IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Spotting and Pinpointing Various Spoofing Adversaries in Wireless Network

Ramya Devi P[1], Ruby Sherly G[2], Hari Prasath L[3]

[1, 2]Student, Department of Information Technology, Anand Institute of Higher Technology, Chennai

[3]Assistant Professor, Department of Information Technology, Anand Institute of Higher Technology, Chennai.

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. This paper proposes 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 a same node identity ; and (3) localizing multiple adversaries. The spatial correlation of received signal strength (RSS) inherited from wireless node is used to detect the spoofing attacks. Then the problem of determining the number of attackers as multiclass detection problem is formulated. Cluster-based mechanism is developed to determine the number of attackers. When the training data is available, Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers. In addition, integrated detection and localization system is used to localize the positions of multiple attackers.

Keywords— *Wireless network security, spoofing attack, attack detection, localization*

1. INTRODUCTION

In wireless transmission medium the attackers can monitor any transmission. Among various types of attacks, spoofing attacks are especially easy to launch and cause significant damage to network performance. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue access point attacks, and eventually Denial-of- Service (DoS) attacks. 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.

Therefore, it is important to

- detect the presence of spoofing attacks,
- determine the number of attackers, and
- localize multiple adversaries and eliminate them.

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 RSS-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since we are concerned with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. 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.

We focus on static nodes in this work, which are common for spoofing scenarios. We addressed spoofing detection in mobile environments in our other work. The works that are closely related to us are proposed the use of matching rules of signal prints for spoofing detection, modelled the RSS readings using a Gaussian mixture model and 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 a same identity to launch attacks, which is the basis to further localize multiple adversaries after attack detection. Although studied how to localize adversaries, it can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power levels.

The main contributions of our work are:

- **GADE:** A generalized attack detection model 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; and

- **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.

In GADE, the Partitioning Around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multi-class 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 distance of clusters, to improve the accuracy of determining the number of attackers. Additionally, when the training data is available, we propose to use 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% 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.

2. SCOPE OF THE PAPER

The scope of this paper is to detect spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. The transmitted information from server is send to client in secure manner. If an intruder comes during transaction server discover and localize that specific system.

3. EXISTING SYSTEM

The identity of a node can be verified through conventional security approaches are not always desirable. Adversaries can easily purchase low-cost devices and use these commonly available platforms to launch a variety of attacks. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance in passive monitoring and then modify its MAC address. It can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, rogue access point (AP) attacks, and eventually denial of service (DOS) attacks. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices. and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network.

4. PROPOSED SYSTEM

The proposed system uses received signal strength (RSS)-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Cluster Based wireless Sensor Network data received signal strength (RSS) based spatial correlation of network Strategy. Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. Comparing to other methods the benefits of SVM are more. SVM is generic because their only goal is to filter spoofed packets. In localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries. 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.

5. OVERVIEW OF TECHNIQUES

(i) Generalized Attack Detection Model

In this section, we describe our Generalized Attack Detection Model (GADE), which consists of two phases: *attack detection*, which detects the presence of an attack, and *number determination*, which determines the number of adversaries.

(ii) Determining the number of attackers

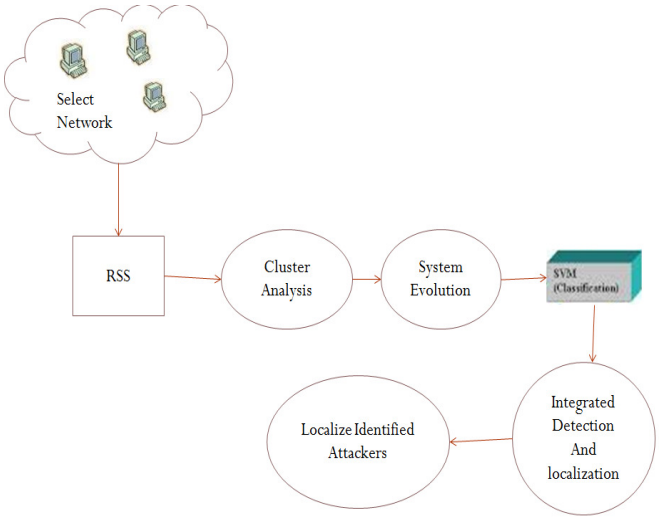
Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS readings.

(iii) Integrated detection and localization framework

In this section we present our integrated system that can both detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach,

especially when attackers using different transmission power levels.

