ISSN:0975-9646

Detection and Localization of Spoofing in Wireless and Sensor Networks

Prof. Chandrakant M. Jadhav#, Prof. Sharad S. Shinde*

#Head of Department of Computer Science & Engineering, B.I.G.C.E., Solapur, India
*Assistant professor, Department of Computer Engineering, M.I.T.M., Sindhudurg, India

Abstract- **In today, networks are becoming dangerous due to IP spoofing attacks. It is specially affecting in the wireless networks i.e. both in the ad hoc and sensor networks. There are various solutions available like cryptographic algorithms that can identify the transmitter but it requires complex key computations. In this paper we argue that it is possible to provide supporting strategies to traditional authentication that can identify device spoofing without any cryptographic algorithm. We propose the forge resistant relationship in the malicious attacks. We first propose an attack detector for spoofing that utilizes K-means cluster analysis. Next, we describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of identify the positions of the attackers We then show that the location of attacker by using two methods i.e. area based localisation or point based localisation. We have done our experiments in both IEEE 802.11 Wi-Fi networks as well as in the IEEE 802.15.4 Zigbee networks. After analysing our methods, it is possible to detect the spoofing with high detection probability and with low false error rate, thereby providing usefulness of K-means spoofing detector as well as the attacker localisation.**

I. INTRODUCTION

Now a day, the wireless and sensor networks are becoming very popular and because of that it will be targeted by various types of malicious attackers. Wireless and sensor networks are open to all and therefore they are vulnerable for malicious attacks where an attacker forges its identity to masquerade as another device. Spoofing attacks are a serious threat as the identity and allow various types of traffic injection attacks. Thus it is required to detect the presence of spoofing and eliminate them from the network. In traditional way, we can use cryptographic authentication. But it requires more complicated infrastructure and it increases network overhead.

In this paper, we are using different approach by using physical properties regarding wireless transmission 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 method uses 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. By analysing the RSS from each MAC address using K-means cluster algorithm, we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. We then describe how we integrated our K-means spoofing detector into a real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms. For two sample algorithms, we show that using the centroids of the clusters in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

To evaluate the performance of our approach, we conducted experiments using both 802.11 as well as 802.15.4 network in real environment. We have built an indoor localization system that can localize any transmitting device on the floor in real time. We analysed the performance of K-means spoofing detector. We found that our detector is highly efficient with 96% success rate and 5% false positive rate.

Further, we analysed that, when we use the centroids in signal space, a large family of localization algorithms achieve the same performance as when they use the averaged RSS in traditional localization attempts. Our experiments show that the distance between the localized results of the spoofing device and the original device is proportional to the true distance between the two devices; thereby we are providing strong evidence of the performance of spoofing detection as well as localizing the positions of spoofing devices.

The remaining paper is organized as follows. Section II describes the previous researches done regarding to spoofing attack identification and related work in localization. In section III, we describe the feasibility of spoofing attacks and their effects, and discuss our methodologies. In section IV, we formulate the spoofing attack detection problem and propose K-means spoofing detection. We introduce the localization system in real time environment and how to find the locations of attackers in section V. Further, we discuss some related points in section VI. Finally, we conclude our work in section VII.

II. RELATED WORK

Recently, researchers are doing huge work on spoofing attacks. We cannot give here all the details of work. Instead, we will take overview of some traditional and new approaches. Then we will describe the works related to our work.

The use of cryptographic authentication is the traditional security approach to deal with identity fraud. An authentication scheme for hierarchical, ad hoc sensor networks is proposed in [1] and a hop by hop authentication scheme is described in [2]. If we use authentication, it requires additional infrastructure and computational power to distribute and maintain the key management which increases huge overhead in the network. [3] Has provided a secure and efficient key management framework (SEKM). A public key infrastructure (PKI) is used by the SEKM. Another key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys is implemented by [4]. In addition, [5], [6] employ cryptographically generated addresses (CGA) to defend against spoofing.

In wireless and sensor devices, the sources are limited and it is needed infrastructural overhead to maintain the authentication scheme. That is why it not desirable. Recently [7],[8] have proposed new approaches to detect spoofing attacks in wireless network. They use a security layer which is separate from conventional network authentication approaches. By using sequence number of packet, traffic interrarrival, the chain of temporary identifiers, and consistency of signal strength, they developed forge-resistant relationships to detect spoofing attacks. [9] has proposed a lower layer approach that uses functions of wireless channel at the physical layer to support high level security functions such as authentication and confidentiality. [10] has given the work which is closely related to our paper which proposed the utilization of signal prints for detection of spoofing.

