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

Detection and Localization of Multiple Spoofing using GADE and IDOL in WSN

U.Kavitha[1]

[1]**PG Student, Department of ECE, CK College of Engineering & Technology, Cuddalore, Tamil Nadu, India**

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. Spatial information, a physical property associated with each node, that is hard to falsify, and not reliant on cryptography is used, 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. Thus received signal strength (RSS) is inherited from wireless nodes to detect the spoofing attacks. Cluster-based mechanisms are developed to determine the number of attackers. In addition, an integrated detection and localization system is developed that can localize the positions of multiple attackers. Thus this detection and localization results provide strong evidence in detecting multiple adversaries.

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

1. 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 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 802.11security 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 [1], such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial-of-Service (DoS) attacks. A broad survey of possible spoofing attacks can be found in [2], [4]. 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 to1) detect the presence of spoofing attacks, 2) determine the number of attackers, and 3) localize multiple adversaries and eliminate them.

Most existing approaches to address potential spoofing attacks employ cryptographic schemes [5], [6]. 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, 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 is used 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.

Thus the focus is on mobile nodes in this work, which are common for spoofing scenarios [7]. The works that are closely related are [2], [7], [9]. Chen et al. [9] 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. Although Chen et al. [9] 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 are: 1) 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; and 2) 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, cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. A cluster-based methods is applied to determine the number of attacker.

Moreover, an integrated system, IDOL, which utilizes the results of the number of attacker returned by GADE is used to further localize multiple adversaries. 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 attacker's in the network.

The rest of the paper is organized as follows. Theoretical analysis and the generalized attack detection model is provided in Section 2. the problem of determining the number of attacker using multiclass detection is provided in section 3.In Section 4. IDOL, the integrated detection and localization system. is presented. results and discussion is illustrated in section 5,Finally, the conclusion of the work in Section 6.

2. Generalized Attack Detection Model

In this section, Generalized Attack Detection ModEl, is described which consists of two phases: attack detection, which detects the presence of an attack, and number determination, which determines the number of adversaries. The number determination phase will be presented in Section 3.

2.1 Theoretical Analysis of the Spatial Correlation of RSS

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. Thus study of RSS, a property closely correlated with location in physical space and is readily available in the existing wireless networks. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks is closely related to the transmitter' s 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 different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

The RSS value vector is defined as $s = \{s_1, s_2, \ldots, s_n\}$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations. Generally, the RSS at the i^{th} landmark from a wireless node is log normally distributed Eq.(1)

$$s_i(d_j)[dB_m] = P(d_0)[dB_m] - 10_\gamma \log(\frac{d_j}{d_0}) + X_i \qquad (1)$$

where $P(d_0)$ represents the transmitting power of the node at the reference distance d_0 , d_j is the distance between the wireless node j and the i^{th} landmark, and γ is the path loss exponent, X_i is the shadow fading which follows zero mean Gaussian distribution with δ standard deviation Eq.(1),(2). For simplicity, assume the wireless nodes have the same transmission power. 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

$$\Delta s_i = 10_\gamma \log(\frac{d_j}{d_0}) + \Delta X_i \qquad (2)$$

where ΔX follows zero mean Gaussian distribution with $\sqrt{2}\delta$ standard deviation.

The square of RSS distance in n-dimensional signal space is then determined by

$$\Delta D^2 = \sum_{i=1}^{n} \Delta s_i^2 \qquad (3)$$

where Δs_i with $i = 1, 2, \ldots, n$ is the RSS distance at ith landmark and is given by Eq.(3).

2.2 Attack Detection Using Cluster Analysis

The above analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that the RSS readings from a wireless node may fluctuate and should cluster together. In particular, 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 time should form different clusters in signal space. We illustrated this important observation in Fig. 1, which presents RSS reading vectors of three landmarks from two different physical locations. 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. 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.

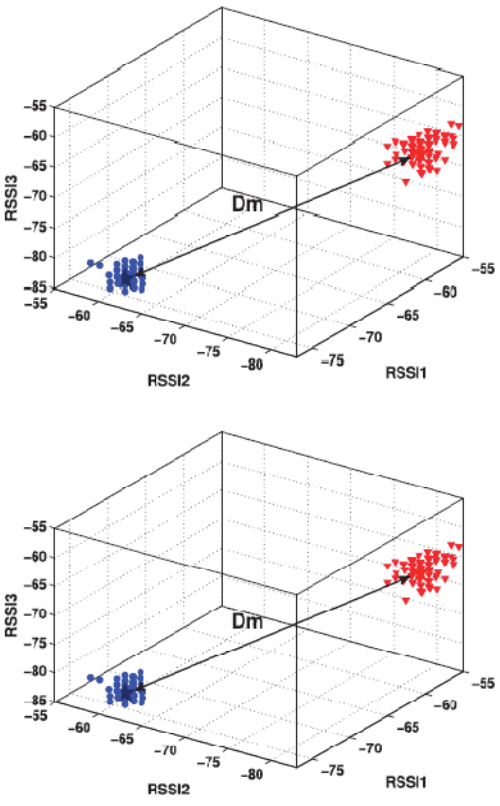

Fig. 1 Illustration of RSS readings from two physical locations.

