Enhanced Security with Localization of Multiple Spoofing Attackers in Wireless Network

Author: Archana Shelar. Guide: M.D.Ingale

Abstract

As the current age is the age of computers, the wireless spoofing attacks that can be easily launched and these attacks also degrade the performance of the system or networks. The cryptography can be used to maintain security in such networks but such conventional approach can't be desirable due to its overhead requirements. Hence in this paper we propose to use RSS (Received Signal Strength) i.e. the spatial information which is the physical property of each node. This physical property is not reliant on any cryptographic scheme and also it is hard to falsify n hence essential to use. This paper mainly focuses on-A.To Detect spoofing attacks in the network B. Determines the number of attackers C. Localizing multiple attackers.

The spoofing attacks can be detected using RSS (Received Signal Strength) and Medoids levels which can be inherited from wireless nodes in the network. Also we then use the multiclass detection problem to find number of spoofing attackers. Further the IDOL model is used to localize positions of actual attackers. Our experimental results show that the techniques used in this paper provide high level of security with topmost hit rate and precision, also it gives the accuracy in localizing multiple adversaries.

Keywords: - Spoofing attack, Attack detection, Localizing attack, Wireless network security.

1. Introduction.

As computing and performing networks are shifting from wired intrastructure to the wireless, mobile and open communication networks, for increasing the speed of computation. But such networks are easily susceptible for multiple and variety of adversary attacks like spoofing attacks [1][2][3][4]. Basically the identity based spoofing attacks or masquerading attacks are easy to launch and also it can cause significant damage to the network performance. Spoofing attacks also facilitate various types of traffic injection attacks, such as attacks on access control Lists (ACL), rogue access point (AP) attacks, and eventually Denial of-Service (DoS) attacks. The cryptographic techniques can be used to address such type of security violations.

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, these cryptographic methods are also 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 paper work we propose to use received signal strength (RSS)-based spatial correlation. It can be used mainly for- A. Detect the presence of spoofing attacks B.Determine the number of attackers C. Localize multiple adversaries and eliminate them.

RSS it's a physical property associated with each node. It is also hard to falsify and not reliant on cryptography. As here we are concerned with attackers with different locations than legitimate wireless nodes, utilizing such spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. The enhanced advantage of this RSS based spatial co-relation is that--it will not require any additional cost or modification to the wireless devices themselves. Previously the Sheng et al. used RSS and K-means cluster analysis to detect spoofing attacks.

However, none of these approaches have the ability to determine the number of attackers when multiple adversaries use the same identity to launch attacks, which is the basis to further localize multiple adversaries after attack detection. The main focus of our work is—1. A generalized attack detection model (GADE): It can detect the spoofing attack in the network as well as can determine the number of spoofing attackers in the same system. Here the attack detection can be performed using

Partitioning Around Medoids (PAM) which calculates the medoid distance. If the medoid distance value is small it means that spoofing attack is not detected but if it is large then it signifies that spoofing attack is detected. Then we used cluster based Multiclass detection problem to determine number of spoofing attackers. Also further we developed and used the SILENCE mechanism to improve the accuracy of finding number of attackers.

2. Integrated detection and localization system (IDOL):-IDOL can detect the attacks and also can accurately localize the positions of spoofing adversaries or attackers. Here IDOL model uses the results returned by GADE model. One key observation is that IDOL can handle attackers using different transmission power levels, and hence provides strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network.

The rest of the paper is organized as follows.

We provide the Existing Approach in Section 2.We provide Proposed system with model in section 3.We describe cluster based Multiclass Detection Problem in section 4.Then we provide advanced IDOL model in section 5.

2. Existing Traditional Approach.

Cryptography is the traditional approach to prevent and detect spoofing attack. It needs secure key management and respective framework. The Public Key Interface (PKI) can be used further to reduce the overhead of key management [5][6]. Also to avoid key compromisation, wool implemented key management mechanism with periodic key refresh and host revocation.

However such cryptographic authentication may not be always applicable because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network.

For ex. The Wired Equivalent Privacy protocol is used in 802.11 networks to protect link-level data during wireless transmission. It depicts Following properties:-

WEP relies on a secret key shared between the communicating parties to protect the body of a transmitted frame of data. Encryption of a frame proceeds as follows:

Checksumming:

First, we compute an integrity checksum on the message. Then we concatenate the two to obtain a plaintext which will be used as input to the second stage.

