INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online),
Volume 4, Number 2, April- June (2014), pp: 9-17

IJCSERD

© PRJ PUBLICATION

PREPARATION GADE AND IDOL MODEL FOR PREVENTING MULTIPLE SPOOFING ATTACKERS IN WIRELESS NETWORKS

[1]Sheetal Pimpale, [2]Krishna Mohana A.J, [3]Dr. Antony P.J

[1]Department of Computer science and Engineering, VTU Belgaum KVGCE, Sullia-574324
[2]Assoc. Professor, Department of Computer science and Engineering, VTU Belgaum KVGCE
[3]Director of PG Studies, Department of Computer science and Engineering, VTU Belgaum KVGCE

ABSTRACT

The Many wireless networks are susceptible to spoofing attacks. In which the identity of a node can be verified through cryptographic authentication but authentication is not always possible because it requires key management and additional infrastructural overhead. This paper propose to show that use spatial information and physical property associated with each node as hard to specifies but not reliant on cryptography, as the basis for-detecting spoofing attacks and determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries and need to propose the use of spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. The problem consists of determining the number of attackers as a multiclass detection problem. The cluster-based mechanisms are developed to determine the number of attackers. When the training of data are available, then using the Support Vector Machines (SVM) method to improve the accuracy of determining the number of attackers. Evaluate the techniques through two test beds using both an 802.11 (Wi-Fi) network and an 802.15.4 (ZigBee) network in two real office buildings. This experiment results show that the propose methods can achieve over 90 percent Hit Rate and Precision when determining the number of attackers and use set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

Key words: spoofing attack, attack detection, localization, Wireless network security.

I. INTRODUCTION

The more wireless and sensor networks are deployed; they will increasingly become tempting targets for malicious attacks. The adversaries can easily purchase low-cost wireless

devices and use these commonly available platforms to launch a variety of attacks with little effort. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. In existing of 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames-an attacker can still spoof management or control frames to cause significant impact on networks. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, access point (AP) attacks, and eventually Denial of-Service (DoS) attacks.

It is important to detect the presence of spoofing attacks and determine the number of attackers then localize multiple adversaries. 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 and eliminate them. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead.

It propose to use received signal strength (RSS)-based spatial correlation and physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. 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 grounded on RSS-based spatial correlations among normal devices and adversaries. IDOL: an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. It is important to detect the presence of spoofing attacks and determine the number of attackers then localize multiple adversaries. It formulates the problem of determining the number of attackers as a multiclass detection problem. As 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. In which by using a set of representative localization algorithms and show that IDOL can achieve similar localization accuracy when localizing adversaries to that of under normal conditions and achieve the various spoofing attacks in wireless networks.

II. RELATED WORK

SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. An authentication framework for hierarchical, ad hoc sensor networks is proposed in [10]. The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication [5, 6, and 10]. Wu et al. [5] have introduced a secure and efficient key management (SEKM) framework. The 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. Brik et al. [12] focused on building fingerprints of 802.11b WLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. Sheng et al. [7] modelled the RSS readings using a Gaussian mixture model. Sang and Arora [14] proposed to use the node's "spatial signature, "including Received Signal Strength Indicator (RSSI) and

Link Quality Indicator (LQI) to authenticate messages in wireless networks. Another method of classification describes the strategy used to map a node to a location. Later approaches [19] use distances to landmarks, while angulations uses the angles from landmarks.

III. SCOPE OF PROPOSED SCHEME

A. Generalized Attack Detection Model

This Paper makes to describe the Generalized Attack Detection Model which consists of two phases: attack detection which detects the presence of an attack and number determination and also determines the number of adversaries.

1) Theoretical Analysis of the Spatial Correlation of RSS: This paper Proposed to study RSS, a property closely correlated with location in physical space and is readily available in the Existing wireless networks. The challenge in spoofing detection is to devise strategies that use the uniqueness of spatial information, but not using location directly as the attackers' positions are unknown. so it affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks [17]. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive.