Even these approaches have different detection and false alarm rates, these approaches do not provide the localization ability of spoofing attackers after spoofing detection. Further, our approach is novel in that we have integrated our spoofing detector into real time localization system which can both detect the spoofing attacks, as well as localize the attacker in the network. Additionally, we have deployed our localization system in real time i.e. in houses or in colleges.

However, the strength of received signal is also utilized to detect Sybil nodes in wireless networks [11]. They did not give the method for localization of Sybil node. The Vehicular Ad Hoc Networks (VANETs) used the signal strength to detect and localize Sybil nodes [12].

Finally, a large amount of work has been developed localization algorithms for wireless networks. Our paper is used the RSS to perform localization along with fingerprint matching and probabilistic techniques [13]-[15].

III. Feasibility Of Attacks

In this section, we have given the brief description of spoofing attacks and their impact. We then see the experimental methodology that we use to implement our method of spoofing detection.

A. Spoofing Attack

As we know, the wireless medium is open to all. It is easy to monitor the communications to find out the layer II MAC address of other nodes. By using the MAC address we can uniquely identify the nodes. In most of the cases, the attackers can easily inject their MAC addresses as another transmitter. As a result, these attackers seem like the part of the network even if they are adversaries. Such type of spoofing attacks is serious threat for the network performance. They produce security threat such as attacks on access control at the access points [16], and denial-of-service through a DE authentication attacks [17]. [7], [10] give the full description of spoofing attack.

B. Experimental Methodology

To evaluate the effectiveness of our spoofing detection technique, we have conducted various experiments in different types of networks. We have implemented our methods on 802.11 (Wi-Fi) networks using an Orinoco silver card, and on 802.15.4 (Zigbee) network using Telosb mote, on 2nd floor of my house. The floor size is 200*80ft (16000 sqft). The 802.11 (Wi-Fi) networks with 4 landmarks are shown to maximize the strength of signal coverage, as shown in red squares in figure 1 (a). Figure 1 (b) shows the 802.1504 (Zigbee) network with 4 landmarks arranged in square setup to achieve optimal landmark placement [18], shown in red rectangles. The locations are denoted by small blue dots in the floor map for spoofing and localization tests.

In the 802.15.4 network, we have taken 300 packet level RSS samples for each of the 100 locations. We have used the actual RSS values given by each packet. We have 286 locations in our 802.11 deployment. These RSS values appear partially synthetic. Only the mean RSS was available to access. But to conduct our experiments we needed a RSS value per packet. At each location, to generate such type of values for 200 simulated packets, we used measured RSS mean fr the mean of distribution. We required standard deviation and for that we computed the difference in the RSS a fitted signal to distant function and then calculated standard deviation of the distribution by using these differences on all locations. We took the maximum deviation on all the landmarks to keep conservative results, which we found 5 dB

We have done lot of work to characterize the distributions of RSS readings indoors. It is not possible to implement most accurate characterization; still we maintained the best balance between algorithmic utilization and the resulting localization error [15], [19].

In addition, we have built a real time localization to find out the locations of both the original nodes and spoofing nodes. Then randomly we selected the points out of the locations as the input data for use by the localization algorithms. For the 802.11 (Wi-Fi) networks, the input data size is 115locations, and for the 802.15.4 network, the size of the input data is 70 locations. We have given the details of our localization system in Section V.

IV. Attack Detector

In this section we mention our spoofing attack detector. We first introduce the spoofing attack detection problem as a classical statistical testing. Next we gave the test statistics for spoofing detection. We then describe the metrics to evaluate the efficiency of our approach. Finally we describe our experimental results.

A. Formulation of Spoofing Attack Detection

RSS is widely available in wireless networks and its values are very closely related with location in physical space. In addition, RSS is common physical entity used in various localization algorithms [13]-[15], [20]. It is an attractive approach using RSS because it reuses the existing wireless infrastructure. Thus we are using the properties of RSS in spoofing attack detector.

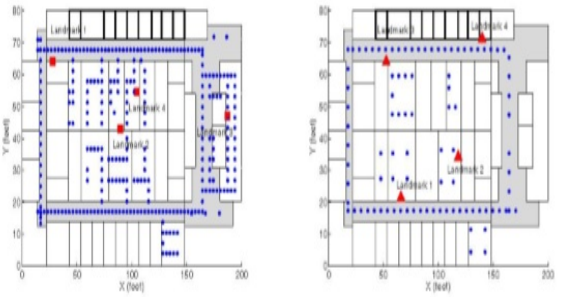
The main goal of spoofing detector is to identify the spoofing attacker. We presented the spoofing detection as a statistical significance test, where the null hypothesis is:

Ho: normal (no attack).

