www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Sep 2015, Page No. 14517-14522

Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

P.Venkteswarlu[#1], Smt. S. Jhansi Rani[#2]
#1 Dept. of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, venki.1032@gmail.com
#2 Assistant Professor, Dept. of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, Jhansirani_auce@yahoo.com

Abstract: - Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In this paper, we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. 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 (WiFi) network and an 802.15.4 (ZigBee) 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***.

I. 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 [5] are especially easy to launch and can cause significant damage to network 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. In spite of existing 802.11
security techniques including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames an attacker frames an attacker can still spoof management to cause significant impact on networks.

Spoofing attacks can further facilitate a variety of traffic injection attacks [10], such as attacks on access control ists, rogue access point (AP) attacks, and eventually Denial of-Service (DoS) attacks [1]. 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 [2]. Therefore, it is important to

- detect the presence of spoofing attacks,

- Determine the number of attackers,
- Localize multiple adversaries.

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[3], 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. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.
The main contributions of our work are:

GADE: a generalized attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods [4] grounded on RSS-based spatial correlations among normal devices and adversaries. In this we are used the Partitioning around Medoids (PAM) cluster analysis method to perform attack detection.

IDOL: an integrated detection and localization system (IDOL) that can both detect attacks as well as find the positions of multiple adversaries. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker. We further developed a mechanism called SILENCE for testing Silhouette Plot and System Evolution with minimum instance of clusters, to improve the accuracy of determining the number of attackers. Additionally, when the training data are available, we propose to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. As we demonstrated through our experiments using both an 802.11 network as well as an 802.15.4 network in two real office building environments, GADE is highly effective in spoofing detection with over 90 percent hit rate and precision. Furthermore, using a set of representative localization algorithms, we show that IDOL can achieve similar localization accuracy when localizing adversaries to that of under normal conditions. One key observation is that IDOL can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network.

The remainder of the paper is organized as follows. Section 2 explores the details about the generalized attack detection model (GADE) approach. Integrated detection and localization system (IDOL) and algorithm are discussed in Section 3. The performance comparisons are discussed in Section 4. The conclusion and the future work are presented in Section 5 and Section 6.

II. GADE

GADE (generalized attack detection model) and this GADE is divided in to two process spoofing attack detection and attack number determination .for that spoofing attack detection we use the process of RSS i.e. Received signal strength for the received signal strength we use the cluster analysis and the result is finalized whether there is attack happened or not.

A. **Spatial Correlation of RSS:**

The main challenge in spoofing detection is devise strategies that use uniqueness of spatial information but not using location directly as the attackers positions are known. Here we propose to study RSS a closely correlated with the location in

physical space and is readily available in the existing wireless network. The RSS measured at a set of landmarks is closely related to the transmitter 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 the different locations in physical space are distinctive. The RSS readings present strong spatial correlation characteristics.

The RSS value vector as $S = \{S_1, S_2, S_3 \ldots\ldots S_n\}$

Here 'n' is the number of landmarks

The RSS at the i_{th} landmark from a wireless node is lognormally distributed .

$$S_i(d_j)[dBm] = P(d_0)[dBm] - 10\gamma\log(\frac{dj}{d0}) + X_i \text{ Here}$$

$P(d_0)$ represent the transmitting power of the node at the reference distance d_o , d_j is the distance between the wireless node j and i_{th} landmark.

γ is the path loss exponent

X_i is the shadow fading which follow zero mean Gaussian distribution with δ standard deviation. If two wireless nodes in physical space the RSS distance between two nodes in signal space at the i_{th} landmark is given by

$$\Delta S_i = 10\gamma\log(\frac{d2}{d1}) + \Delta X$$

B. **Attack Detection Using Cluster Analysis:**

The Spatial Correlation of RSS analysis provides the theoretical support of using the RSS based spatial correlation inherited from wireless nodes to perform spoofing attack detection[7][8]. The RSS readings from a wireless node may fluctuate and should cluster together. 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 the time should from different clusters in signal space. Under the spoofing attack the victim and 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.

Under the spoofing attack the RSS readings from the victim node and 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. To perform the cluster analysis in RSS we utilize partitioning around medoids [PAM] method. The PAM method is a popular iterative descent clustering algorithm. Which is used compare the popular K-means method . And the PAM method is more robust in presence of noise and outliers. 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 .

We formulate the spoofing detection as a statical significance testing problem. And the null hypothesis is

H_0 : normal (no spoofing attack)

Here T is used to evaluate whether observed data belong to the null-hypothesis or not. In our attack detection phase we partition the RSS vectors from the same node identity into clusters to detect the presence of attacks. And we calculate the distance between two medoids D_m.

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

Here M_i, M_j are the medoids of the two clusters.

Under the normal conditions D_m should be small since there is basically only one cluster from a single space location .in spoofing attack there is more than one node at different physical locations claiming same node identity .due to this more than one clusters will be formed in signal space and D_m will be large . Medoid is nothing but one element from each cluster.

C. **Result of Attack Detection:**

- If the Dm > T then spoofing happened.

Here D_m is the distance between two medoids , T is the threshold.

DOI: 10.18535/ijecs/v4i9.75

D. **Attack Number Determination:**

For the attack number determination we use the silhouette plot [4]. A silhouette plot is a graphical representation of a cluster [4] which is used to determine the number of attackers. The illustration of silhouette plot is shown in below.