Where $s_i(d_j)[dB_m]=p[d_0][dB_m]-10\log(d_j/d_0)+x_i$.wherep$[d_0]$represents a given two wireless nodes in the physical space, the RSS distance between two nodes in signal space at the i^{th} landmark is given by $\Delta s=10\log(d_2/d1)+\Delta x_1$, where Δx_1follows zero mean Gaussian distribution with standard deviation. Fig. 1 presents the numerical results of receiver operating characteristic (ROC) curves based .when randomly placing two wireless devices in a 100 by 100 feet square area. There are four landmarks deployed at the four corners of the square area.

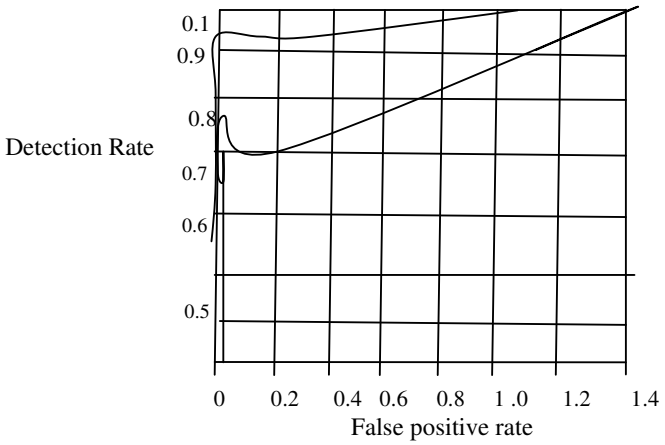

Fig. 1 presents the numerical results of receiver operating characteristic (ROC).

2) Attack Detection Using Cluster Analysis: In this paper that might be RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. The above analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node (i.e., spoofing node or victim node).

3) Evaluation Strategy: Test the performance of the attack detection approach to evaluate an approach in real office building environments. They conduct experiments in two office buildings: one is the Wireless Information Network Laboratory (WINLAB) using an 802.11 (WiFi) network and the other is the Computer Science Department at Rutgers University using an 802.15.4 (ZigBee) network. In this addition, then make to build an integrated system to both detect attacks as well as localize the positions of adversaries and during the localization process, the following steps.

- A Transmitter sends a packet. Some number of Landmarks observes the packet and records the RSS.
- Each Landmark forwards the observed RSS from the transmitter to the Server.
- The Server collects the complete RSS vector for the transmitter and sends the information to a solver instance for location estimation.
- The Solver instance performs localization and returns the coordinates of the transmitter back to the Server. If there is a need to localize hundreds of transmitters at the same time, the server can perform load balancing among the different solver instances.

