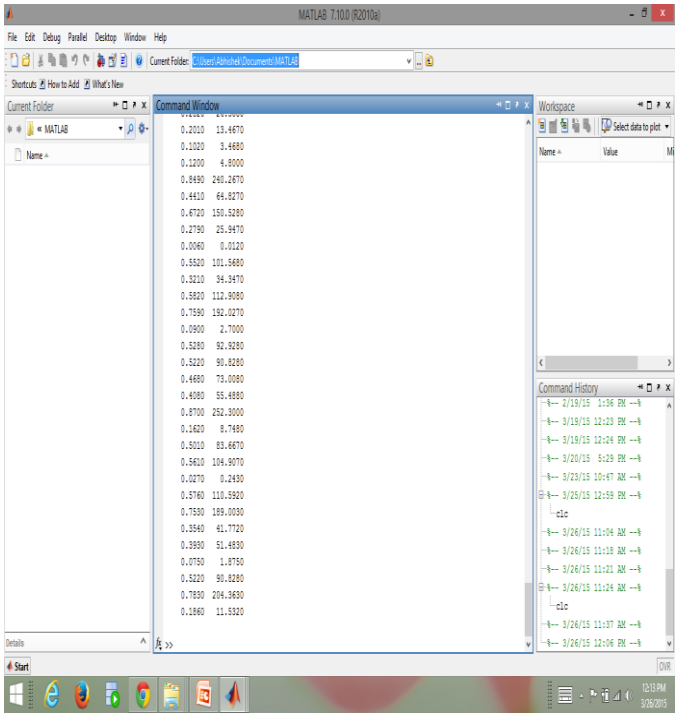

Fig.4 Location coordinates

Fig.5, shows the Received Signal Strength of the sensor nodes. We are using Grey Prediction algorithm to predict the RSSI. To find the location coordinates, we are using the dynamic triangulation algorithm. This dynamic triangulation along with grey prediction, minimizes the error due to node movements.