The RSS sample points S = (S_1 ,…….S_N) Here N is the total number of samples

Let

C = (C_1 ,…….C_k) Here K is the number of clusters .

$D(s_k,s_l)$ is the distance between s_k and s_l

Let

C_j = {S^j_1,……S^j_{mj}} is the j_{th} cluster

Here j = 1 ……K where $m_j = |c_j|$

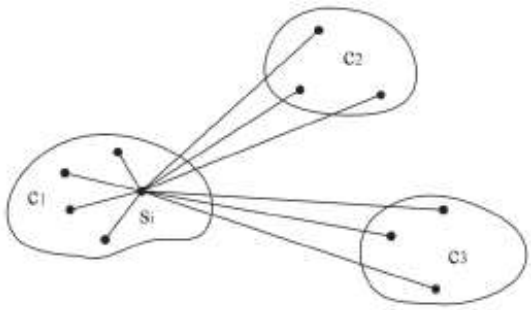

Fig 4.1.1 silhouette plot

The silhouette index for partition P that partitions the data set into K clusters is

$$W(K)_p = \frac{1}{K}\sum_{j=1}^{K} wj$$

The silhouette coefficient SC is used to determine the number of attackers. And it selects best value of number K by choosing the K to make W(K) as high as possible across all partitions.

$$SC = \max_k W(K)_p$$

E. **System Evolution:**

This method is used to analyze cluster structure and estimate number of clusters and it is used twin-cluster model. Twin-cluster model is used for energy calculation. Here we calculate the partition energy (E_p (k)) and merging energy (E_m (k)). The partition energy denotes the border distance between the twin clusters and merging energy denotes the average distance between elements in the border region of the twin clusters.

Partition Energy Ep(K) as

$$E_p(k) = \frac{1}{na+nb}\{\sum_{i=1}^{na} min_{j=1\ldots\ldots nb} D(a_i,b_j) + \sum_{j=1}^{nb} min_{i=1\ldots\ldots na} D(a_i,b_j)\}$$

Merging Energy $E_m(K)$ as

$$E_m(K) = \frac{1}{na+nb}\sum_{i=1}^{(na+nb-1)}\sum_{j=i+1}^{(na+nb)} D(S_i, S_j)$$

Here $D(a_i,b_j)$ is the Euclidean distance between the elements a_i and b_j in the cluster a and b. and $X_{si,sj}$ which are elements in the border region of the twin cluster.

If $E_p(K) > E_m(K)$ and $E_p(K+1) <= E_m(K+1)$ then we identify the adversaries in the network using the same node identity to perform spoofing attacks.

III. IDOL:

Integrated detection and localization system utilizes the RSS medoids returned from GADE as inputs to localizations algorithms to estimate the positions of adversaries. Here we use the Bayesian networks[6] for localizing the attackers in the network.

A. **Algorithm:**

Bayesian Network localization is a multilateration algorithm that encodes the signal-to-distance propagation model into Bayesian graphical model for localization.

DOI: 10.18535/ijecs/v4i9.75

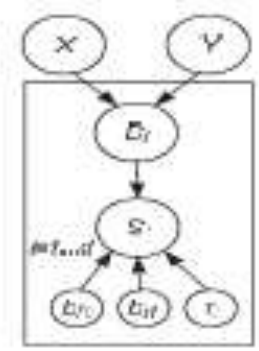

Fig 4.1.2 Bayesian network

The vertices X and Y represent location.

The vertex Si is the RSS reading from the land mark.

The vertex Di represents the Euclidean distance between the locations specified X and Y and the i^{th} landmark.

The value of Si follows a signal propagation model

$$Si = b_{0i}+b_{1i}lod\ Di$$

Here b_{0i}, b_{1i} are the parameters specific to the ith landmark.

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

Bayesian returns the sampling distribution of possible location of X and Y as the localization results.

IV. Performance Comparisons:

The 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. The accuracy of determining the number of attackers. Additionally, when the training data are available, we propose to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

The basic idea behind using the System Evolution method to determine the number of attackers is that all the rest of clusters are separated if the twin clusters are separable. The Hit Rate is lower when treating four attackers as errors than treating two attackers as errors. This indicates that the probability of misclassifying three attackers as four attackers is higher than that of misclassifying three attackers as two attackers. 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.

V. Conclusion

In this paper, we proposed to use received signal strength based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks[9]. We provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. We derived the test statistic based on the cluster analysis of RSS readings. Our approach can both 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. Determining the number of adversaries is a particularly challenging problem. We developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution, which use cluster analysis alone. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system.

VI. Future Work

We have to implement this project further by using the training data which is collected from offline, we propose to use the Support Vector

Machines (SVM) method to further improve the accuracy of determining the number of attackers.

VII. 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] 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.

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

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

[6] D. Madigan, E. Elanhrawy, R. Martin, W, Ju, P. Krishnan, and A.S. Krishna Kumar , "Bayesian Indoor Positioning System," proc. IEEE INFOCOM, pp. 324-331, Mar. 2005.

[7] 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.

[8] 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.

[9] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[10] Q. Li and W. Trappe, "Relationship-Based Detection of SpoofingRelated Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.