(iv) Data Flow Diagram



5. MODULES DESCRIPTION

Attack Detection

Spoofing detection is to devise strategies that use the uniqueness of spatial information. In location directly as the attackers' positions are unknown network RSS, a property closely correlated with location in physical space and is readily available in the wireless networks. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. The number of attackers when there are multiple adversaries masquerading as the same identity.

Partitioning Around Medoids

Localization is based on the assumption that all measurements gathered received signal strength (RSS) are from a single station and, based on this assumption, the localization algorithm matches a point in the measurement space with a point in the physical space. 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. RSS - based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

Attacker Number Determination

The System Evolution is a new method to analyze cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters 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 of the twin clusters.

Finding feasible path

Convert the large dataset into medium format for the computation purpose. In this medium the rows consists of http request and columns consists of time for a particular user (IP address).Received Signal Strength Indicator Formula, 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.

Constructing Inter-Domain Packet Filters

The clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions and fake RSS clusters caused by outliers and variations of the signal strength. The minimum distance between two clusters is large indicating that the clusters are from different physical locations. The minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers.

Receiving the valid packets

The transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately. The CDF of localization error for RADAR - Gridded and ABP when adversaries using different transmission power levels. In detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of network.

6. ALGORITHMS

RSS distance calculation:

The RSS distance between the two nodes in signal space is calculated by,

$$\Delta s_i = 10\gamma \log\left(\frac{d_2}{d_1}\right) + \Delta X,$$

Where the d1 and d2 are the distance between two wireless nodes and X is a zero mean Gaussian distribution with sqrt(2δ) standard deviation.

Distance between two mediods:

The group of cluster is called as the mediods.The distance between the group of cluster is calculated by,

$$D_m = \|\mathbf{M_i} - \mathbf{M_j}\|,$$

Where Mi and Mj are the mediods of two cluster and Dm is the distance between two mediods.

The condition to find out the presence of spoofing attack is,

Dm > Threshold

Attacker Number Determination:

System Evolution method uses the twin cluster model which is nothing but the two closest clusters.This odel is used for energy calculation. The partition energy Ep(K) is calculated by,

$$E_p(K) = \frac{1}{n_a + n_b}\left\{ \sum_{i=1}^{n_a} \min_{j=1,\dots n_b} D(a_i, b_j) + \sum_{j=1}^{n_b} \min_{i=1,\dots n_a} D(a_i, b_j) \right\},$$

Where na and nb is the number of sample points,and the merging energy Em(K) is calculated by,

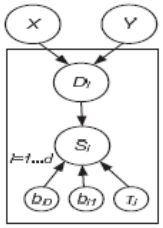
$$E_m(K) = \frac{1}{\binom{n_a+n_b}{2}} \sum_{i=1}^{(n_a+n_b-1)} \sum_{j=i+1}^{(n_a+n_b)} D(\mathbf{s_i}, \mathbf{s_j}),$$

Where D(si,sj) is the Euclidian distance between the elements of cluster a and b. The condition to determine the number of attackers

When K = n with Ep(K) > Em(K)

Bayesian Networks (BN):

BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Figure 13 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex si is the RSS reading from the ith landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of si follows a signal propagation model si = b_{0i}+b_{1i} logDi, where b_{0i}, b_{1i} are the parameters specific to the ith landmark.



Bayasian graphical model in our study

The distance Di =$\sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τi: si~N(b_{0i} + b_{1i} logDi, τ_i). Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

7. CONCLUSION

In this work, we proposed to use received signal strength (RSS) 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. 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 that use cluster analysis alone. Additionally, when the training data is available, we explored using Support Vector Machines (SVM) based mechanism to further improve the accuracy of determining the number of attackers present in the system.

To validate our approach, we conducted experiments on two test-beds through both an 802.11network (Wi-Fi) and an 802.15.4 (Zig-Bee) network in two real office building environments. We found that our detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of adversaries, achieving over 90% hit rates and precision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. 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]. Jie Yang, Yingying Chen, and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE 2012.

[2]. 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.

[3]. F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to dos attacks in 802.11 networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2004.

[4]. 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.

[5]. Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in *Proc. IEEE SECON*, 2006.

[6]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in *Proc. IEEE IPDPS*, 2005.

[7]. 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.

[8]. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. IEEE INFOCOM*, April 2008.

[9]. J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Proc. IEEE SECON*, 2009.

[10]. Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wirelss spoofing attacks," in *Proc. IEEE SECON*, May 2007.