MULTIPLE SPOOFING IDENTIFICATION FOR NETWORK LEVEL SECURITY

G.Srikanth1, M.Ashok Kumar2
Student, M.Tech, V.R. Siddartha, Kanuru, Vijayawada
Assistant Profressor, M.Tech, V.R. Siddartha, Kanuru, Vijayawada

ABSTRACT

It’s easy to spoof the wireless networks using the mac identity and the ipconfig. The techniques which have been used based on the Matching rules of signal prints for spoofing detection, RSS readings using a Gaussian mixture model, RSS and K-means cluster analysis. None of the approach can determine number of attackers when used the same identity by adversaries. And the other techniques used to localize the attack detection Chen-et-al studied how to localize adversaries but can only handle only a single attack this study cannot detect if the attacker use different transmission power levels for sniffing the network. Where it is not possible to gain the knowledge needed to implement. We can overcome these approaches disadvantages by using our proposed system. We use ABP, Silence Mechanism, SVM for our proposed system, beside of the algorithms based on Radar-gridded algorithm, Bayesian network for the graphical identity, cluster analysis and the area based probability.

INTRODUCTION

The wireless transmission medium, adversaries can monitor any transmission. In various types of attacks, identity based spoofing attacks are especially easy to launch and can cause significant damage to network performance. In 802.11 networks, 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 ipconfig command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA),or 802.11i (WPA2) [3], such methodology can only protect data frames - an attacker can still spoof management or control frames to cause significant impact on networks.

IDS watch the wired and wireless network from the inside and report or alarm depending on how they evaluate the network traffic they see. They continually monitor for access points to the network and are able, in some cases, to do comparisons of the security controls defined on the access point with pre-defined company security standards and either reset or closedown any non-conforming AP’s they find. The distinction between placing IDS sensors on both wired and wireless networks is an important one as large corporate networks can be worldwide. IDS systems can also identify and alert to the presence of unauthorized MAC addresses on the networks. This can be an invaluable aid in tracking down hackers.

Spoofing attacks can further facilitate a variety of traffic injection attacks, 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 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 [1]. Therefore, it is important to detect the presence of spoofing attacks, determine the number of attackers, and localize multiple adversaries and eliminate them.

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 [1] an integrated detection and localization system that can both detect attacks as well as find he positions of multiple adversaries even when the adversaries vary their transmission power levels.

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 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.

The fact that wireless channel response de-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 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.

In WSN network 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 in performs of 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.

REVIEW OF LITERATURE

1) Supporting Anonymous Location Queries in Mobile Environments with Privacy grid

AUTHORS: B. Bamba, L. Liu, P. Pesti, and T. Wang

This paper presents Privacy Grid [4] - a framework for supporting anonymous location-based queries in mobile information delivery systems. The Privacy Grid framework offers three unique capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment. We develop dynamic bottom-up and top-down grid cloaking algorithms with the goal of achieving high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. A hybrid approach that carefully combines the strengths of both bottom-up and top-down cloaking approaches to further reduce the average anonymization time is also developed. Last but not the least, Privacy Grid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. We also discuss Privacy Grid mechanisms for supporting anonymous location queries. Experimental evaluation shows that the privacy Grid approach can provide close to optimal location k-anonymity as defined by per user location P3P without introducing significant performance penalties.

2) On the Value of a Random Minimum Weight Steiner Tree

AUTHORS: B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov

Consider a complete graph on n vertices with edge weights chosen randomly and independently from an exponential distribution with parameter λ. Fix k vertices and consider the minimum weight Steiner tree which contains these vertices. We prove that with high probability the weight of this tree is (1 + o(1))(k − 1)/(log n) when k = o(n) and n → ∞.

3) Random Key Predistribution Schemes for Sensor Networks

AUTHORS: H. Chan, A. Perrig, and D. Song

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary [6]. We present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key redistribution’s strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, we present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

4) Enhancing Base Station Security in Wireless Sensor Networks

AUTHORS: J. Deng, R. Han, and S. Mishra

Wireless sensor networks that are deployed in applications such as battlefield monitoring and home security systems face acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes. Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource constrained sensor nodes [7]. Prior work that has focused on securing the routing between sensor nodes has assumed that the base station is sufficiently powerful to defend itself against security threats. This paper considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. First, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks and/or compromise. Second, confusion of address and identification fields in packet headers via hashing functions is explored as a technique to help disguise the location of the base station from eavesdroppers. Third, relocation of the base station in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage.

5) Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks

AUTHORS: J. Deng, R. Han, and S. Mishra
Wireless sensor networks face acute security concerns in applications such as battlefield monitoring. A central point of failure in a sensor network is the base station, which acts as a collection point of sensor data. In this paper, we investigate two attacks that can lead to isolation or failure of the base station [8]. In one set of attacks, the base station is isolated by blocking communication between sensor nodes and the base station, e.g. by DOS attacks. In the second attack, the location of the base station is deduced by analyzing data traffic towards the base station, which can lead to jamming and/or discovery and destruction of the base station. To defend against these attacks, two secure strategies are proposed. First, secure multi-path routing to multiple destination base stations is designed to provide intrusion tolerance against isolation of a base station. Second, anti-traffic analysis strategies are proposed to help disguise the location of the base station from eavesdroppers. A performance evaluation is provided for a simulated sensor network, as well as measurements of cryptographic overhead on real sensor nodes.

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 cause significant 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. 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.

PROPOSED SYSTEM

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. 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 and Chen et al. used RSS and K-means cluster analysis to detect spoofing attacks [20]. 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 proposed System used Inter domain Packet filters (IDPFs) architecture, a system that can be constructed solely based on the locally exchanged BGP updates.
• Each node only selects and propagates to neighbors 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 a packet can reach to the destination through one of its upstream neighbors.
• 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.
The data we retrieved and the protocol we selected for the network configuration is shown in the below output screenshot as we discussed previously in the previous figure.

Here in this frame we are creating the fifteen static nodes which are generated dynamically assuming the different signal strengths received by the different nodes. Where nodes represent the number of users and the signal strengths are calculated using signal prints which are calculated previously and we are making the nodes to communicate by forming a connection between the two different nodes. Such that we can make some attack on the node for the sake of attack detection.

The below T.B INSTRUMENTATION test application to vary the network bandwidth graph just for the monitoring of the network in the wave format and to highlight the network monitoring is being done in our developed project. With this test application we can change the graph format into sine wave, angular and etc, and here we even can monitor the noise redundancy of the network and usage of the bandwidth by the user.

Here we are finding the spoofing area from where the attack is being happened and on which node particularly the attacker is aiming to intrude some malware or spoofing the data or to monitor the conversation being happened between the two wireless users.

Here we are creating fifteen nodes again for the sake of detecting network coverage, RSSI locator, signal position, here the message popups are raised to show the different levels of our selecting options to which belonging we are giving the input of the network.
Here this is our final output shown depending the selection and classifiers mode the output is displayed, and in this frame we are detecting the multiple number of attackers on the same network identity, by using the mac address of the device and ip configured to the wireless device.

If we observe there are multiple options for the varying output depending on the selection of mode. The following screens demonstrate the different modes of the output on our preference of selection of the methodology on various mechanisms we used as discussed previously in the proposed system.

**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 for detecting 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 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 testbeds through both an 802.11 network (WiFi) and an 802.15.4 (ZigBee) 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


