RESEARCH ARTICLE OPEN ACCESS

Spoofing Detection in Wireless Networks

S.Manikandan[1],C.Murugesh[2]
[1]PG Scholar, Department of CSE, National College of Engineering, India.mkmanikndn86@gmail.com
[2]Associate professor, Department of CSE, National College of Engineering, India.cmurugesh07@gmail.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. Using spatial information the following are performed 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. Spatial information is a physical property associated with each node which is hard to falsify, and not reliant on cryptography. Spatial correlation of received signal strength (RSS) inherited from wireless nodes are used to detect the spoofing attacks. Cluster-based mechanisms are developed to determine the number of attackers. An integrated detection and localization system is proposed to localize the positions of multiple attackers. This integrated detection and localization system provides high accuracy of localizing multiple adversaries.
Keywords: Wireless network security, spoofing attack, attack detection, localization

I INTRODUCTION

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 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, 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 proposed system is 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.

When focus on static nodes in this work, which are common for spoofing scenarios [7]. Spoofing detection in mobile environments is addressed in [8]. The works that are closely related to this are [3], [7], [9]. [3] proposed the use of matching rules of signal prints for spoofing detection, [7] modelled 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.

II METHODS

2.1 Attack Detection Using Cluster

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, which presents RSS reading vectors of three landmarks (i.e., n = 3) 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 (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that the user 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.

In this work, Partitioning Around Medoids Method is used to perform clustering analysis in RSS. The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method, the PAM method is more robust in the presence of noise and outliers. Thus, 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.

In particular, in attack detection phase, partition the RSS vectors from the same node identity into two clusters (i.e., K = 2) no matter how many attackers are using this identity, since the objective in this phase is to detect the presence of attacks. Then choose the distance between two medoidsDm as the test statistic T in significance testing for spoofing detection, Dm = (Mi ,Mj), where Mi and Mj are the medoids of two clusters. Under normal conditions, the test statistic Dm should be small since there is basically only one cluster from a single physical location. However, under a spoofing attack, there is more than one node at different physical locations claiming the same node identity. As a result, more than one clusters will be formed in the signal space and Dm will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space.

2.2 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, 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 and fake RSS clusters caused by outliers and variations of the signal strength. such a situation where there are three attackers masquerading the same identity.

Based on this observation, SILENCE mechanism is developed, testing SILhouette Plot and System EvolutioN with minimum distanCE of cluster, which evaluates the minimum distance between clusters on top of the pure cluster analysis to improve the accuracy of determining the number ofattackers. The number of attackers K in SILENCE is thus determined by

$$K = \begin{cases} K_{sp} \;\; if \;\; K_{sp} = K_{se}; \\ K_{sp} \;\; if \;\; \min(D_m^{obs})_{K_{sp}} > \min(D_m^{obs})_{K_{se}}; \\ K_{se} \;\; \text{if} \;\; \min(D_m^{obs})_{K_{sp}} < \min(D_m^{obs})_{K_{se}}; \end{cases}$$

Where Dobs m is the observed value of Dm between two clusters. SILENCE takes the advantage of both Silhouette Plot and System Evolution and further makes the judgment by checking the minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers. Hence, when applying SILENCE to the case, SILENCE returns K = 3 as the number of attackers, which is the true positive in this example.

2.3 GADE

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.

2.4 Integrated Detection and Localization Framework (IDOL)

In this section integrated system is described. Integrated systems that can detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of the proposed approach, especially when attackers using different transmission power levels.

2.5 Algorithms

In order to evaluate the generality of IDOL for localizing adversaries, have to chosen 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) .

RADAR-Gridded: The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from . 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 vector **s**. ABP then computes the probability of the wireless device being at each tile Li, with i = 1...L, on the floor using Bayes' rule:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})}$$

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

Bayesian Networks (BN): BN localization is a 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 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.