In testing, to evaluate whether observed data belongs to null-hypothesis or not, a test statistic T is used. If the observed test statistic differs from the null-hypothesis, the null-hypothesis is rejected and we conclude the presence of spoofing attack.

B. Test Statistics for Spoofing Detection

The RSS value vector s = {s1, s2, …sn} (n is the number of landmarks/access points) is affected by random noise, environmental bias and multipath propagation effects; still it is closely related with physical location of transmitter and determined by the distance to the landmarks [15]. At different locations in physical space, the RSS readings are distinctive. Each vector s is corresponding to a point in a n dimensional signal space [21].



(a) 802.11 network (b) 802.15.4 network

Fig. 1. Landmark setups and testing locations in two networks.

If there is no presence of spoofing, for N\AC address, the sequence of RSS sample vectors will be close to each other, and fluctuation will be there at a mean vector.

However, if there is spoofing attack, there is more than one node claiming that same MAC address at different locations. As a result, the RSS sample readings from the MAC address of spoofing device will be mixed with RSS readings from at least one other location. Based on the signal strength properties, the RSS readings from the same physical location will be belonging to the same cluster points in the n dimensional signal space; in the physical space the RSS readings from different locations should form different clusters in the signal space.

This observation shows that to identify spoofing, we can use K-means cluster analysis [22] on the RSS readings from each MAC address. If it results M RSS sample readings for a MAC address, the M sample points are partitioned into K disjoint subsets Si containing M_j sample points so as to minimize the sum-of-squares criterion by the K-means clustering algorithm.

$$J_{\min} = \sum_{j=1}^{k} \sum_{Sm \in sj}^{Sm \in sj} \| sm - \mu j \|^2 \qquad (1)$$

Where the S_m is a RSS vector denoting the m^{th} sample point and it gives the centroid of the sample points for S_j in signal space. In normal case, the distance between the centroids will be close to each other because there is basically single cluster. In spoofing condition, the distance between centroids is increased as the centroids are derived from the different RSS clusters associated with different locations in physical space. We then choose the distance between two centroids as the test metric T for spoofing detection:

$$D_c = \| \mu_{i} - \mu_{j} \| \qquad (2)$$

Where I,j € {1,2,…K}. From the collected data set we will use empirical methodologies to determine thresholds for defining the critical region for the significance testing. For more illustration, we will use following definitions, the original node P_{org} is referred as wireless device with the legitimate MAC address. The spoofing device P_{spoof} is referred as the wireless device that is forging its identity and behaving as another device. There is the possibility of multiple spoofing nodes of the same MAC address.

As we know, our K-means spoofing detector can support packets from different transmission power levels. If an attacker is sending packets with varying transmission power level from the original node with the same MAC address, there will be two distinct RSS clusters in signal space. Thus, we can find out the spoofing attack based o the distance between two centroids obtained from the RSS clusters.

C. Determining Thresholds

The appropriate threshold T will allow the spoofing detector to be robust to false detections. We can determine the thresholds through empirical training. During the off line phase, we can collect the RSS readings for a set of known locations over the floor and obtain the distance between two centroids in signal space for each point pair. We use the distribution of the training information to determine the threshold T. At run time, based on the RSS sample readings for a MAC address, we can calculate the observed value DCbS. Our condition for declaring that a MAC address is under a spoofing attack is:

We are taking here the appropriate threshold T will allow the robustness in spoofing detection. By using empirical training, we can determine the thresholds. In the offline conditions, for set of known locations we can collect the RSS readings over the floor and get the distance between two centroids in signal space for every point pair. To determine the threshold T, we use the distribution of the training information. At run time, for a MAC address based on the RSS sample readings, we can calculate the observed value D_c^{abs}. For declaring that a MAC address is under a spoofing attack we use the condition:

$$D_c^{abs} > T \qquad (3)$$

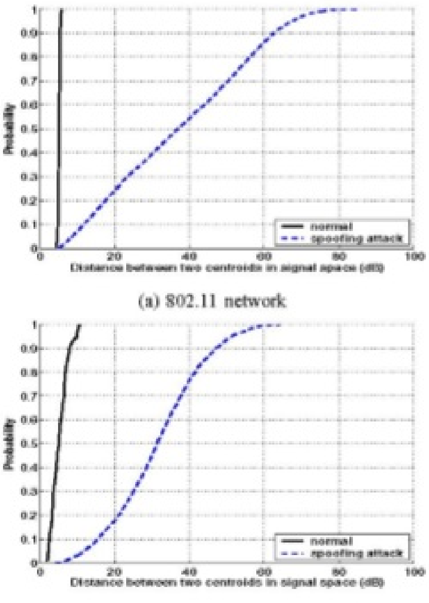
The CDF of the DC in signal space for both the 802.11 networks and 802.15.4 networks is shown in Figure 2 (a) and (b). We got that the curve of DC shifted hugely t the right under spoofing attacks, therefore it suggests that using DC as a test statistic is an effective way for detecting spoofing attack.

D. Performance Metrics

To evaluate the performance of our spoofing attack detector by using K-means cluster analysis, we have used following metrics:

Detection Rate and False Positive Rate: Due to spoofing attack, it causes the significance test to reject Xo. Thus we will do the statistical characterization of the spoofing detection attempts over all the possible spoofing attacks on the floor. The detection rate is defined as the percentage of the spoofing attack attempts that are derived to be under attack. Note that, in the presence of spoofing attack, the detection rate corresponds to the probability of detection P_d, while in the normal condition; it corresponds to the probability of declaring false positive P_{fa}. Under different thresholds, the detection rate and false positive rate vary.

Receiver Operating Characteristic (ROC) curve: We can evaluate attack detection by studying together the false positive rate P_{fa} and probability of detection P_d. The ROC curve shows the plot of attack detection accuracy versus the false positive rate. It can be measured by varying the detection thresholds.



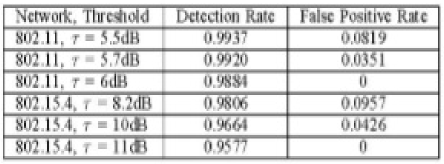
(a) 802.11 network

(b) 802.15.4 network

Fig. 2. Cumulative Distribution Function (CDF) of D_c in signal space

E. Experimental Evaluation

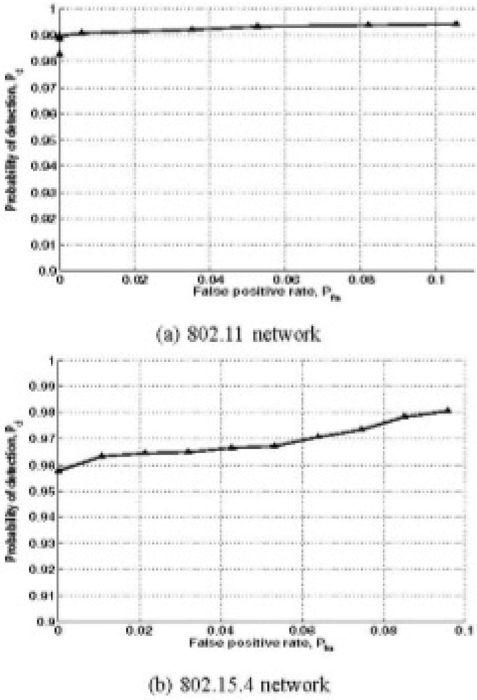
In this section we will evaluate the results of the effectiveness of the spoofing attack detection. Table I gives the detection rate and false positive rate for both the 802.11 and 802.15.4 network under different thresholds. The Figure 3 displays corresponding ROC curves. The results are showing that false positive rates less than 10%, the detection rates are above the 95%. These results are encouraging for us. The detection rate is still more than 95% even when the false positive rate goes to zero in both 802.11 and 802.15.4 networks. We will further study that when the spoofing node is at varying distances from the original node in the physical space, how the spoofing node can be detected by using our spoofing attack detector. The detection rate as a function of the distance between the spoofing node and original node is represented in Figure 4. We found that the detection rate high when the distance between P_{spoof} and P_{org} is maximum. detection rate goes over 90% when P_{spoof} is 13 feet away from P_{org} under the condition T equals to 5.5dB. On the other hand, in the 802.15.4 network the detection rate is above 90% when the distance between P_{spoof} and P_{org} is 20 feet at threshold equals to 9dB. Thus we can say that the average localization estimation errors are about 10 – 15 feet using RSS [15]. When the node distance is less than 10 – 15 feet, possibly they may generate similar RSS readings and thus rate of spoofing detection falls below 90% but still it is greater than 60%. The attacker may get exposed itself when it goes closer to the original node. When the spoofing node is about 45 -50 feet away from original node, the detection rate goes to 100%.



