Detecting and localizing multiple spoofing attackers in wireless network

Deepa Hurali
III Semester, M-Tech, Dept of CSE
KLS Gogte Institute of Technology
Udhyambag, Belgaum, Karnataka, India

Prof. Vidya R. Kulkarni
HOD, Dept of MCA
KLS Gogte Institute of Technology
Udhyambag, Belgaum ,Karnataka ,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. 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 nodes is used to detect the spoofing attacks. Then the problem of determining the number of attackers as multi-class detection problem is formulated. Cluster-based mechanisms 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

I. INTRODUCTION

Due to the openness of wireless transmission medium, attackers can monitor any transmission. Further, these attackers 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. Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], 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 in [3], [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 to

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

Most existing approaches employ cryptographic schemes to address potential spoofing attacks [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. This paper proposes 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 the concern is on the 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 focus is on static nodes in this work, which are common for spoofing scenarios [7]. The works that are closely related are [3], [7], [9]. [3] Proposed the use of matching rules of signal prints for spoofing detection, [7] modeled the RSS readings using a Gaussian mixture model and [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 a same identity to launch attacks, which is the basis to further localize multiple adversaries after attack detection. Although [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 of the 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. The problem of determining the number of attackers as a multi-class detection problem is formulated. Then cluster based methods are applied to determine the number of attacker. Further a mechanism called SILENCE is used 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, Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers. Moreover, an integrated system, IDOL, is used which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries

II. RELATED WORK

The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication [5], [6], [10]. Wu et al. [5] have introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Wool [6] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys.

Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorelates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations, and thus to detect spoofing attacks in wireless networks [11].Brik et al. [12] focused on building fingerprints of 802.11bWLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. However, there is additional overhead associated with wireless channel response and radiometric signature extraction in wireless networks. Li 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 [13] 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 works [3], [7], [14] using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton [3] proposed the use of matching rules of signalprints for spoofing detection. 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. 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. Further, they do not have the ability to localize the positions of the adversaries after attack detection.

Turning to studying localization techniques, in spite of its several meter-level accuracy, using RSS [14], [15], is an attractive approach because it can reuse the existing wireless infrastructure and is highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties such as RSS [14], [15], Time Of Arrival (TOA) , Time Difference Of Arrival (TDOA), and direction of arrival (DoA). Whereas range-free algorithms use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Lateration approaches use distances to landmarks, while angulation uses the angles from landmarks. Scene

matching strategies [15] use a function that maps observed radio properties to locations on a pre constructed signal map or database. Further, Chen proposed to perform detection of attacks on wireless localization and Yang proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, we choose a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy.

This work differs from the previous study in that here the spatial information is used to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, this work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, this approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

III. OVERVIEW OF TECHNIQUES

(1)Generalized attack detection model

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

(2)Determining the number of attackers

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. Since it is not known that 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.

(3)IDOL: Integrated detection and localization framework

Integrated systems that can detect spoofing attacks, determine the number of attackers, and localize multiple adversaries.

(4)Data flow diagram

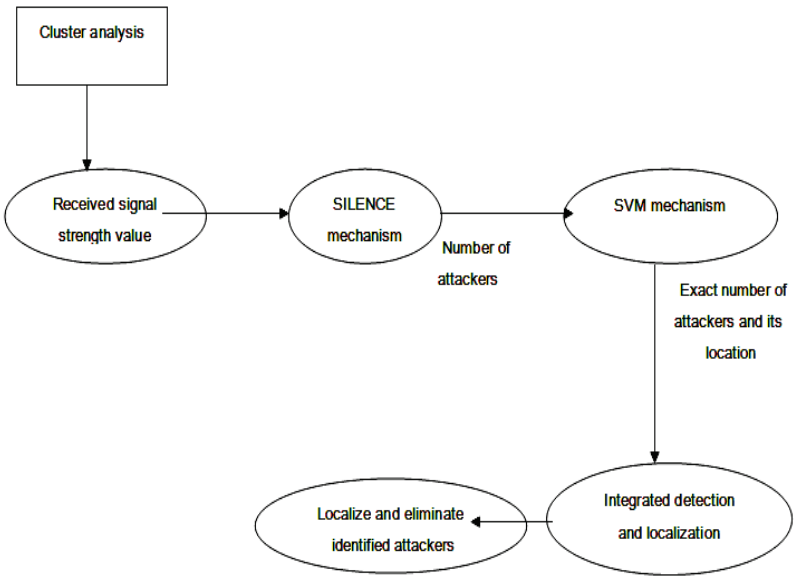

Figure 1 Data flow diagram

IV. 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. Since the concern is on the 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.

V. ALGORITHMS

In order to evaluate the generality of IDOL for localizing adversaries, a set of representative localization algorithms ranging from nearest neighbor matching in signal space (RADAR), to probability-based (Area-Based Probability), and to multilateration (Bayesian Networks) are chosen.

RADAR-Gridded:

The RADAR-Gridded algorithm is a scene-matching localization algorithm. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR 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.

Area Based Probability (ABP):

ABP also 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 vectors. ABP then computes the probability of the wireless device being at each tile Li, with i = 1...L, on the floor using

Bayes' rule:

$$P(L_i|s) = P(s|L_i) * p(L_i) / P(s)$$

Given that the wireless node must be at exactly one tile satisfying $\sum^{L}_{i=1} P(Li|s) = 1$, ABP normalizes the probability and returns the most likely tiles/grids up to its confidence α.

Bayesian Networks (BN):

BN localization is a multi lateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Figure 2 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.

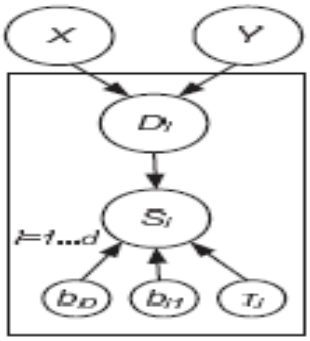

Figure 2 Bayesian graphical model in our study

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: $si \sim N(b_{0i} + b_{1i} \log Di, \tau_i)$. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

VI. CONCLUSION

This work, 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. This approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that any number of attackers can be localized and can eliminate them. Determining the number of adversaries is a particularly challenging problem. This paper uses 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, Support Vector Machines (SVM) based mechanism is used to further improve the accuracy of determining the number of attackers present in the system.

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.

[11] M. bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2003, pp. 79–87.

[12] V.Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures".

[13] P.Bahl and V.N.Padmanabhan, "RADAr: An in-Building RF-Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[14] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc.IEEE INFOCOM, Apr.2007

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