DETECTION OF IP SPOOFING ATTACK BASED ON RSS SPATIAL CORRELATION IN WIRELESS NETWORK

Visalakshmi[1], Vasugi[2]

[1]*Vasugi, M.TECH CSE Student, Department of Computer Science and Engineering, SRM University, Kattankulathur campus, Kancheepuram District- 603 203, Tamilnadu, India*

[2]*P.Visalakshi, Asst.Professor(S.G)., Department of Computer Science and Engineering, SRM University, Kattankulathur campus, Kancheepuram District- 603 203, Tamilnadu, India*

Abstract

IP spoofing-based flooding attacks are a open and serious security problem on the current Internet. The best current anti-spoofing practices have been implemented long in modern routers. The proposed system detect the spoofing attacks using the spatial correlation of Received Signal Strength (RSS) inherited from wireless nodes. Then it determines the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers to achieve monotonically increasing deployment incentives for all types of spoofing attacks, and the system design is lightweight and practical. GADE: A Generalized Attack Detection Model (GADE) that can both determine the number of adversaries using cluster analysis methods and detect spoofing attacks grounded on RSS among normal devices and adversaries IDOL: An Integrated Detection and Localization (IDOL) system that can detect both attacks and find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

Keywords: *Generalized Attack Detection Model, Integrated Detection and Localization, correlation of RSS*

INTRODUCTION

The spoofing attacks are influenced with many traffic attacks [1] [2] such as attacks on rogue access point (AP) attacks, access control lists 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. 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 which have the unique power not only to identify the presence of these attacks but also localize adversaries.

The main contributions of the work are: **GADE:** a **G**eneralized **A**ttack **De**tection model (GADE) that can detect both 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.

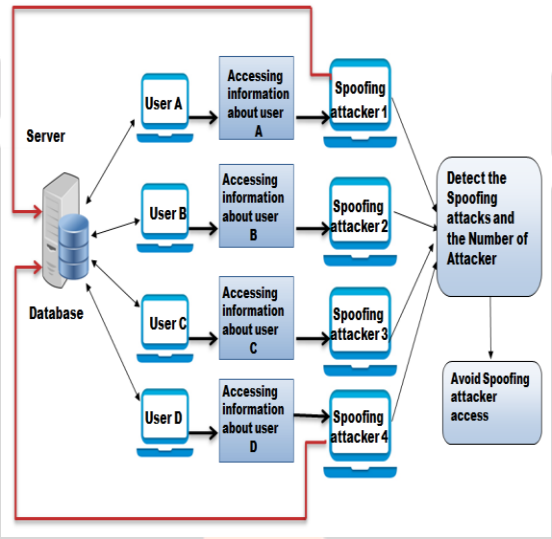
IDOL: an Integrated Detection And localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. In GADE, the Partitioning Around Medoids (PAM)cluster analysis method is used to perform attack detection.

GENERALIZEDATTACK DETECTION MODEL

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

RELATED WORK

The traditional approach to preventing spoofing attacks is to use cryptographic-based authentication..we 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 implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. An authentication framework for hierarchical, ad hoc sensor networks is proposed.



Generalized Attack Detection Model

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.

Determining the number of attackers

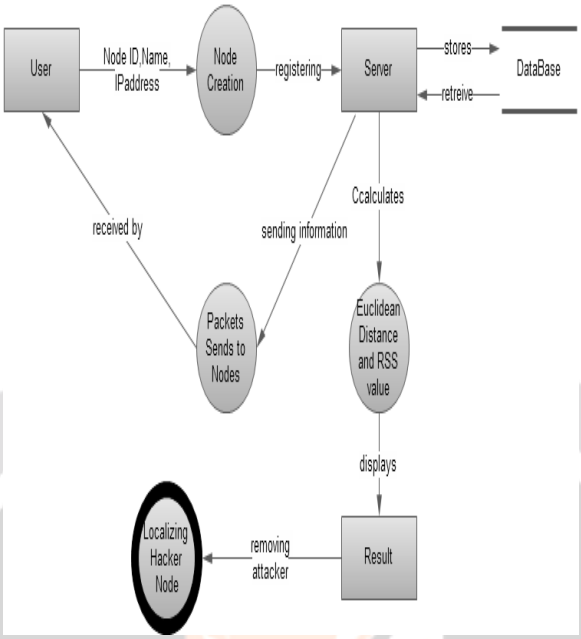
Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node identity to launch attacks, we determine the number of attackers using different transmission power levels. An Integrated Detection And Localization (IDOL) system that can both detect attacks as adversaries even when the adversaries vary their transmission power levels. The proposed system is used to detect the spoofing attacks, determine the number of attackers in the network and avoid the spoofing attacker access by eliminating them.