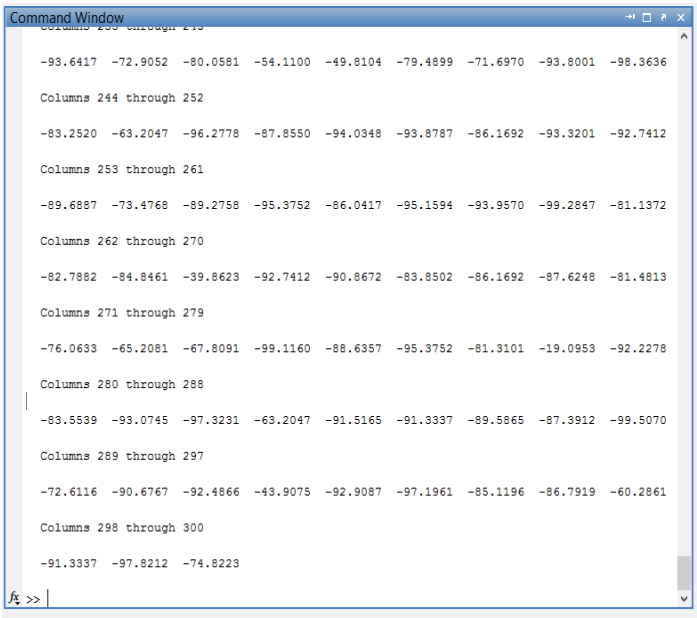

fig.5 RSSI Values

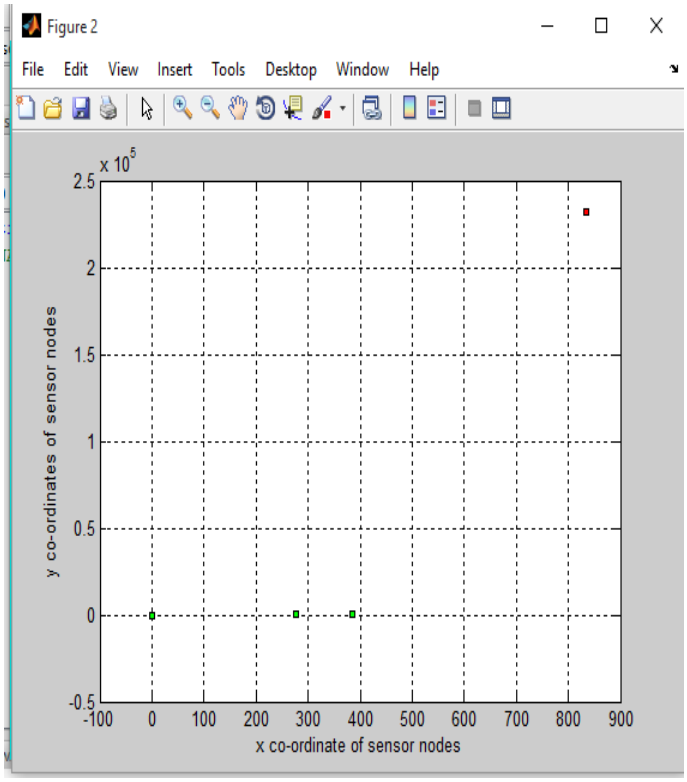

Fig.6 Cluster of nodes

In fig.6, we are denoting all the nodes in the form of clusters. We are taking cluster of 4. The RSSI values are taken from each node for 300 samples and we will localize the nodes. Here red dot is for the nodes that are behaving unusual.

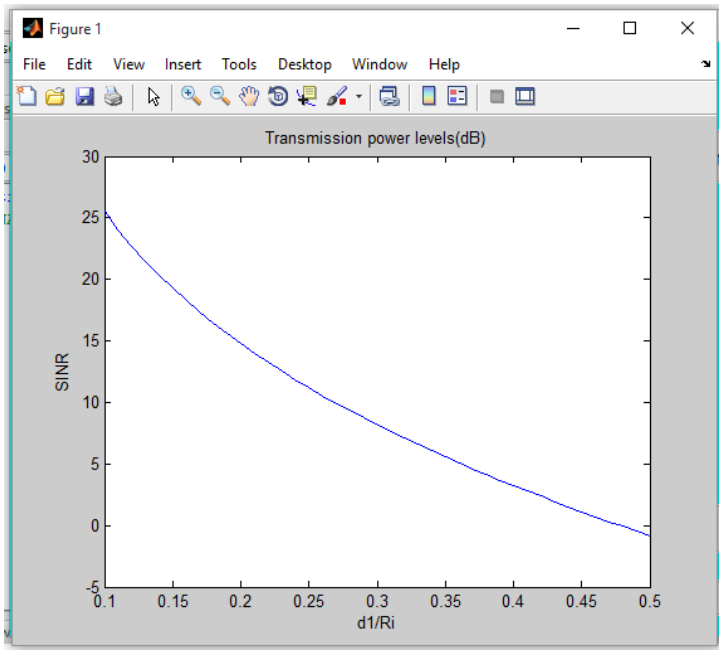

Fig.7 Transmission Power Level

Signal to noise ratio denotes the interference of nodes while di/Ri denotes the resistance of sensor nodes. Value of interference decreases as resistance increases. And it is shown in fig.7.

Partitioning Around Medoids is used to detect spoofing attack, in it the RSSI value of a single node is divided into two clusters and their medoids are found. The distance between both these medoids are found, the distance is taken as test metrics. If the distance is less, it means the RSSI value is from the same node, but if the distance is more, it means the RSSI value is combination of value of more than one node. So we conclude that, there is spoofing attack as the value of node is the combination of values of more than one node.

System evolution and silhouette algorithm is applied to find the number of attackers. Both these algorithm is applied separately to find the no. of attackers. Then with the help of SILENCE mechanism we choose the best result.

