Detection and Localization of Multiple Spoofing

Attackers in Wireless Networks

**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. 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 spoofing 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. 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

testbeds 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 adversaries.

**Existing System**

The existing approaches to address potential spoofing attacks employ cryptographic schemes [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.

**Disadvantages**

* The 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.
* The accuracy of determining the number of attackers. 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.

**Proposed System**

The path loss exponent is set to 2.5 and the standard deviation of shadowing is 2 dB. From the figure, we observed that the ROC curves shift to the upper left when increasing the distance between two devices. This indicates that the farther away the two nodes are separated, the better detection performance that our method can achieve. This is because the detection performance is proportional to the noncentrality parameter which is represented by the distance between two wireless nodes together with the landmarks. Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space. The System Evolution is a new method to analyze cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energyis calculated as the average distance between elements in the border region of the twin clusters.

**Adavntages**

* The basic idea behind using the System Evolution method to determine the number of attackers is that all the rest of clusters are separated if the twin clusters are separable.
* The Hit Rate is lower when treating four attackers as errors than treating two attackers as errors. This indicates that the probability of misclassifying three attackers as four attackers is higher than that of misclassifying three attackers as two attackers.
* The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters.

**System Configuration**

**H/W System Configuration:-**

Processor – Intel core2 Duo

Speed - 2.93 Ghz

RAM – 2GB RAM

Hard Disk - 500 GB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor – LED

**S/W System Configuration:-**

Operating System: XP and windows 7

Front End: Visual studio 2010

Back End: SQL Server-2000