IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com
ISSN 2348 – 7968

Detection and Localization of Multiple Spoofing Attackers in Wireless Networks Using Data Mining Techniques

Nandini P[1] Nagaraj M.Lutimath[2]
[1]PG Scholar, Dept. of CSE Sri Venkateshwara College, VTU, Belgaum, Karnataka, India
[2]Asst.Prof, Dept. of CSE Sri Venkateshwara College of Engineering, VTU, 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. Here we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for detecting the spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. We first propose a generalized attack-detection model that utilizes the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks and cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, we explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers.

***Index Terms*—** Localization, Spoofing attack, Attack detection and Wireless network.

1. INTRODUCTION

The flexibility and openness of wireless networks enables an adversary to masquerade as other devices easily. Among various types of attacks, identity-based spoofing attacks are serious network threats as they can facilitate a variety of advanced attacks to undermine the normal operation of networks.

Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], 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 [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.

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 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 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 [7]. We addressed spoofing detection in mobile environments in our other work [8]. The works that are closely related to us are [3], [7], [9]. Faria and Cheriton [3] proposed the use of matching rules of signal prints for spoofing detection, Sheng et al. [7] modeled the RSS readings using a Gaussian mixture model and 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 of our work are:

GADE: a generalized attack detection model (GADE) that can both detect spoofing attacks as well

ISSN 2348 – 7968

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.

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 multiclass detection problem. We then applied cluster-based methods to determine the number of attacker. Additionally, when the training data are available, we propose to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

Finally, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. 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.

The scope of this paper is to detecting 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.

2. EXISTING SYSTEM

. The existing system uses the cryptographic-based authentication, for example 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 which uses periodic key refresh and host revocation to prevent the compromise of authentication keys. 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. 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.

3. PROPOSED SYSTEM

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. An integrated detection and localization system that can detect both attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. Fig.1 considers a wireless network with N nodes.

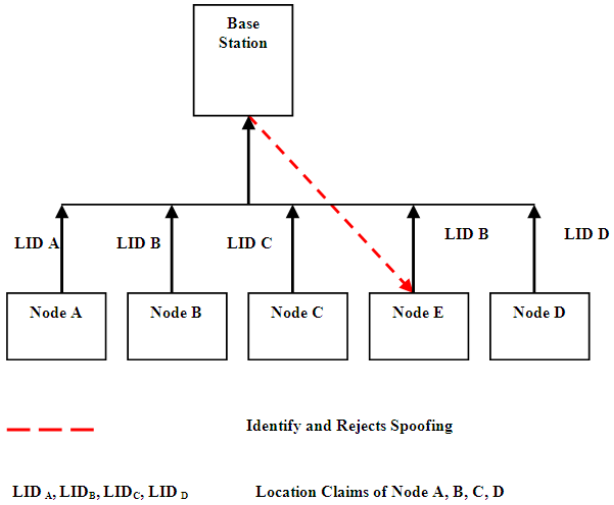

Fig.1 Architecture of Proposed System

Let N denote the set of all nodes in the network. Nodes are deployed in 2D platform. Each node is associated with unique location identifier. If any one of the node needs to communicate with the base station, it will check the location ID of respective node. If the base station finds that any two nodes has the same location ID (i.e. Node B), then it meant that spoofing has taken place. A base station is a radio receiver or transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. It typically consists of a low-power transmitter and wireless router.

3.1 System Module

Detection and Localization of Spoofing attackers are identified from the following modules:

- Detection of Spoofing Attack
- Determine the Number of Attackers
- Localization of Attackers

3.1.1 Detection of Spoofing Attack

Spoofing attack detection is performed using Cluster Analysis. As the wireless network is

ISSN 2348 – 7968

deployed as clusters, the attackers are identified in each and every cluster separately. Fig.2 under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets (i.e., spoofing node or victim node). Since under a spoofing attack, the data packets from the victim node and the spoofing attackers are mixed together, this observation suggests conducting cluster analysis on location id in order to detect the presence of spoofing attackers in wireless network.

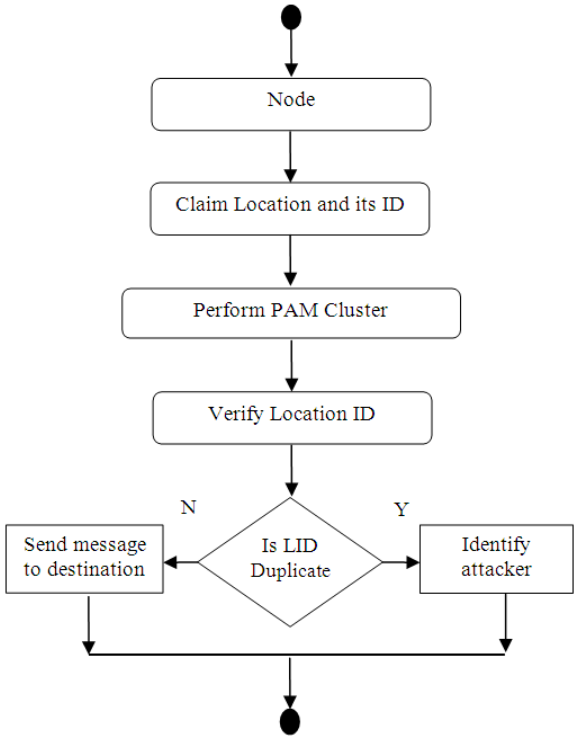

Fig.2 Activity diagram of proposed system

Generalized Attack Detection Model (GADE): It can both detect spoofing attacks as well as determine the number of adversaries using Cluster analysis. In GADE, the Partitioning Around Medoids (PAM) cluster analysis method is used to perform attack detection and then applied cluster-based methods to determine the number of attacker.