Network, Threshold	Detection Rate	False Positive Rate
802.11, τ = 5.5dB	0.9937	0.0819
802.11, τ = 5.7dB	0.9920	0.0351
802.11, τ = 6dB	0.9884	0
802.15.4, τ = 8.2dB	0.9806	0.0957
802.15.4, τ = 10dB	0.9664	0.0426
802.15.4, τ = 11dB	0.9577	0

TABLE I

DETECTION RATE AND FALSE POSITIVE RATE OF THE SPOOFING ATTACK DETECTOR.



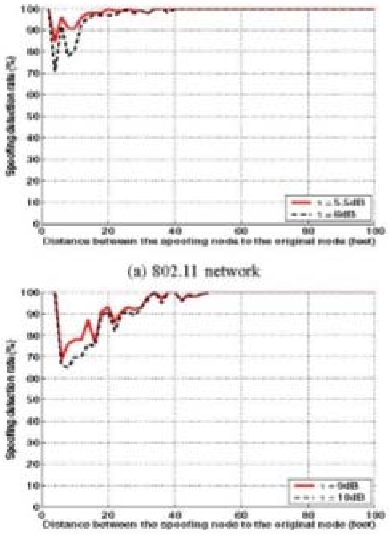
(a) 802.11 network

(b) 802.15.4 network

Fig. 3. Receiver Operating Characteristic (ROC) curves

V. LOCALIZING ADVERSARIES

If the spoofing attack detector determines the spoofing attack, then it is needed to localize the adversaries and further to eliminate the attackers from the network. In this section we present the localization system in real time environment to locate the positions of attackers. To estimate the positions of adversaries, we present the localization algorithms. To evaluate the effectiveness of our approach, we presented the experimental results.



(a) 802.11 network

(b) 802.15.4 network

Fig. 4. Detection rate as a function of the distance between the spoofing node and the original node.

A. **Localization System**

To perform a real time indoor positioning, we have developed a general purpose localization system. It is having fully distributed functionality and easy to plug-in localization algorithms. It contains four logical components: Transmitter, Landmark, Server, and Solver. The Figure 5 shows system architecture.

Transmitter: Any device that can transmit the packet is localized. To localize the transmitter, it is not needed to alter the application code on sensor node.

Landmark: The landmark is the component which listen the packet traffic and extract the RSS reading for each transmitter. The RSS information is then forwarded to the Server component. The landmark is stateless and deployed on each landmark or access point with known location.

Server: The roll of centralized server is to collect RSS information from all the landmarks. The server component performs the spoofing detection. The server maintains the summary of RSS information such as clustering or averaging, then the information is forwarded to the solver component for localization estimation.

Solver: First the solver takes input from the server. The solver performs the localization by using the localization algorithms plugged in, and return the localization results to the server. We can create multiple instances of solver and each solver can localize multiple transmitters simultaneously.

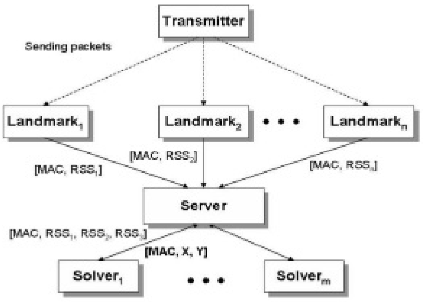


Fig. 5. Localization system architecture

During the localization process, the following steps will take place:

1. The following steps will takes place during localization process:
2. The transmitter sends the packet. Some landmarks check the packet and record the RSS.
3. After checking the packet, each landmark forwards the RSS to the server.
4. The server creates the complete RSS vector for the transmitter and sends the information to the instance of solver for estimation of location.

The solver instance then performs the localization process and returns the information regarding the coordinates of the transmitter back to the server.

B. **Attack Localizer**

When our spoofing detector identifies an attack for a particular MAC address, the server uses the centroids returned by the K-means clustering analysis in signal space and sends to the solver for location estimation. As an example using a location on the testing floor, the relationship among original

RADAR: As a localization result, the point based methods return an estimated point. The RADAR scheme is the primary example of a point based method [13]. In RADAR system, as in the offline phase, a wireless transmitter with known position broadcasts beacons periodically, and the RSS readings are measured at a set of landmarks or access points. The averaged RSS readings collected together from each of the landmarks for a set of known locations provides a radio map. Then at the runtime phase, localization is carried out by measuring a transmitter's RSS at each landmark, and the RSS vector is compared to the radio map. The location of the transmitter is declared by comparing the record in the radio map whose signal strength vector is closest in the Euclidean sense and the observed RSS vector. In this work, we use the RSS centroids obtained from K-means clustering algorithm as the observed RSS vector instead of using the averaged RSS in the traditional approach for localizing a MAC address.