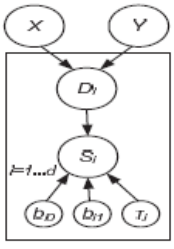
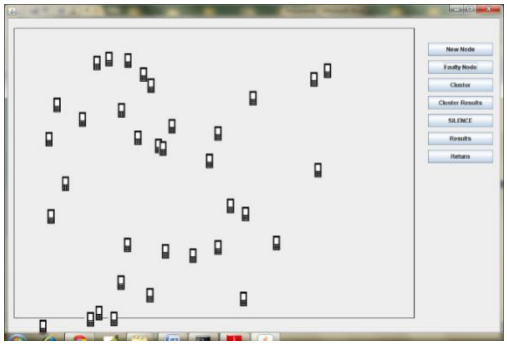


Fig 1: Bayasian graphical model

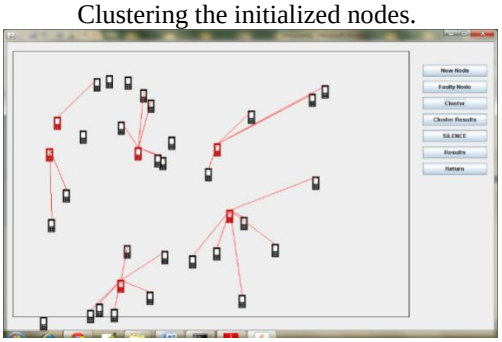
The distance Di =$\sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance 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.

III EXPERIMENTAL RESULT

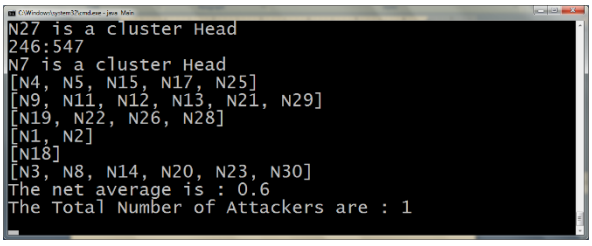
Initialize the correct and fault nodes using the control buttons.



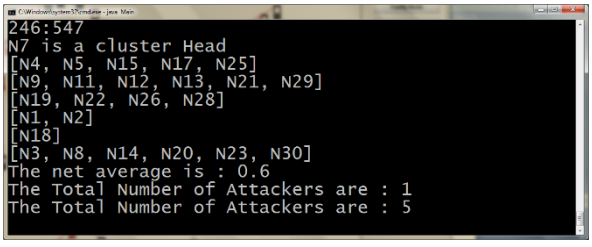
Clustering the initialized nodes.



The average RSS between clusters are calculated and the number of attacker detected as 1.



Applying the silence mechanism the number of attackers increased as 5.

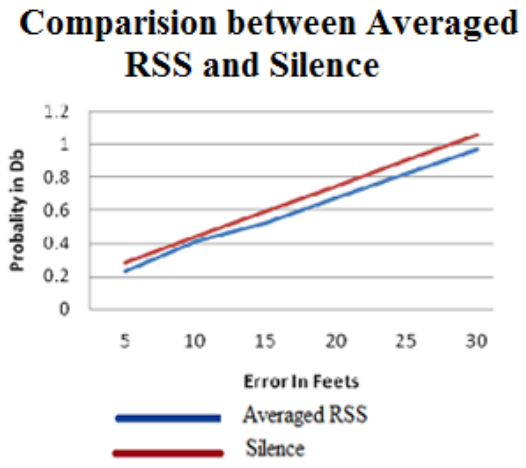


IV PERFORMANCE EVALUATION

The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of proposed approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

Feet (db)	Averaged RSS	SILENCE
5	0.23	0.28
10	0.41	0.44
15	0.52	0.59
20	0.676666667	0.746667
25	0.821666667	0.901667
30	0.966666667	1.056667

Proposed 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 based mechanism. Further, based on the number of attackers determined by proposed mechanisms, integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels.



The above table and the figure presents the localization error CDF when using the returned RSS medoids from SILENCE and the averaged RSS, respectively, similar localization performance is observed when using the returned RSS medoids to the traditional approaches using averaged RSS.

VI CONCLUSION AND FUTUREWORK

In this work, 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 is used as the basis for detecting spoofing attacks in wireless networks. Theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes is provided for attack detection. Based on the cluster analysis of RSS readings test statistic is derived. Proposed approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that anyone can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers and localizing adversaries is developed.

In future FUZZY mechanism is developed that employs the maximum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers.

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.