ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 6 Issue 3 (Pages 43- 50)
IJREB
Journal home page: www.ijreb.org

AN INTEGRATED INTRUSION DETECTION SYSTEM (IIDS) FOR MULTIPLE SPOOFING ATTACKS

Shiyas K R[1], A. Anitha[2], A. Anisha[3]

[1,2]Department of Computer Science & Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, KanyaKumari , Tamil Nadu, India
[3] Department of Computer Science & Engineering, St.Xavier's Catholic College of Engineering, Chunkankadai, KanyaKumari , Tamil Nadu

ABSTRACT

Open nature of wireless transmission is risky for communication and transmission of information. Any adversaries can monitor and intrude the network communication within the transmission range. Attackers can take variety forms instance attackers can impersonate the IP (internet protocol) address of any existing system in the network and acquire information and affect the performance of the system. Generally the traditional intrusion detection system identify a node through cryptographic authentication, conventional security approaches which is always desirable because of their overhead requirements .This paper proposes the usage of spatial information, a physical property associated with each node, which is hard to falsify, and not dependent on cryptography, this will help determining the number of attackers when multiple adversaries masked as the same node identity and localizing multiple adversaries. This paper use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Based on the signal strength from the sensor to system the attackers can be mapped.

KEYWORDS: Wired Equivalent Privacy; WiFi Protected Access; Integrated detection and localization; Received Signal Strength; GADE; IDOL

I. INTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities. The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real-time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to in situ monitoring of the health of structures or equipment, while often

referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world.

The most straightforward application of wireless sensor network technology is to monitor remote environments for low frequency data trends. For example, a chemical plant could be easily monitored for leaks by hundreds of sensors that automatically form a wireless interconnection network and immediately report the detection of any chemical leaks. Unlike traditional wired systems, deployment costs would be minimal. Instead of having to deploy thousands of feet of wire routed through protective conduit, installers.

Simply have to place quarter-sized device, such as the one pictured in Figure at each sensing point. The network could be incrementally extended by simply adding more devices – no rework or complex configuration. With the devices presented in this thesis, the system would be capable of monitoring for anomalies for several years on a single set of batteries.

In addition to drastically reducing the installation costs, wireless sensor networks have the ability to dynamically adapt to changing environments. Adaptation mechanisms can respond to changes in network topologies or can cause the network to shift between drastically different modes of operation. For example, the same embedded network performing leak monitoring in a chemical factory might be reconfigured into a network designed to localize the source of a leak and track the diffusion of poisonous gases. The network could then direct workers to the safest path for emergency.

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 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.

II.RELATED WORKS

Faria et al. [1] proposed that a transmitting device can be robustly identified by its signal print, a tuple of signal strength values reported by access points acting as sensors. This method show thatthe MAC addresses or other packet contents are different from attackers does not have as much control regarding the signal prints they produce. This system also demonstrates that signal prints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity.

Yang et al. [2] proposed a method for detecting spoofing attacks in the mobile wireless environment, which is when wireless devices, such as the victim node and/or the spoofing node are moving. We develop the DEMOTE system, which exploits Received Signal Strength (RSS) traces collected over time and achieves an optimal threshold to partition the

RSS traces into classes for attack detection. Further, a novel algorithm alignment prediction (ALP), when without the knowledge of spatial constraint of the wireless nodes, utilizes temporal constraints to predict the best RSS alignment of partitioned RSS classes for RSS trace reconstruction over time. This approach does not require any changes or cooperation from wireless devices other than packet transmissions.

The major contribution of Wu et al. [3] is SEKM,designed to provide efficient share updating among servers and to quickly respond to certificate updating, which are two major challenges in a distributed CA scheme. The basic idea is that server nodes form the underlying service group for efficient communication. For efficiency, only a subset of the server nodes initiates the share update phase in each round.

Ferreri et al. [4] identifies some simple attack schemes that might lead to a DoS effect and then observed the reactions of various types of infrastructure networks to these attacks. This method identified that 802.11 protocol is based on the exchange of request/response messages: each request sent by a station (STA) in the network triggers a corresponding response on its counterpart, which can be, in turn, another station or an Access Point (AP) infrastructure networks rely on an access point (or a set of them) as a central node through which every communication is routed, thus an AP can easily become a bottleneck for the entire network (or, at least, for the Basic Service Set it defines1). An AP failure causes the block of the entire network or a part of it attack patterns should be as simple as possible, in order to apply both to open systems and WEP-protected networks. From this viewpoint, a malicious station should be able to launch an attack even if it is neither associated nor authenticated to the target network. To carry out such attacks only commodity hardware and software components are required.

