International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2320-7248

PREVENTION OF MULTIPLE WIRELESS SPOOFING ATTACK PROTOCOLS

B.VIDHYA M.E (CSE)

ARASU ENGINEERING COLLEGE,
KUMBAKONAM
bvidhyakrishna@gmail.com

***ABSTRACT*—** *Wireless networks are vulnerable to spoofing attacks which allows for many other forms of attacks on the networks. The identity of node can be verified through cryptography authentication scheme, this authentication scheme is not always desirable because it requires key management and additional infrastructure overhead. In this paper, I proposed to use spatial information, physical property associated with each wireless node that is hard to falsify not based on cryptography authentication scheme, as basis for detecting spoofing attacks, determining the number of spoofing attackers when multiple attackers use same node identity and localizing multiple attackers. I proposed to use spatial correlation received signal strength (RSS), inherited from multiple wireless node to detect the spoofing attack. Then I proposed to use generalized attack detection model (GADE) to detect and determine the number of attackers. In addition, I developed integrated detection and localization system that can localize the multiple spoofing attackers.*

Keywords—Wireless network security, spoofing attack, attack detection, localization

1, 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 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]. [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 level The main contributions of our 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. We formulate the problem of determining the number of attackers as a multi-class detection problem. We then applied cluster based methods to determine the number of attacker. We further developed a mechanism called SILENCE 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, we propose to use Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. As we demonstrated through our experiments using both an 802.11 network as well as an 802.15.4 network in two real office building environments, GADE is highly effective in spoofing detection with over 90% hit rate and precision. 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.

2, RELATED WORKS:

The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication. Wu et al. 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. However, the crypto-graphic authenticationmay not be always applicable because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network 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 decorrelates 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. Brik et al. focused on building fingerprints of 802.11b WLAN 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 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 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 using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton proposed the use of matching rules of signal prints for spoofing detection. Sheng et al. modeled the RSS readings using a Gaussian mixture model. Sang and Arora 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 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 land-marks using the measurement of various physical properties such as RSS, 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 use a function that maps observed radio properties to locations on a preconstructed signal map or database. Further, Chen et al. proposed to perform detection of attacks on wireless localization and Yang et al. proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, I choose a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy.Our work differs from the previous study in that I use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, our 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, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations

3, PROBLEM STATEMENT

Detecting multiple spoofing attackers using wireless network.Determine the number of attackers, and localize multiple adversaries and eliminate them.

4, OVERVIEW OF TECHNIQUES

4.1 Generalized attack detection model

In this section, we describe our 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.

4.2 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, determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS readings.

4.3 IDOL: Integrated detection and localization framework

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

4.4, Data flow diagram

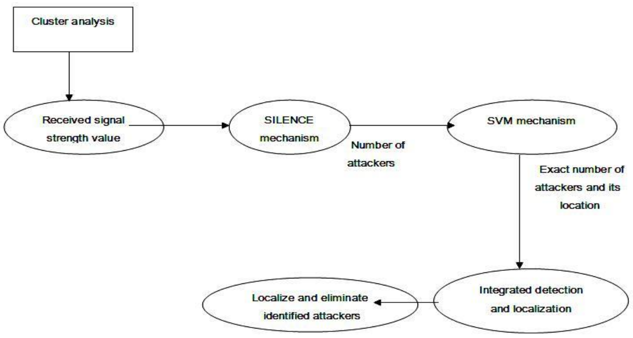

Cluster analysis
Received signal strength value
SILENCE mechanism
Number of attackers
SVM mechanism
Exact number of attackers and its location
Integrated detection and localization
Localize and eliminate identified attackers

Fig1.1 Data flow diagram

5, PROPOSED SYSTEM

- Use spatial information to identify the attackers it not only identify the attackers but also localize adversaries.

- It also detects attackers when multiple users use the same node identity.
- It does not require additional cost.

- The training data is available, we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

- In localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

- The Cluster Based wireless Sensor Network data received signal strength (RSS) based spatial correlation of 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 networks.

6, ALGORITHMS

In order to evaluate the generality of IDOL for localizing adversaries, we have 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

.

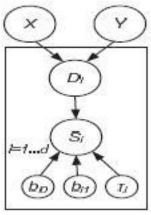
6.1, Area Based Probability (ABP): ABP also utilizes an interpolated signal map [16]. Further, the experimental area is divided into a regular grid of equal sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading 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:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})} \qquad (30)$$

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.

6.2, 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 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.



Bayasian graphical model in our study

The distance Di =$\surd(X - x_i)^2 + (Y - y_i)^2$ 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.

7. CONCLUSION

In this work, we 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 fordetecting spoofing attacks in wireless networks. We provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. We derived the test statistic based on the cluster analysis of RSS readings. Our approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. We developed 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, we explored using Support Vector Machines (SVM) based mechanism to further improve the accuracy of determining the number of attackers present in the system.To validate our approach, we conducted experiments on two test-beds through both an 802.11network (Wi-Fi) and an 802.15.4 (Zig-Bee) network in two real office building environments. We found that our 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 and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

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] 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 LocalizingWireless Spoofing Attacks,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[10] M. Bohge and W. Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[11] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” Proc. IEEE Int’l Conf. Comm. (ICC), pp. 4646-4651, June 2007.

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

Signatures,” Proc. 14th ACM Int’l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

[13] F. Guo and T. Chiueh, “Sequence Number-Based MAC Address Spoof Detection,” Proc. Eighth Int’l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

[14] L. Sang and A. Arora, “Spatial Signatures for Lightweight Security in Wireless Sensor Networks,” Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

[15] P. Bahl and V.N. Padmanabhan, “RADAR: An in-Building RFBased User Location and Tracking System,” Proc. IEEE INFOCOM, 2000.

[16] E. Elnahrawy, X. Li, and R.P. Martin, “The Limits of Localization Using Signal Strength: A Comparative Study,” Proc. IEEE Int’l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[17] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, “A Practical Approach to Landmark Deployment for Indoor Localization,” Proc. IEEE Int’l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.

[18] 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.

[19] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.

[20] Z .Yang, E. Ekici, and D. Xuan, “A Localization-Based Anti-Sensor Network System,” Proc. IEEE

INFOCOM, pp. 2396-2400, 2007.

[21] T. He, C. Huang, B. Blum, J.A. Stankovic, and T. Abdelzaher, “Range-Free Localization Schemes in Large Scale Sensor Networks,” Proc. MobiCom ’03, 2003.

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

[23] A. Goldsmith, Wireless Communications: Principles and Practice. Cambridge Univ. Press, 2005.

[24] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, “A Survey of Various Propagation Models for Mobile Communication,”IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 51-82, June 2003.

[25] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Courier Dover, 1965

BIOGRAPHY

Vidhyam.B, M E (Cse) from Arasu Engineering College, Kumbakonam