2.3 Results of Attack Detection

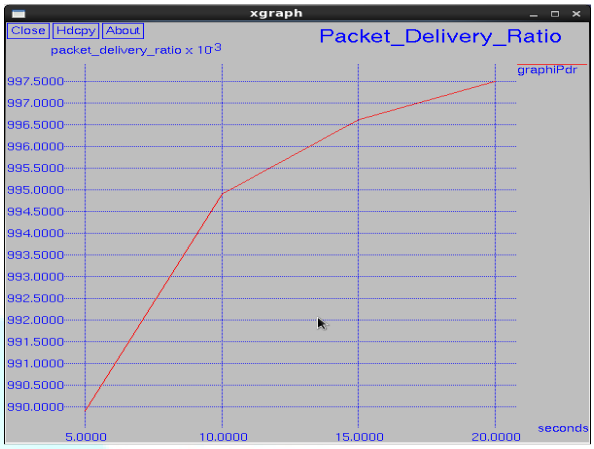

Fig. 2 Packet delivery ratio in attack detection

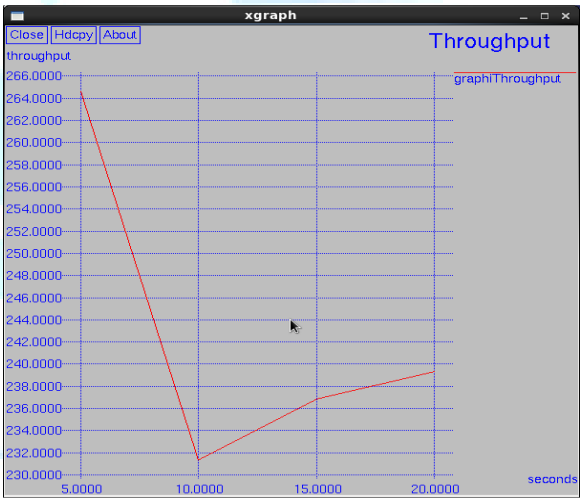

Fig. 3 Throughput in attack detection

Fig. 4 End to end delay in attack detection

The effectiveness of using cluster analysis for attack detection is presented in Fig.2 .It provides high packet delivery ratio . The end to end delay is also reduced drastically that is described in Fig 4. Thus RSS based attack detection provides efficient result

3. Determining the Number of Attackers

3.1 Problem Formulation

In accurate 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 multiclass detection problem and is similar to determining how many clusters exist in the RSS readings. If C is the set of all classes, all possible combination of number of attackers. For instance, $C = \{1 , 2 , 3 , 4\}$. For a class of specific number of attackers c_i, e.g., $c_i = 3$, we define P_i as the positive class of c_i and all other classes as negative class N_i

$$P_i = c_i$$

$$N_i = \bigcup_{j \neq i} C_j \in C$$

Further, we are interested in the statistical characterization of the percentage that the number of attackers can be accurately determined over all possible testing attempts with mixed number of attackers. Associated with a specific number of attackers, i, we define the Hit Rate HR_i as $HR_i = \frac{N_{true}}{P_i}$ where N_{true} is the true positive detection of class c_i. Let N_{false} be the false detection of the class c_i out of the negative class Ni that do not have i number of attackers. We then define the false positive rate FP_i for a specific number of attackers of class c_i as $FP_i = \frac{N_{false}}{N_i}$. then, the Precision is defined as

$$Percision_i = \frac{N_{true}}{N_{true} + N_{false}}$$

4. IDOL: Integrated Detection and Localization

In this section, an integrated system is presented that can both detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. This approach is effective especially when attackers using different transmission power levels.

4.1 Framework

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. The traditional method of averaging RSS readings cannot differentiate RSS readings from different locations and thus is not feasible for localizing adversaries.

Different from traditional localization approaches, this integrated detection and localization system utilizes the RSS as inputs to localization algorithms to estimate the positions of adversaries. The return positions from the system includes the location estimate of the original node and the attackers in the physical space.

Handling adversaries using different transmission power levels. An adversary may vary the transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately. We examine the pass loss equation that models the received power as a function of the distance to the landmark:

$$p(d)[dBm] = p(d_0)[dBm] - 10\gamma \log (\frac{d}{d0}) \quad (4)$$

where Pðd0Þ represents the transmitting power of a node at the reference distance d0, d is the distance between the transmitting node and the landmark, and is the path loss exponent. Further, we can express the difference of the received power between two landmarks, i and j, as

$$p(d_i) - p(d_j) = 10\,\gamma_i \log (\frac{d_i}{d_0}) - 10\,\gamma_i \log (\frac{d_j}{d_0}) \quad (5)$$

Based on Eq.(5), found that the difference of the corresponding received power between two different land-marks is independent of the transmission power levels. Thus, 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

5. Results and Discussion

In this work, a method for detecting spoofing attacks as well as localizing the adversaries in wireless and sensor networks is proposed. In contrast to traditional identity oriented authentication methods, this RSS based approach does not add additional overhead to the wireless devices

and sensor nodes and spoofing detection problem has been formulated as a classical statistical significance testing problem. Therefore, the results obtained in Fig.5 provide strong evidence of the effectiveness of this approach in detecting the spoofing attacks and localizing the positions of the adversaries.