PROPOSED FRAMEWORK

The proposed system use received signal strength RSS-based spatial correlation, which is 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. We are concerned with attackers who have different locations than legitimate wireless nodes, utilizing the spatial information to address spoofing attacks has the unique power do not only identify the presence these attacks but also localize adversaries an added advantage of spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

In localization results provide strong evidence of high accuracy of localizing multiple adversaries. The cluster-based wireless sensor network data received signal network strategy. 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 network.



Attack detection model

This model consists of two phases: Attack detection determination which determines the no of adversaries in the network the in spoofing detection is to devise strategies that use the uniqueness of spatial information but not using the location directly as the attacker's position on unknown. The RSS property closely correlated with location in physical space and is readily available in the existing wireless networks although affected by random noise, multipath effects, environmental bias and the RSS measured at set of landmark is closely related to the transmitter's physical location and is governed by the distance of landmarks. The RSS reading at the same physical area are comparable those RSS readings at diverse areas in physical space are particular. Hence the RSS readings present solid spatial connection qualities. RSS value vector as {s1,s2,..sn} where n is the no of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations.

Given two remote nodes in the physical space, the RSS distance between two nodes in signal space at the ith point of interest is given by

$$s_i(d_j)[dBm] = P(d_0)[dBm] - 10\gamma \log\left(\frac{d_j}{d_0}\right) + X_i,$$

Where

$p(d_0)$ represents the transmitting power of the node at the reference distance d0,dj is the distance between the wireless node j and the ith landmark is given by

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

Where

d1,d2 are the Euclidean distance between two wireless nodes in the networks Δx follows zero mean Gaussian distribution with √2δ_ standard deviation.

$$D_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$$

The distance in turn depends on the location (x,y) of the measured signal and the coordinates (xi,yi) of the landmarks.

Integrated detection and localization

Integrated system that can both detect the spoofing attacks and number of attackers and localize multiple adversaries. The implementations results are presented to evaluate the effectiveness of our approach, when the attackers using different transmission power levels.

The localization approaches based on averaged RSS from each node identity inputs to estimate the position of a node in wireless spoofing attacks the RSS stream of a nodes identity may blend with RSS reading of both the original node and additional spoofing nodes from different physical areas. RSS reading cannot differentiate RSS reading from different location and thus is not feasible for localizing adversaries. an adversaries may vary in their transmission power levels when performing spoofing attacks .so that the localization system cannot estimate its location accurately.

We examine the path loss exponent equation that models the received power as a function of the distance to the landmark.

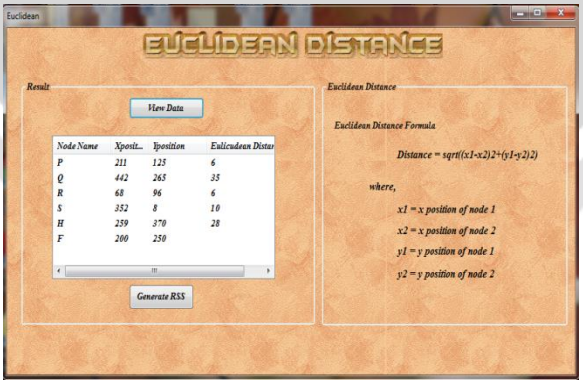
$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right)$$

Where P(d0) represents the transmitting power of a node at the reference distance d0, d is the distance between the transmitting node and the landmark and gamma is the path loss exponent , the difference of the received power between the two landmarks I and j as

