ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Secure Localization with Attack Detection in WSN

Pradnya Boga[1], Bhavana Ghodke[2], Vaishnavi Kadam[3], Prof. Aher S. M. [4]

B. E Student, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India

Asst. Professor, Dept. of Computer Engineering, SCSMCOE, Nepti, Ahmednagar, Maharashtra, India

ABSTRACT:Wireless 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. In this paper, 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 1) detecting attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multiclass detection problem.

KEYWORDS:Wireless network security, Spoofing attack, Attack detection, Localization.

I. 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 tolaunch 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 802.11

security techniques including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames—an attacker can still spoof management or control frames to causesignificant impact on networks.

Spoofing attacks can further facilitate a variety of traffic injection attacks 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. 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 1) 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. 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. We addressed spoofing detection in mobile environments in our other work . The works that are closely related to us are .Faria and Cheriton proposed the use of matching rules of signal prints for spoofing detection, Sheng et al. modeled the RSS readings using a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Gaussian mixture model and Chen et al. 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. 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: 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.

II. LITERATURE SURVEY

.

Paper Name	Author Name	Year Of Paper	Description
Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE	JieYang,StudentMember,IEEE,Yingying(Jennifer)	2013	1.Detect presence of the attacks.
Detecting spoofing attacks in mobile wireless environments,"	J. Yang, Y. Chen, and W. Trappe,	2009	Detecting attacks in the mobile wireless environment that is when wireless devices, such as the victim node and/or the spoofing node are moving.
Detecting Identity-Based Attacks in Wireless Networks Using Signal prints	Faria D. and Cheriton D	2006	We show that, deferent from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce.
802.11 Denial-of-Service Attacks: Real," Proc. USENIX Security Symp.,	J. Bellardo and S. Savage	2003	This use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated.

III. PROPOSED SYSTEM

The proposed system I proposed to use 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 an integrated detection and localization system (IDOL) that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels

.

A. ALGORITHM

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

3.1.1 RADAR-Gridded:

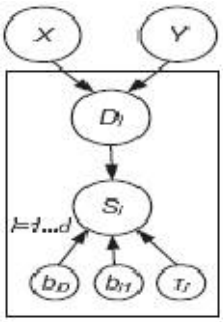
The RADAR-Gridded algorithm is a scene-matching localization algorithm. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR returns the x, y of the nearest neighbor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

3.1.2Area 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
Given that the wireless node must be at exactly one tile satisfying
) / P(s)
L
i=1

3.1.3 Bayesian Networks (BN):

P(Li|s) = 1, ABP normalizes the
!"#$%$&'&()*%+,*"-(."+/*(0-*1#/(*'&2-')*(&'-/34"&,/*.!*(#*&(/*5#+6&,-+5-*78*
BN localization is a multi lateration algorithm that encodes the signal-to-distance propagation model intothe 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 DiRepresents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of siFollows a signal propagation model si = b0i+b1i logDi, where b0i, b1i are the parameters specific to the ith landmark.



The distance Di =9:;* < xi)2 + (Y <yi)2 in turn depends on the location (X, Y) of the measured signal and the coordinates (xi, yi) of the ith landmark. The network models noise and outliers by modeling the si as a Gaussian ,&/("&$.(&#+*%"#.+,*(0-*%$#=-*!"#!%4%(&#+*1#,-'>*?&(0*=%"&%+5-*@&A*/&~N(b0i + b1i '#4B&>*@. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

IV. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

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. 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 802.11Networks,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. M. Bohge and W. Trappe, An Authentication Framework forHierarchical Ad Hoc Sensor Networks, Proc. ACMWorkshop Wireless Security (WiSe), pp. 79-87, 2003.
5. Y. Chen, W. Trappe, and R.P. Martin, Detecting and LocalizingWireless Spoofing Attacks, Proc. Ann. IEEEComm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.
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. A. Wool, Lightweight Key Management for IEEE 802.11 WirelessLans with Key Refresh and HostRevocation,ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005..