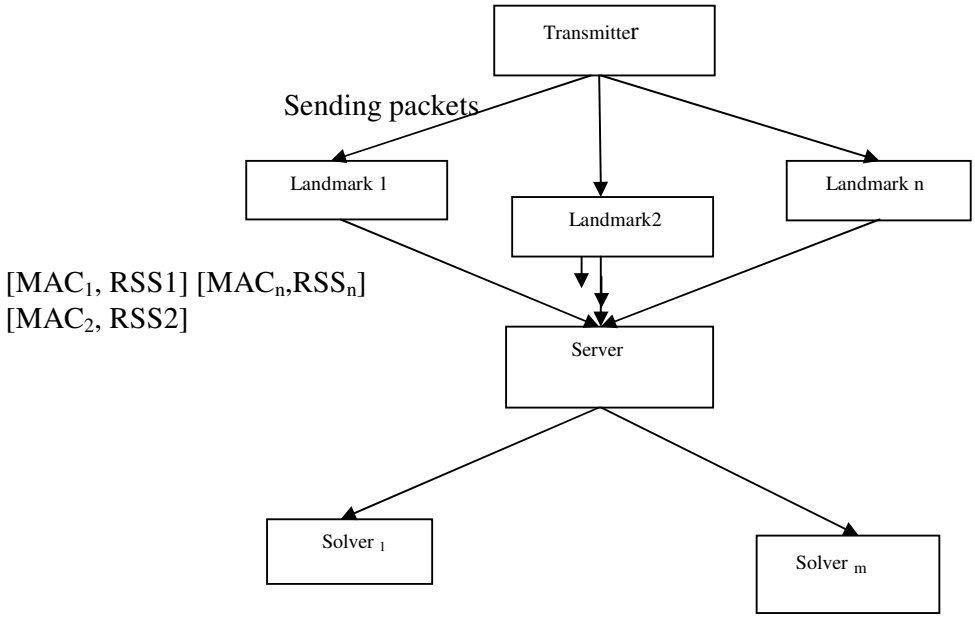

Figure 2: Location of System Architecture

4) Impact of Threshold and Sampling Number: The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a thresh-hold enables the attack detector to be robust to false detections and euclidean distance calculation given below.

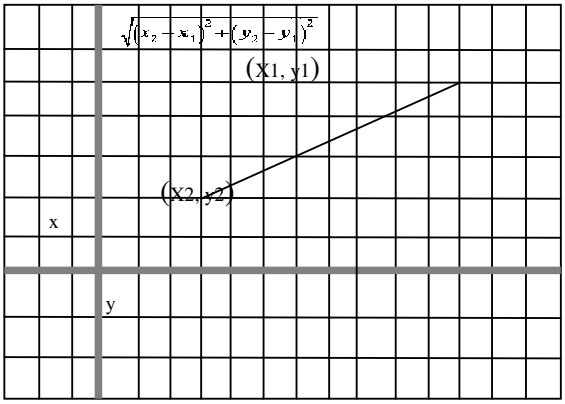

Fig. 3 shows the Cumulative Distribution Function.

Fig. 3 shows the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. They may observe that the curve of Dm shifted greatly to the right under spoofing attacks. Thus, when Dm > □.It can declare the presence of a spoofing attack. The short lines across the CDF lines are the averaged variances of Dm under different sampling numbers.

5) Handling Different Transmission Power Levels: If a spoofing attacker sends packets at a different transmission power level from the original node, based on our cluster analysis there will be two distinct RSS clusters in signal space (i.e., Dm will be large). They varied transmission power for an attacker from 30 mW (15 dBm) to 1 mW(0 dBm). It found that in all cases Dm is larger than normal conditions. It represents an example of the Cumulative Distribution Function of the Dm for the 802.11 network when the spoofing attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB transmission power levels. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

6) Performance of Detection: To evaluate the effectiveness of using cluster analysis for Attack detection and presents the Receiver Operating Characteristic curves of using Dm as a test statistic to perform attack detection for both the 802.11 and the 802.15.4 networks and the detection rate and false positive rate for both networks under different threshold settings. The results are encouraging, showing that for false positive rates less than 10 percent, the detection rate are above 98 percent when the threshold is around 8 dB. Even when the false positive rate goes to zero, the detection rate is still more than 95 percent for both networks is still more than 95 percent for both networks.

IV. DETERMINING THE NUMBER OF ATTACKERS

A. Problem Formulation

The problem consist of cryptographic schemes requires a 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. Due to the openness of the wireless transmission medium adversaries can monitor any transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance.

B. Silhouette Plot

A Silhouette Plot is a graphical representation of a cluster. To determine the number of attackers, May construct Silhouettes in the following way: the RSS sample points $s=\{s_1\ s_2 \ldots s_n\}$.The detection rate as a function of the distance between the spoofing node and the original node. The average distance between the i^{th} RSS vector in the cluster and the other RSS vectors in the same cluster is thus given by each RSS value. Finally need to define Silhouette Coefficient (SC) to determine the number of attackers.

C. System Evolution

The System Evolution is a new method to analyse cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters (e.g., clusters a and b) among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is calculated as the average distance between elements in the border region twin cluster.

D. The SILENCE Mechanism

The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters. However, we observed that for both Silhouette Plot and System Evolution methods, the Hit Rate decreases as the number of attackers increases, although the Precision increases. This is because the clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions.