Chen et al. [5]proposed a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks. First an attack detector for wireless spoofing that utilizes K-means cluster analysis is proposed. Next, this work integrated the attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. Then it showed that the positions of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case. The proposed methods are evaluated through experimentation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network.

Bohge et al. [6] explored the task of providing data and entity authentication for hierarchical ad hoc sensor networks. The sensor network of this method consists of three tiers of devices with varying levels of computational and communication capabilities. The lowest tier

consists of compute-constrained sensors that are unable to perform public key cryptography. To address this resourceconstraint, a new type of certificate, called a TESLA certificate that can be used by low-powered nodes to perform entity authentication is used. Theframework authenticates incoming nodes, maintains trust relationships during topology changes through an efficient handoff scheme, and provides data origin authentication for sensor data. Further, the framework assigns authentication tasks to nodes according to their computational resources, with resource-abundant access points performing digital sig- natures and maintaining most of the security parameters.

III.PROPOSED METHOD

Most existing approaches to address potential spoofing attacks employ cryptographic schemes. Mobile ad hoc networks are special type of wireless networks in which a collection of mobile hosts with wireless network interfaces may form a temporary network, without the aid of any fixed infrastructure or centralized administration. While mobile ad hoc networks can be quickly and inexpensively setup as needed, security is a critical issue compared to wired or other wireless counterparts. Many passive and active security attacks could be launched from the outside by malicious hosts or from the inside by compromised hosts Cryptography is an important and powerful tool for security services, namely authentication, confidentiality, integrity, and non-repudiation. Key management is a basic part of any secure communication. Most cryptosystems rely on some underlying secure, robust, and efficient key management system.

Key management deals with key generation, storage, distribution, updating, revocation, and certificate service, in accordance with security policies. The major contribution of this scheme is that SEKM is designed to provide efficient share updating among servers and to quickly respond to certificate updating, which are two major challenges in a distributed CA scheme.

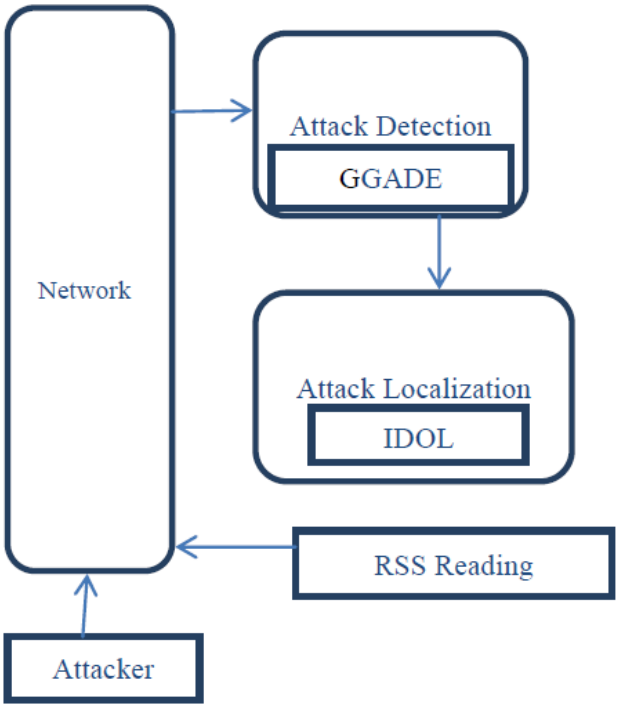

Fig. 1. Architecture of the proposed System.

The basic idea is that server nodes form the underlying service group for efficient communication. For efficiency, only a subset of the server nodes initiates the share update phase in each round.

This paper proposes the usage of spatial information, a physical property associated with

each node, which is hard to falsify, and not dependent on cryptography, this will help determining the number of attackers when multiple adversaries masked as the same node identity and localizing multiple adversaries. This project use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Based on the signal strength from the sensor to system the attackers can be mapped. Fig. 1.portraits the architecture for the proposed system.

This work proposesthe usage of received signal strength (RSS)-based spatial correlation, A physical property associated with each wireless node that is hard to falsify and not reliant (dependent) 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. The main advantage of using RSS is that employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves. This work focuses on static nodes, which are common for spoofing scenarios.

