Volume : 5 | Issue : 1 | JANUARY 2016 • ISSN No 2277 - 8179

Research Paper

Detection of Multiple Spoofing Attackers in Wireless Networks

Engineering

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

Santosh Dange

ME Student, Department of Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule, Pune University, India

ABSTRACT

Wireless spoofing attacks are easy to launch and significantly impact on the performance of networks. Although the identity of a node can be verified through cryptographic authentication and conventional security approaches. 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 of detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity, 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. 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. We evaluated our techniques through two frameworks using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90 percent Hit Rate and Precision when determining the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple attacks.

Introduction

Wireless sensor networks represent an emerging technology that has become very appealing to researchers.The attacks can monitor any transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch 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. 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. 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 to the wireless devices.

Therefore , it is important to the following steps

- Detect the presence of spoofing attacks
- Determine the number of the attackers
- Localize multiple adversaries and eliminate them

OVERVIEW OF THE TECHNIQUES

Generalized attack detection model

In this section, we describe our Generalized Attack Detection Model (GADE), which consists of two phases attack detection , which detects presence of attacks and to determine the number of attackers.

Determining the number of attackers

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple attacks. As we will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node identity to lunch attacks and to determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS.

Integrated detection and localization framework (IDOL)

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.

PROPOSED SYSTEM

The proposed approach to prevent spoofing attacks is to use cryptographic-based authentication [5], [6], [7]. We have introduced a secure and efficient key management framework. Each node only selects and propagates to neighbours based on two set of routing policies. They are Import and Export Routing policies. The IDPFs uses a feasible path from source node to the destination node and the packet can reach to the destination through one of its upstream neighbours. 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. An authentication framework for hierarchical, ad hoc sensor networks is proposed However, 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.

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 correlates 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 [5]. 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. The MAC sequence number has also been used in 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 [3],[7],[4] using RSS to defend against spoofing attacks are most closely related to us. 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 proposed to use the node's "spatial signature," including Received Signal Strength Indicator (RSSI) and Link Quality Indicator 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.

ALGORITHM

To evaluate the generality of IDOL for localizing attacks we have chosen a set of representative localization algorithms ranging from nearest neighbour matching in signal space (RADAR), to probability based (Area-Based Probability), and 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 neighbour 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)

Area-based probability ABP also utilizes an interpo-lated signal map [7].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 ¼ 1 . . . L, on the floor using Bayesian 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 ΣL

P(Li|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 1.1 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 = b0i+b1i logDi, where b0i, b1i are the parameters specific to the ith landmark.

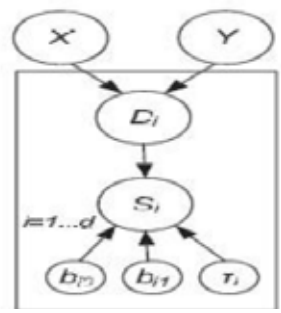

Fig 1.1 Graphical Model of Bayasian Network

The distance Di = √(X -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 distribution around the above propagation model, with variance τi: si~N(b0i + b1i logDi, τi). Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

CONCLUSION

In our conclusion is proposed to use received signal strength 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. 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. To further improve the accuracy of determining the number of attackers present in the system.

REFERENCE

[1] Yingying Chen,Jie Yang, Wade Trappe, Richard P. Martin,"Detecting and Localizing Identity Based Attacks in Wireless and Sensor Networks"- JUNE 2010. | | [2] Jie Yang, Student Member, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE,Wade Trappe, Member, IEEE, and Jerry Cheng "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks"- JAN 2013. | | [3] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil attacks in sensor networks," in Proc. 25th IEEE ICDCSW, Jun. 2005,pp. 185–191. | | [4] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc.OSDI, 1999, pp. 173–186. | | [5] A. Banerjea, "A taxonomy of dispersity routing schemes for fault-tolerant real-time channels," in Proc. ECMAST, May 1999, vol. 26, pp. 129–148. | | [6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC-layer spoofing using received signal strength," in Proc. IEE INFOCOM, Apr. 2008, pp. 1768–1776. | | [7] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., 2003,pp. 15–28. | | [8] W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," IEEE Wireless Commun., vol. 9, no. 6, pp. 44–51, Dec. 2002. | |