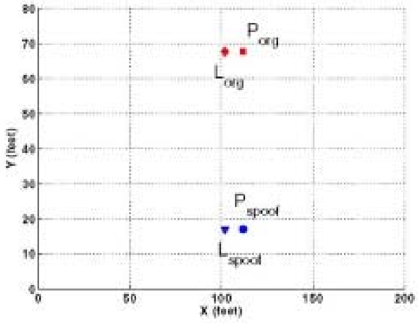


Fig. 6. Relationships among the original node, the spoofing node, and their location estimation through localization system.

Area Based Probability (ABP): Area-based algo- rithms return a most likely area in which the true location resides. One major advantage of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. ABP returns an area, a set of tiles on the floor, bounded by a probability that the transmitter is within the returned area [15]. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution. The Gaussian random variable from each landmark is independent. ABP then computes the probability ofthe transmitter being at each tile L on the floor using Bayes' rule:

Area Based Probability (ABP): The area based algorithms return the location of residential area of node. One main advantage of area based methods compared to point based methods is they return a region, which can give transmitter's true location. The ABP gives an area. It is the set of tiles on the floor bounded by a probability that the transmitter is within the returned area [15]. The ABP considers the distribution of RSS for each landmark follows Gaussian distribution. For each landmark the Gaussian random variable is independent. Then by using Bayes' rule, the ABP computes the probability of the transmitter being at each tile L on the floor.

$$P\,(L_i/S) = \frac{P(S|L)\times P(L)}{P(S)} \qquad (4)$$

As given, the transmitter must be resided at exactly one tile satisfying $\sum_{i=1}^{L} P(\,Li \mid S\,) = 1$, the ABP normalizes the probability and returns the most efficient tile to its confidence α. To localize the positions of the attackers, our experiments employed both RADAR and ABP.

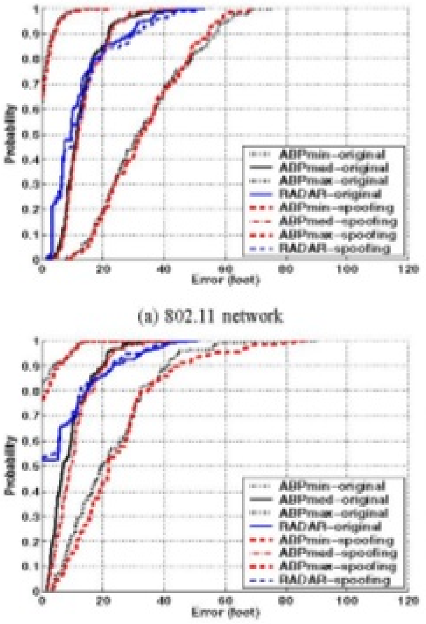
C. Experimental Evaluation

Here we are interested in the following performance metrics to evaluate the effectiveness of our localization system.

Localization Error CDF: We get the cumulative distribution function (CDF) of the location estimation error from all the localization attempts and it includes both the original nodes and spoofing nodes. Then we compare the error CDF of all original nodes to the possible spoofing nodes on the floor. We then report CDFs of minimum and maximum error for area based algorithms. In the given localization attempt, these are the points in the returned area that are closest to the true location.

Relationship between the true and estimated distances: How accurate our attack localizer can report the positions of both the original node and attackers is evaluated by using the relationship between true distances of the spoofing node to the original node || P_{org} - P_{spoof} || and the distance between the location estimate of the spoofing node and the original node || L_{org} – L_{spoof} ||.

We first present the statistical characterization of the location estimation errors. Figure 7 presents the localization error CDF ofthe original nodes and the spoofing nodes for both RADAR and ABP in the 802.11 network as well as the 802.15.4 network. For the area-based algorithm, the median tile error ABP-med is presented, as well as the minimum and maximum tile errors, ABP-min and ABP-max. We found that the location estimation errors from using the RSS centroids in signal space are about the same as using averaged RSS as the input for localization algorithms [15]. Comparing to the 802.11 network, the localization performance in the 802.15.4 network is qualitatively better for both RADAR and ABP algorithms. This is because the landmark placement in the 802.15.4 network is closer to that predicted by the optimal and error minimizing placement algorithm as described in [18]. First we describe the statistics of location estimation errors. The localization error CDF of the original nodes and the spoofing nodes for both RADAR and ABP in the attack has not been detected by the K –means spoofing detector. As compared to Figure 4, the spoofing attacks are100% detected when ||P_{org} - P_{spoof}|| equals to or is greater than about 50 feet.