The main contributions of this paper 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.

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.

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 percentage 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.

IV. RESULTS AND DISCUSSIONS

This proposed system consists of two types of sensors in the network model. The wireless sensors deployed in the large scale area and the landmarks/access points that are

monitoring the RSS of the wireless nodes and know their locations. We focus on static nodes in this work, which are common for spoofing scenarios, wireless sensor networks and Access points.

In 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 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. 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.

We propose to study RSS, a property closely correlated with location in physical space and is readily available in the existing wireless networks. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks. We describe our Generalized Attack Detection Model, which consists of two phases: attack detection, which detects the presence of an attack, and number determination, which determines the number of adversaries.

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 multiclass 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 are available, we propose to use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

IDOL isan 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. We developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries.

This work uses RSS, a property closely correlated with location in physical space and is readily available in the existing wireless networks. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e.,

reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

The RSS value is defined as $s = \{s1; s2; \ldots . sn\}$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations. Generally, the RSS at the itch landmark from a wireless node is lognormally distributed.

V. PERFORMANCE ANALYSIS

The performance of the proposed IIDS for multiple spoofing attacks is analyzed for the number of intrusions and the detection rate is identified. Because of the GADE, the Partitioning AroundMedoids (PAM) cluster analysis method to detect the attack the detection rate is higher as the number of intrusions increases.IDOL isan integrated detection and localization system detected attacks as well as found the positions of multiple adversaries even when the adversaries vary their transmission power levels. The integrated system IDOL, utilized the results of the number of attackers returned by GADE to further localize multiple adversaries.

The detection rate of the proposed method is higher compared to the existing cryptographic system. 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. The cryptographic methods are vulnerable to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned. Due to these disadvantages the detection rate of the existing system is very low compared to the proposed system.

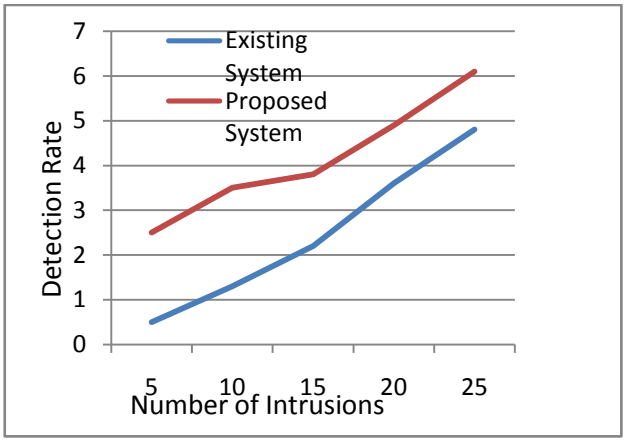

Fig.2. Analysis of the Detection Rate with increasing number of intrusions

Fig.2 portraits the analysis of the detection rate with the increasing number of intrusions. As the number of intrusions increases the proposed method with the GADE performs well than the existing cryptographic system with high detection rate.

VI. CONCLUSION

This paper use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Based on the signal strength from the sensor to system the attackers are mapped. This method used the GADE to detect the attack,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. This method use the IDOL, can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. The performance of the proposed system is analysed with multiple intrusions and the detection rate is compared with the existing cryptographic system. The proposed IIDS for multiple spoofing attacks with the GADE and IDOL achieved high performance even in the presence of high level of intrusions.

REFERENCES

[1].Daniel B. Faria, David R. Cheriton,"Detecting IdentityBased Attacks Literature in Wireless Networks Using Signalprints", Proceedings of the 5th ACM workshop on wireless security, September 2006, pp.43-52.

[2]. Jie Yang, Yingying Chen, Wade Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments ",6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2009 , pp. 1-9 .

[3]. Bing Wu, Jie Wu, Eduardo B. Fernandez, Spyros Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks", Journal of Network and ComputerApplications, Vol. 30, No. 3, August 2007, pp. 937-954.

[4]. F. Ferreri, M. Bernaschi , L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks" Journal of Wireless Networks, Springer, Vol.14, October 2006, pp. 159-169.

[5]. Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks", IEEE Transactions on Vehicular Technology, Vol.59, No.3, June 2010, pp. 2418-2434.

[6]. M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks", Proceedings on the 2nd ACM workshop on Wireless Security, September 2003, pp. 79-83.