Encryption: In the second stage, we encrypt the plaintext derived above using RC_4. We choose an initialization vector (IV). The RC4 algorithm generates a keystream i.e., a long sequence of pseudorandom bytes—as a function of the IV and the key. This Then, we use exclusive-or (XOR, denoted by) the plaintext with the key stream to obtain the ciphertext.

Transmission:

Finally, we transmit the IV and the ciphertext over the radio link.

Recently the current approaches use physical properties like RSS (Received Signal Strength) associated with wireless nodes so as to address spoofing attacks in the wireless network. The channel-based authentication scheme was proposed to discriminate between transmitters at different locations, and thus used to detect spoofing attacks in wireless networks [8].L_i and Trappe [4] introduced a security layer that used forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks. The MAC sequence number has also been used in [9] 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 basic RSS work was also proposed in [3], [7], [10]. 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. Also they do not have the ability to localize the positions of the adversaries after attack detection. Here is the main point that our work uses the spatial information to detect the attacks instead of any cryptographic scheme, and hence it differs from the previous techniques. Additionally our approach is innovative and more creative as it helps find number of spoofing attackers and also gives the accuracy in localizing such multiple adversaries masquerading with the same identity.

3. Proposed System.

- GADE
- IDOL

Fig.1 gives the overall pictorial presentation of this new security technique.

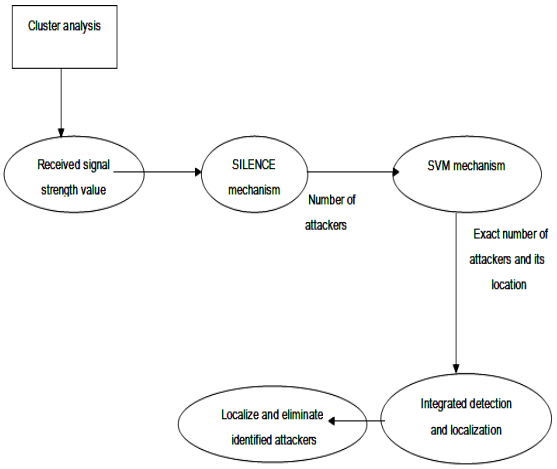

Fig 1.Overall working view of the system

1.GADE(Generalised attack Detection Model):- Here we used to porpose RSS,a physical proprety closely co-related with location in physical space and also it is readily available in the existing wireless networks. As RSS can be affected due to random noise, environmental bias, and multipath effects then also the RSS measured at a set of landmarks is closely related to the transmitter's physical location [11].According to this the RSS readings present strong spatial correlation characteristics.

The RSS vector is defined with value vector as- S= $\{s_1, s_2, s_3 \ldots s_n\}$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations.

In case of spoofing attack, the two main elements are-

- Victim
- Attacker

Here both can transmit data packets by using same ID and the RSS readings of that ID is the mixture of readings measured from each individual node (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space. In this paper work, we propose to use Partitioning Around Medoids (PAM) Method so as to perform clustering analysis in RSS. The PAM Method is a popular iterative descent clustering algorithm [12]. Also the evaluation results showed that PAM method is more robust than popular K-means clustering algorithm [13].Particularly our objective in this method is to detect the presence of attacks. Here null hypothesis indicates that no spoofing attack. T is the Test spec i.e. (Test specification) it is used to indicate wether observed data belongs to the null hypothesis or not. We then consider the distance between two medoids as Dm.

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

Where Mi and Mj are the medoids of two clusters. Under normal condition (i.e. when there is no spoofing attack) it is treated that basically there should be only one cluster from a single physical location. In such normal case D_m should be small. However, under a spoofing attack, there is more than one node at different physical locations claiming the same node identity. As a result, more than one cluster will be formed in the signal space and hence Dm will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space. Finally this model suggests that if the value of D_m distance is small then it means that there is no spoofing attack present in the system. But if D_m distance is large then it means that spoofing attack is detected.

4. Multiclass Detection Problem.

Multiclass detection problem includes determining number of attackers and similar in determining how many clusters existing in the RSS readings.

$$P_i = C_i$$

$$N_i = \bigcup c_j \in C$$

Here C is the set of all classes.c_i is the specific number of attackers under particular class.N_i is the all other class as negative class. The related precision and F-measure are in[14].This gives the number of attackers in the system.