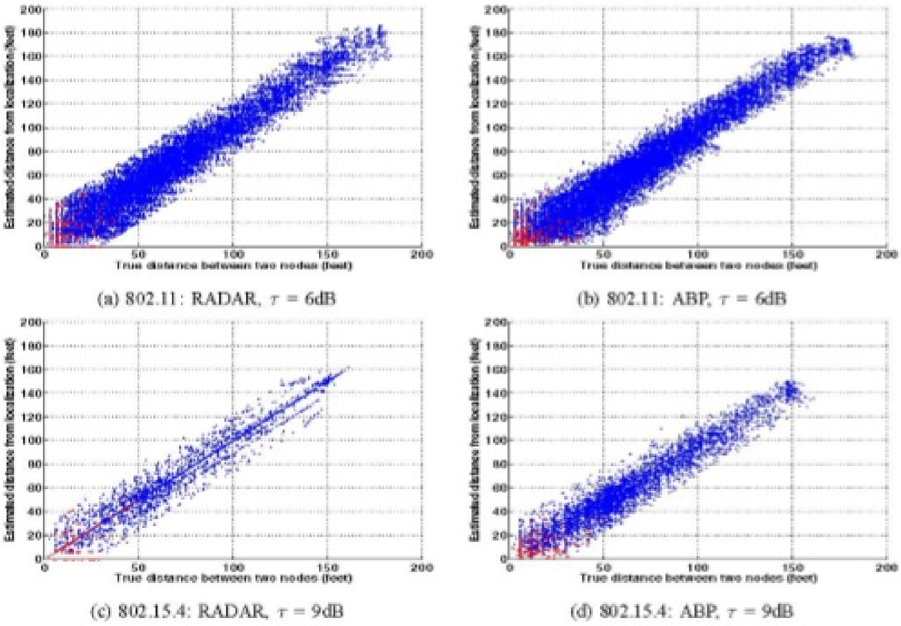
(a) 802.11 network

(b) 802.15.4 network

Fig. 7. Localization error CDF across localization algorithms and networks.

802.11 and 802.15.4 networks is shown in Figure 7. In area based algorithm, the minimum and maximum tile error, ABP-min and ABP-max as well as the median tile error ABP-med are presented. We found that using averaged RSS centroids in signal space, the location estimation errors are nearly same as using averaged RSS as the input for localization algorithms [15].

The important thing we have observed that localization performance of the original nodes is qualitatively same as the spoofing node. This is very similar performance that using the centroids obtained from the K-means cluster analysis as effective in both identifying as well as localizing the attacks. The challenge in position localization arises because the system does not know the positions of the either original MAC address or the



(a) 802.11: RADAR, τ = 6dB

(b) 802.11: ABP, τ = 6dB

(c) 802.15.4: RADAR, τ = 9dB

(d) 802.15.4: ABP, τ = 9dB

Fig. 8. Relationship between the true distance and the estimated distance for the original node and the spoofing node across localization algorithms and networks.

Further, the relationship between $||L_{org} - L_{spoof}||$ and $||P_{org} - P_{spoof}||$ is come with the 45 degree straight line. This is indicating that $||L_{org} - L_{spoof}||$ is directly proportional to $||P_{org} - P_{spoof}||$ and our localization is highly effective for localizing attackers. The values of $||L_{org} - L_{spoof}||$ fluctuate around the true distance value at a fixed distance value of $||P_{org} - P_{spoof}||$. This fluctuation reflects the localization errors of both P_{org} and P_{spoof}. When the $||P_{org} - P_{spoof}||$ is larger, the fluctuation of $||L_{org} - L_{spoof}||$ becomes smaller, at about 10 feet maximum. In contrast, the attack localizer can find te position of attacker's and estimate the distance from the original node to the attacker at about 10 to 20 feet maximum error.

VI. Discussion

So far we have examined the K-means cluster analysis in signal space. It provides great inspiration to explore packet-level localization at the server, means the localization is performed for each packet received at the landmarks. The server uses each RSS reading vector for localization. Over a certain time period i.e. for example 60 seconds, there will be a cluster of location estimates in physical space for a MAC address. We think that there will be distinctive location clusters around the original node and the spoofing nodes in the physical space. Our intention was that the cluster results from packet localization would allow the detection and localization of attackers in one step.