E. Support Vector Machines-Based Mechanism

Provided the training data collected during the offline training phase, it can further improve the performance of determining the number of spoofing attackers. In addition to given several statistic methods available to detect the number of attackers, such as System Evolution and SILENCE, So need to can combine the characteristics of these methods to achieve a higher detection rate.

F. Experimental Evaluation

They validate of effectiveness of the SVM-based mechanism for determining the number of attackers, they randomly choose half of the data as training data, whereas the rest of data for testing. The features may used are the combination of the difference of partition energy and merge energy from System Evolution and the minimum distance between two clusters from SILENCE.

V. ANOTHER SCOPE OF PROPOSED SCHEME IS IDOL: INTEGRATED DETECTION AND LOCALIZATION FRAMEWORK.

The integrated system that can detect spoofing attacks, determine the number of attackers and localize multiple adversaries. The experiment results are present to evaluate the effectiveness of this approach and especially when attackers using different transmission power levels.

A. Framework

The Different from traditional localization approaches to integrated detection and localization system utilize the RSS medoids returned from SILENCE as inputs to localization algorithm to estimate the positions of adversaries. The traditional localization approaches are based on averaged RSS from each node identity inputs to estimate the position of a node. However, in wireless spoofing attacks, the RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations.

B. Algorithms

RADAR-gridded: The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from [15]. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known locations.

Area-based Probability: It utilizes an interpolated signal map. Further, the experimental area is divided into a regular grid of equal-sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector s. ABP then computes the probability of the wireless device being at each title.

Bayesian-Networks: BN localization is a multi-late ration algorithm that encodes signal-to-distance propagation model into Bayesian Graphical Model for localization. The vertices X and Y represent location and the vertex s_i is the RSS reading from the i^{th} landmark.

VI. PERFORMANCE ANALYSIS

The cluster-based mechanisms are developed to determine the number of attackers even when the training of data are available, then using the Support Vector Machines (SVM) method to improve the accuracy of determining the number of attackers. This experiment results show that the propose methods can achieve over 90 percent Hit Rate and Precision when determining the number of attackers and use set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries. To evaluate the effectiveness of using cluster analysis for attack detection, perform attack detection for both the 802.11 and the 802.15.4 networks. The results are encouraging, showing that for false positive rates less than 10 percent, the detection rate are above 98 percent.

To evaluate the performance approach by using the difference of returned medoids-Adversaries used the same transmission power levels as the original node and the returned medoids are used and Adversaries changed their transmission power level from 15 to 10 dB and the returned medoids are used; the localization performance is much worse than the traditional approaches if the difference of returned medoids is not used when localizing adversaries using different transmission power levels. When using in this approach, It can achieve the median error of 13 feet for both RADAR-Gridded and ABP will achieve 40-50

percent performance improvement, comparing to the median errors of 20 and 19 feet for RADAR Gridded and ABP, respectively. Thus, IDOL is highly effective in localizing multiple adversaries with or without changing their transmission power levels. Adversaries changed their transmission power level from 18 to 15 dB and the returned medoids are used; the localization performance is much worse than the traditional approaches.

VII. CONCLUSION

In this work, They may 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. It provides theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. In this approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

REFERENCES

[1] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. USENIX Security Symp, pp. 15-28, 2003.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.

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

[4] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[5] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and Efficient Key Management in Mobile Ad Hoc Networks,” Proc. IEEE Int’l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[6] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans with Key Refresh and Host Revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,” Proc. IEEE INFOCOM, Apr. 2008.

[8] J. Yang, Y. Chen, and W. Trappe, “Detecting Spoofing Attacks Mobile Wireless Environments,” Proc. Ann. IEEE Comm. Soc. Conf.Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

[9] Y. Chen, W. Trappe, and R.P. Martin, “Detecting and Localizing Wireless Spoofing Attacks,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[10] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. Xiao,L.J.

[11] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646-4651, June 2007.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

[13] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

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