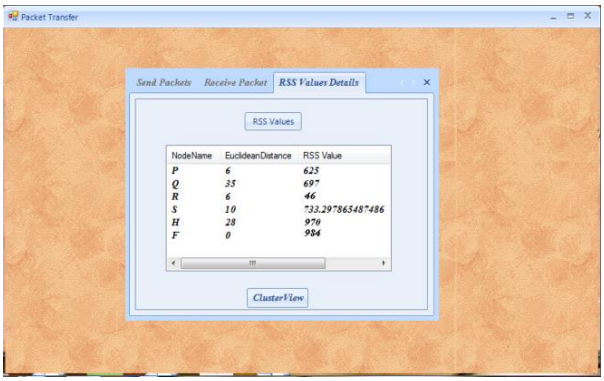
$$P(d_i) - P(d_j) = 10\gamma_i \log_{10}\left(\frac{d_i}{d_0}\right) - 10\gamma_j \log_{10}\left(\frac{d_j}{d_0}\right).$$

This formula, we found that the difference of the corresponding received power between two different landmarks is independent of transmission power levels. When an adversaries dwelling at a physical area shifts its transmission power to perform a spoofing attack, the distinction of RSS reading between two separate landmarks from the adversaries is consistent since the RSS reading are acquired from a solitary physical area. IDOL is highly effective in localizing multiple adversaries with or without changing their transmission power levels.

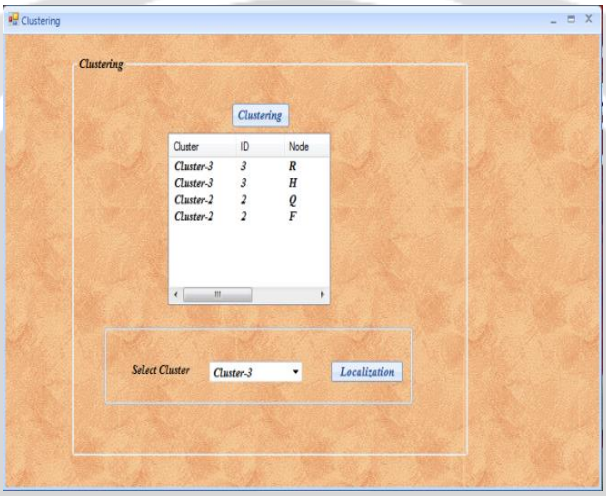
RESULTS AND DISCUSSION



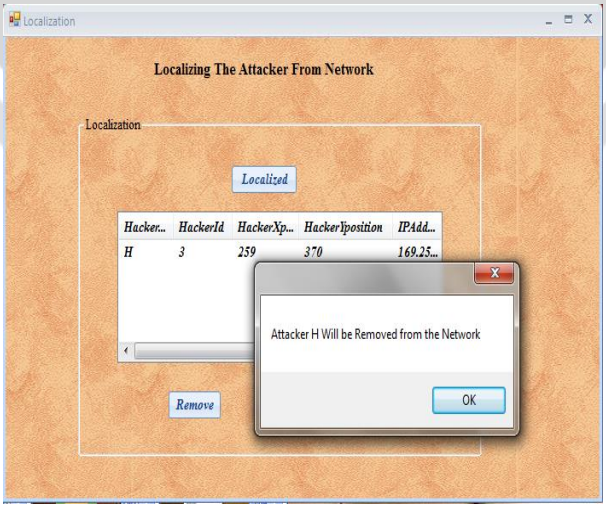
Calculating Euclidean Distance



Calculating RSS Values



Detecting and Selecting Cluster for Localization



Removing Attacker from Network

CONCLUSION

We use received signal strength RSS based spatial correlation, which is physical property associated with each wireless device that is hard to falsify and reliant on cryptography as basis for detecting spoofing attack in wireless network. Theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. We determined the test measurement taking into account the poncho examination of RSS reading. We can both identify the number of adversaries, which spoofing the same node identity, we confine any number of attacker and remove them from the network.

REFERENCES

[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] 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.

[6] 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.

[7] 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.

[8] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

[9] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

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

[11] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R.P. Martin, "The Robustness of Localization Algorithms to Signal Strength Attacks: A Comparative Study, Proc. Int'l Conf. Distributed Computing in Sensor Systems (DCOSS), pp. 546-563, June 2006.