4.1 SILENCE Mechanism.

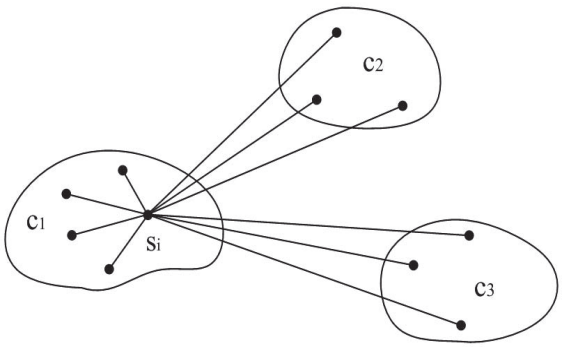

Fig.2.Cluster Representation view

This SILENCE mechanism's basic Silhouette Plot for cluster is in [17][18].Based on this observation we developed SILENCE,SILhouette Plot and System EvolutioN with minimum distanCE of cluster. This evaluates the minimum distance between clusters so as to improve the accuracy of determining the number of Attackers. SILENCE gives the K as number of attackers in the system. This K also depends on Dm-that's the distance between medoids.

4.2 Support Vector Machine (SVM) based mechanism.

SVM is a set of kernel-based learning Methods for data classification that involves a training phase and a testing phase [19]. Here each data instance in the training set consists of a target value (i.e., class label) and several attributes (i.e., features).
The performance of determining number of spoofing attackers can be improved further by using SVM based mechanism. In this section, Support Vector Machines is used to classify the number of spoofing attackers and hence to improve the detection rate. SVM accurately predicts the number of attackers by using model based on training data. The comparison between the results of SVM to those of Silhouette Plot, System Evolution and SILENCE methods leads to the final decision that SVM is the best one as it gives significant increase in Hit rate, Precision etc.

5. IDOL.

This section gives the Integrated Detection and Localization Model. Our integrated detection and localization system makes use of localization algorithm so as to detect or estimate the positions of adversaries or attackers. Here this model utilizes RSS medoids returned from SILENCE as inputs to localization algorithms. The resulted returned positions include the location estimate of the original node and the attacker in the physical space. When an adversary residing at a physical location
Varies its transmission power to perform a spoofing attack, the difference of the RSS readings between two different landmarks from the adversary is a constant since the RSS readings are obtained from a single physical location. We can then utilize the difference of the medoids vectors in signal space obtained from SILENCE to localize adversaries. In this way on improving [14] the advanced enhancement is obtained as IDOL.
The proposed model makes use of three such localization algorithms:-

- RADAR Grid algorithm
- Area Based Probabilistic algorithm
- Multilateration algorithm

1. RADAR Grid: -

This algorithm is the scene matching algorithm given in [15].It uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. It 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.

2. Area Based Probabilistic algorithm:

This algorithm is given in [16].Then here it is further extended to give value of P (L_i/S).
Here the given 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

$$P(L_i/S) = P(S/L_i) \times P(L_i)/P(S)$$

This gives the probable area of location where the attackers or adversaries may be present. From this probable location actual position of adversaries can be obtained in terms of x and y co-ordinates using multilateration algorithm.

3. Multilateration algorithm:

Bayesian network localization is the multilateration algorithm [19].This proposed algorithm encodes signal to distance propagation model into Bayesian Graphical Model for localization.

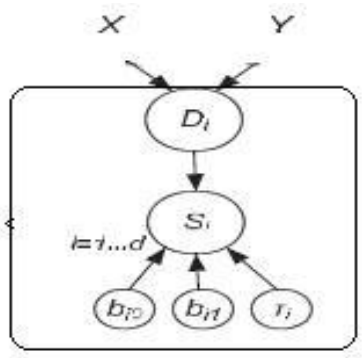

Fig 3.Bayesian Model Overview

Here Di represents the Euclidean distance between the location specified by X and Y. (x_i, yi) be the co-ordinates of i^{th} landmark.

$$D_i = \sqrt{(X-x_i)^2 + (Y-y_i)^2}$$

This determines the actual position of adversaries in wireless network.

6. Conclusion.

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]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.

[9] 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.

[10] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," *Proc. IEEE INFOCOM, pp*. 2137- 2145, 2008.

[11] 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.

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

[13] 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.

[14] C. van Rijsbergen, Information Retrieval, *second ed. Butterworths,*1979.

[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] P. Rousseeuw, "Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis," *J. Computational and Applied Math., vol*. 20, no. 1, pp. 53-65, Nov. 1987.

[18] K. Wang, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," *Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China,* 2007.

[19] D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S. Krishnakumar, "Bayesian Indoor Positioning Systems," *Proc. IEEE INFOCOM, pp*. 324-331, Mar. 2005.