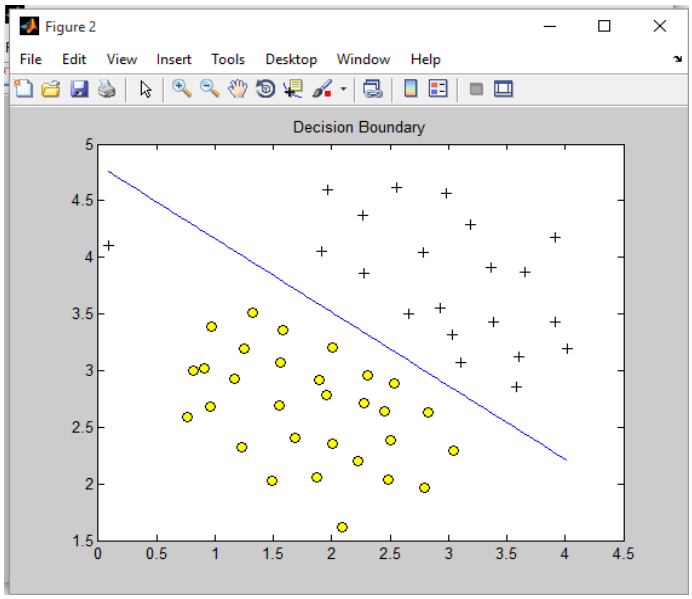

Fig.8 SVM decision boundary

Once the no. of attackers is determined, SVM is applied to increase the accuracy in determining the no. of attackers. SVM decision boundary while its training is shown in fig.8.

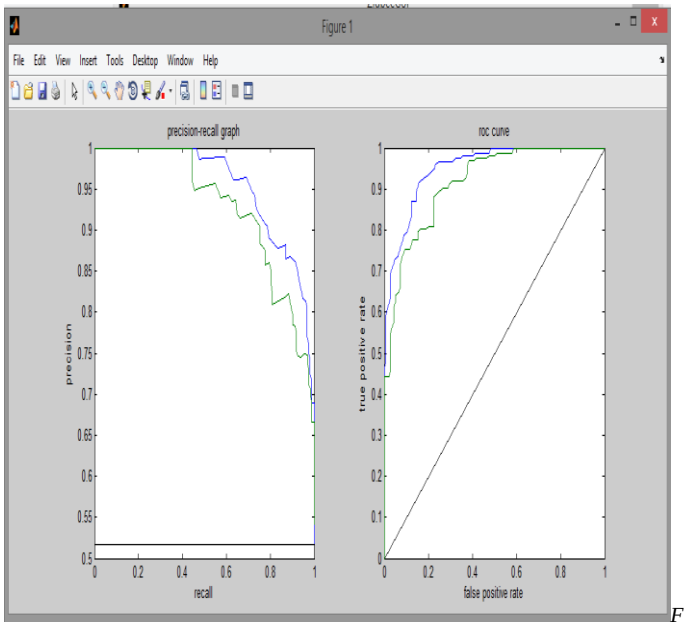

Fig.9 Precision Recall Graph

Fig.9 denotes the precision recall graph and the ROC curve. Figure 10 presents the graph of Probability of Detection Rate and False Positive Rate as well as graph between False Positive Rate and Hit Rate in normal environment and in spoofed environment.