PAM: This 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. Spoofing attack detection is performed using Cluster Analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Consider the wireless nodes are composed of several clusters of ordinary Nodes.

The PAM algorithm partitioned a dataset of 'n' objects into a number of clusters ('k'), where both the dataset and the number k is an input of the algorithm. This algorithm works with a matrix of dissimilarity, where its goal is to minimize the overall dissimilarity between the represents of each cluster and its members.

Fig.3 shows, how Spoofing attacks are detected by same location id. Attacker gets the ID of normal node and makes use of the same to send packets to Destination node.

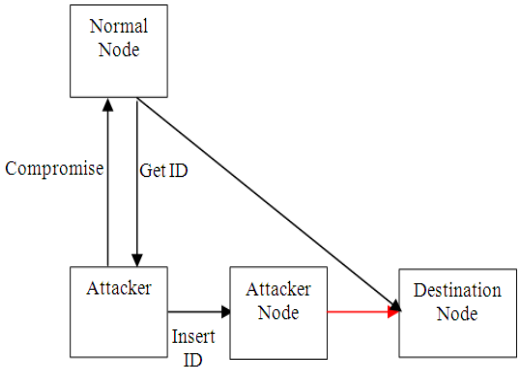

Fig.3 Spoofing Attack Detection

3.1.2 Determine the Number of Attackers

Here we explore using Support Vector Machines to classify the number of spoofing attackers in the network. The advantage of using SVM is that it can combine the intermediate results (i.e., features) from different statistic methods to build a model based on training data to accurately predict the number of attackers. On detecting an attacker in the wireless network, SVM increment the target Value by '1', else '0'. SVM can be applied to solve classification and regression problems.

Particularly, SVM is a set of kernel-based learning methods for data classification, which involves a training phase and a testing phase. Each data instance in the training set consists of a target value (i.e., class label) and several attributes (i.e., features). The goal of SVM is to produce a model from the training set to predict the target value of data instances (i.e., the testing data).

Fig.4 shows on detecting multiple adversaries present in a Wireless network. In Multi Spoofing attack, ID of a compromised Node is used by multiple adversaries present in the network, to send packet to Destination Node.

ISSN 2348 – 7968

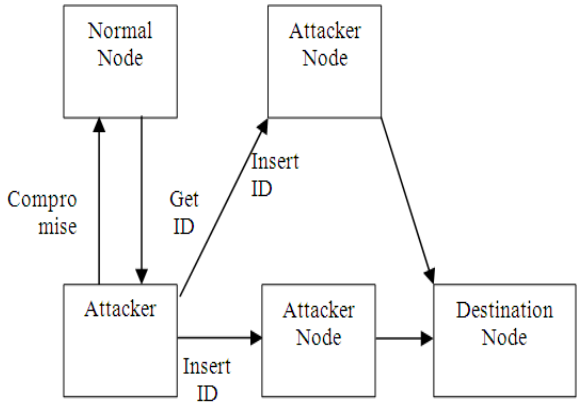

Fig.4 Detection of Multi Spoofing Attack

3.1.3. Localization of Attackers

We developed an integrated detection and localization (IDOL) 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 utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries.

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.

1. 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.

2. 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:

$$P(Li|s) = P(s|Li) * P(Li) / P(s)$$

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

3. Bayesian networks:

BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Fig.5 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex s_i is the RSS reading from the ith landmark; and the vertex D_i 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 = $b_{0i}+b_{1i}$ logD_i, where b_{0i}, b_{1i} are the parameters specific to the ith landmark.

The distance $D_i=\sqrt{(X-x_i)^2 + (Y-y_i)^2}$ 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. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

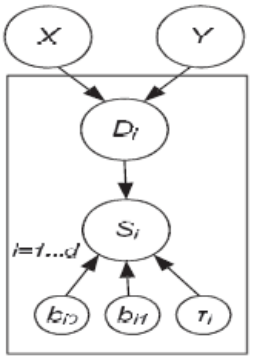

Fig.5 Bayesian graphical model in our study

4. CONCLUSION

This work, proposed to use received signal strength (RSS) based spatial correlation for detecting spoofing attacks as well as determine the number of adversaries. When the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers. Further, based on the number of attackers determined by the mechanisms, an integrated detection and localization system can localize any number of attackers.

In future, based on the outcome of this model, explore further to find ways to eliminate those identified multiple adversaries, from the wireless

network. Thus way, wireless networks will be more robust and less prone to attack.

REFRENCES

[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 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.
[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.

First Author

Nandini P is a Post Graduate student Department of CSE, Sri Venkateshwara college of Engineering, Karnataka, India. Received Bachelor of Engineering (CSE) from PES College of Engineering, Mandya in 2011. Her areas of interest include Wireless Sensor Network, Data Mining and Network Security.

Second Author

Mr.Nagaraj M.Lutimath is Assistant Professor, Department of CSE, Sri Venkateshwara college of Engineering, Karnataka, India. He is undergoing research under VTU. His areas of interest include Data Mining, Wireless Ad-Hoc Networks and Network Security.