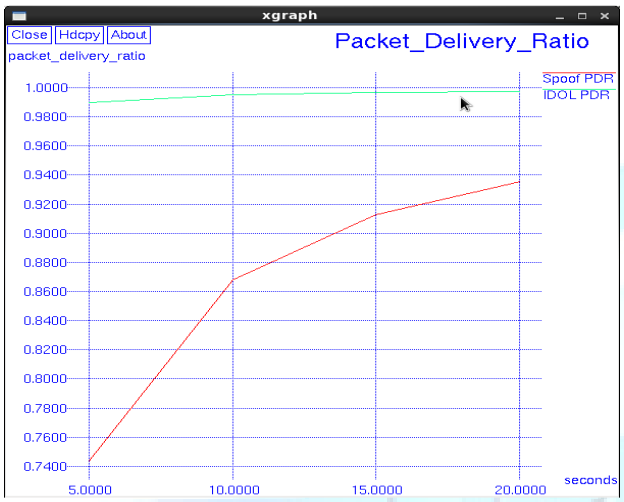

Fig. 5 Effectiveness of IDOL through packet delivery ratio

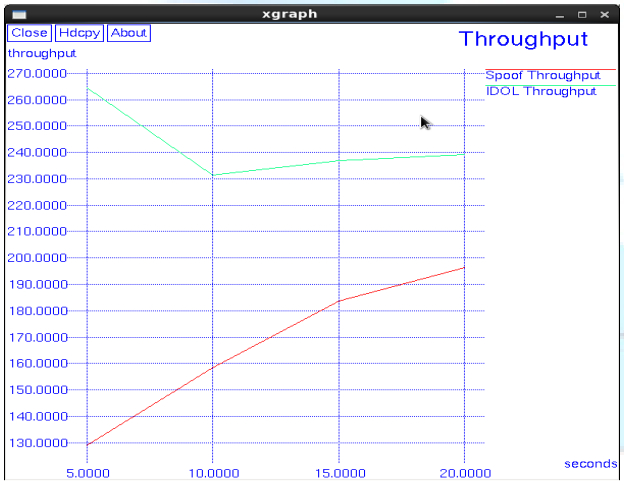

Fig. 6 Effectiveness of IDOL through throughput

The Throughput will be high for spoofing as the multiple adversaries also send information. Thus once detection and localization is done, the adversaries arre prevented from being communicating the base station, thereby reducing the throughput. Fig.6 describes the comparison graph of spoof and grapgh after detection and localization. To increase the throughput, time in seconds is reduced, as that would increase the more number of packet delivery. This finally gives increased throughput increasing the efficiency of the sytem.End to end delay is reduced whichis illustrated in Fig.7.

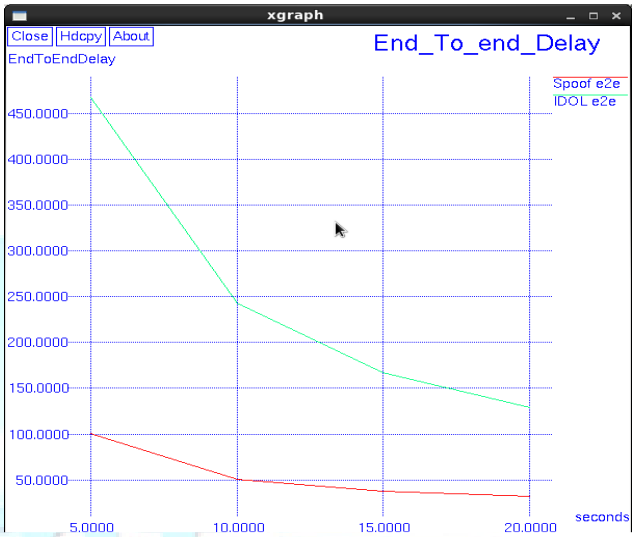

Fig. 7 Effectiveness of IDOL through end to end delay

6. Conclusions

In this work, received signal strength based spatial correlation is used, 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. Thus this theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection is used. This 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, thus cluster analysis is used 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. Further, based on the number of attackers determined this 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] J.Yang, Yingying (Jennifer) Chen, W. Trappe, J.Cheng "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" IEEE Transactions on parallel and distributed systems, Jan 2013

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

[3] T. He, C. Huang, B. Blum, J.A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Net- works," Proc. MobiCom '03, 2003..

[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 in 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] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001. [20] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007

[11] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.
Shih-Hau Fang,Chung-Chih Chuang, and Chiapin Wang "Attack-Resistant Wireless Localization Using an Inclusive Disjunction Model" IEEE transactions on communications, May 2012.