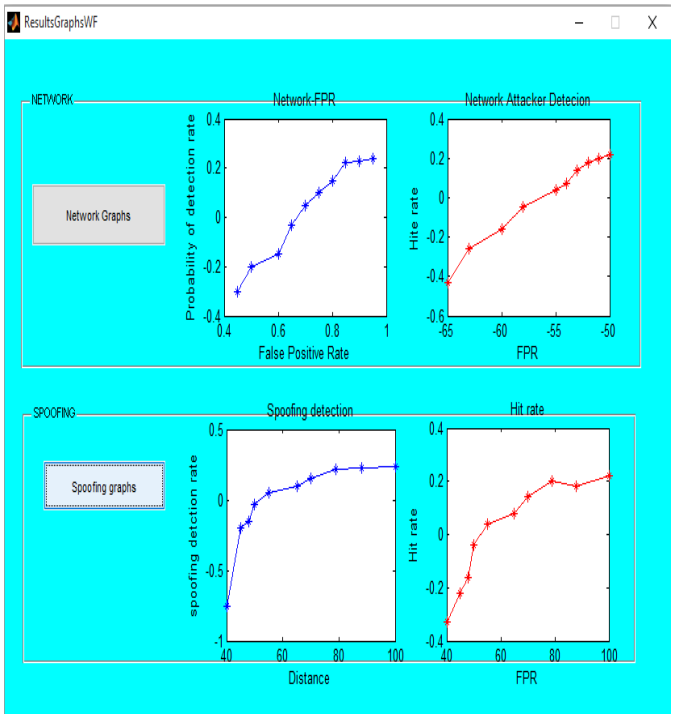

Fig.10 Network & Spoofing Graph

Conclusion

In this work, we are utilizing a physical property associated with each wireless device, received signal strength (RSS) based spatial correlation, which is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. We are using PAM for attack detection and RSS reading to develop Test statics for PAM. We have developed SILENCE mechanism to find the number of attackers. In-order to increase the accuracy we are using SVM mechanism. Our approach can 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.

REFERENCES

[1] *Detection and Localization of Multiple Spoofing Attackers in Wireless Networks by "Jie Yang, Student Member, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE, and Jerry Cheng"*

[2] *Attack Detection in Wireless Localization by "Yingying Chen, Wade Trappe, Richard P. Martin".*

[3] *A Localization-Based Anti-Sensor Network System by "Zhimin Yang, Eylem Ekici , and Dong Xuan".*

[4] *Access points vulnerabilities to DoS attacks in 802.11 networks by "F. Ferreri and M. Bernaschi, L. Valcamonici".*
[5] *The Limits of Localization Using Signal Strength: A Comparative Study by "Eiman Elnahrawy, Xiaoyan Li, Richard P. Martin".*
[6] *"Secure and Efficient Key Management in Mobile Ad Hoc Networks by "Bing Wu, Jie Wu, Eduardo B. Fernandez, Spyros Magliveras".*
[7] *Relationship-based Detection of Spoofing-related Anomalous Traffic in Ad Hoc Networks by "Qing Li, Wade Trappe".*
[8] *Detecting and Localizing Wireless Spoofing Attacks by "Yingying Chen, Wade Trappe, Richard P. Martin".*
[9] *Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength by "Yong Sheng3, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell".*
[10] *Spatial Signatures for Lightweight Security in Wireless Sensor Networks by "Lifeng Sang and Anish Arora".*
[11] *Detecting Spoofing Attacks in Mobile Wireless Environments by "Jie Yang , Yingying Chen and Wade Trappe ".*
[12] *https://en.wikipedia.org/wiki/Wi-Fi*
[13] *Mobile user localization in wireless sensor network using grey prediction method by "R.C.Luo, Ogst Chen, S.H.Pan" IEEE 2005.*
[14] *ANALYSIS OF MOBILE USER IDENTIFICATION INSIDE THE BUILDINGS,(2011), INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS 05/2011; VOL. 1(N.2)*
[15] *J. Bellardo and S. Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Proc. USENIX Security Symp., pp. 15-28, 2003.*
[16] *F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.*
[17] *D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.*
[18] *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.*
[19] *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.*
[20] *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.*
[21] *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*
[22] *J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in Proc. IEEE SECON, 2009.*
[23] *J. Wright, "Detecting wireless LAN MAC address spoofing," 2003, technical document. [Online]. Available: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf*
[24] *NS2 Tutorial http://www.isi.edu/nsnam/ns*
[25] *M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.*
[26] *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.*
[27] *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.*
[28] *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.*
[29] *L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137-2145, 2008.*
[30] *P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.*
[31] *E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'lConf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.*
[32] *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.*
[33] *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.*
[34] *P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.*
[35] *Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.*