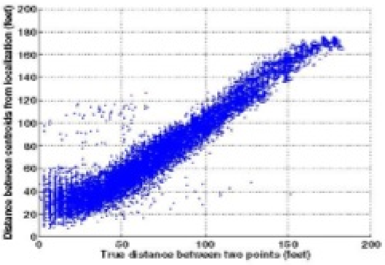


Fig. 9. Packet-level localization: relationship between the true distance and the estimated distance for the original node and the spoofing node when using RADAR in the 802.11 network.

VII. Conclusion

In this paper, we have proposed the method for detecting spoofing attacks as well as localizing the attacker in wireless and sensor network. As compared to the traditional identity oriented authentication methods, our RSS based approach does not add network overhead. We proposed the spoofing detection problem as a classical statistical significance testing problem. We then used the K-means cluster to derive statistics. To locate the positions of attackers, we have built a real time localization system and integrated our K-means spoofing detector into the system.

We have experimented the generality and effectiveness of our spoofing detector and localizer in both 802.11 (WiFi) and 802.15.4 (ZigBee) networks in real office building environment. The performance of the K-means spoofing detector is evaluated by using the terms detection rates and receiver operating characteristics curves. After experimentation, we found that our spoofing detector has achieved high detection rates i.e. over 95% and low false positive rates i.e. below 5%. In our real time localization system, we have used point based and area based algorithms to locate the position of attackers. Therefore our experimental results are providing strong evidence of effectiveness and importance of our approach in detecting the spoofing attacks and localization of positions of attackers.

References

[1] M. bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003, pp. 79-87.

[2] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Lhap: A lightweight hop-by-hop authentication protocol for ad-hoc networks," in Proceedings of the IEEE International Workshop on Mobile and Wireless Network (MWN), 2003, pp. 749-755.

[3] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure a1nd efficient key management in mobile ad hoc networks," in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2005.

[4] A. Wool, "Lightweight key management for ieee 802.11 wire- less lans with key refresh and host revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[5] T. Aura, "Cryptographically generated addresses (cga)," RFC 3972, IETF, 2005.

[6] E. Kempf, J. Sommerfeld, B. Zill, B. Arkko, and P. Nikander, "Secure neighbor discovery (send)," RFC 3971, IETF, 2005.

[7] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), September 2006.

[8] Q. Li and W. Trappe, "Light-weight detection of spoofing attacks in wireless networks," in Proceedings of the 2nd International Workshop on Wireless and Sensor Network Security (WSNS), October 2006.

[9] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2006.

[10] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.

[11] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in Proceedings of the International Workshop on Advanced Experimental Activities on Wireless Networks and Systems, 2006.

[12] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS), 2006.

[13] P. Bahl and V. N. Padmanabhan, "Radar: An in-building rf- based user location and tracking system," in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2000, pp. 775-784.

[14] M. Youssef, A. Agrawal, and A. U. Shankar, "Wlan location determination via clustering and probability distributions," in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom), Mar. 2003, pp. 143-150.

[15] E. Elnahrawy, X. Li, and R. P. Martin, "The limits of localization using signal strength: A comparative study," in Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON2004), Oct. 2004, pp. 406-414.

[16] W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 network has no clothes," IEEE Wireless Communications, vol. 9, no. 6, pp. 44-51, Dec. 2002.

[17] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 - 28.

[18] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, "A practical approach to landmark deployment for indoor localization," in Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), September 2006.

[19] A. Haeberlen, E. Flannery, A. Ladd, A. Rudys, D. Wallach, and L. Kavraki, "Practical robust localization over large scale 802.11 wireless networks," in Proceedings of the Annual ACMIIEEE International Conference on Mobile Computing and Networking (MobiCom), September 2004.

[20] T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J. Sievanen, "A probabilistic approach to WLAN user location estimation," International Journal of Wireless Information Networks, vol. 9, no. 3, pp. 155-164, July 2002.

[21] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, "The robustness of localization algorithms to signal strength attacks: a comparative study," in Proceedings of the International Con- ference on Distributed Computing in Sensor Systems (DCOSS), June 2006, pp. 546-563.

[22] T. Hastie, R. Tibshirani, and J. Friedman, the Elements of Statistical Learning, Data Mining Inference, and Prediction. Springer, 2001.