Survey Paper on Spoofing Detection in Wireless Network

Pratibha Thakre, Prof. A. N. Jaiswal, Prof. S. J. Karale

Abstract—**Spoofing Attack is one of the vulnerabilities in the wireless networks, which is a situation in which the intruder successfully pretends as legal one. These attacks will affect the network performance violating the network protocols. A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware, or bypass access controls While significant research effort has been dedicated to wireless localization over the past decades, most aspects of location security have been overlooked. In particular, adversaries can take advantage of security vulnerabilities of current location systems to launch location spoofing attacks, thus disguising their position in the network. The node can be prevented and verified by cryptography but conventional security approaches are cannot be executed always due to their tough prerequisites. In this paper we are proposing far-reaching information which will detect the IP spoofing attack and prevent it using received signal strength (RSS).**

***Keywords*—Wireless network, Spoofing attack, attack detection**

I. Introduction

Today is a wireless world. Almost every network is shared and attackers take the advantage of this for collecting useful identity information by passive monitoring. This gathered identity is being used by attackers resulting into SPOOFIING Attack. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and utilize the identity information to launch spoofing attacks in wireless and sensor networks.

Spoofing is the action of making something look like something that it is not in order to gain unauthorized access to a user's private information. It is of type-
IP Spoofing, URL Spoofing, Email Spoofing, DNS Spoofing
We are concentrating on the IP address or IP spoofing only in this paper

A. *IP Spoofing Overview*

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false (or “spoofed”) source address in order to disguise it. Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses. There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target’s IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target’s IP address, all responses to the spoofed packets will be sent to (and flood) the target’s IP address. IP spoofing attacks can also be used to bypass IP address-based authentication. This process can be very difficult and is primarily used when trust relationships are in place between machines on a network and internal systems. Trust relationships use IP addresses to verify machines’ identities when attempting to access systems. This enables malicious parties to use spoofing attacks to impersonate machines with access permissions and bypass trust-based network security measures.

IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. IP address spoofing is the creation of IP packets using somebody else’s IP source addresses. This technique is used for obvious reasons and is employed in several of the attacks.

II. Feasibility of Attacks

In this section, we provide a brief overview of IP-Spoofing attack and their impact to the wireless and sensor networks.

A. *Blind Spoofing*

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data could be sent to the target.

B. *Non-Blind Spoofing*

This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets. The threat of this type of spoofing is session hijacking and an attacker could bypass any authentication measures taken place to build the connection. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.

C. *Man-in-the-Middle Attack*

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances. A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other — it is an attack on mutual authentication. A Man-in-the-Middle Attack allows a malicious actor to intercept, send, and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.

D. *Denial-Of-Service Attack*

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests’. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management. It is essential best practice to implement ant spoofing mechanisms to prevent IP spoofing wherever feasible. Anti spoofing control measures should be implemented at every point in the network where practical, but they are usually most effective at the borders among large address blocks or among domains of network administration.

III. Related Work

There has been active research recently on spoofing as well as those facilitated by adversaries masquerading as another wireless device. We cannot cover the entire body of works in this section. Rather, we give a short overview of traditional approaches and several new methods. We then describe the works most closely related to our work.

The traditional security approach to prevent identity fraud is to use cryptographic authentication [10]. As it is not always desirable to use authentication due to limited resources on wireless nodes and infrastructural overhead involved, recently new approaches utilizing wireless transmission properties such as RSS and the wireless channel have been proposed [11], [4]. [11] introduced a security layer that is separate from conventional network authentication methods. They developed forge-resistant relationships based on packet traffic to detect spoofing attacks. [9] Utilizes properties of the wireless channel to support security objectives. To detect mobility of wireless nodes, [10] determined mobility from GSM traces using Euclidean distance in signal space. [11] used RSS collected in wireless LAN to detect wireless device mobility. In [9] signal variance is used with Hidden Markov Model (HMM) to eliminate oscillations between the static and mobile states for mobility detection. Further, [2] proposed to use correlation coefficients on RSS traces to detect wireless devices that are moving together. The works that are most closely related to us are [3], [1]. [11] proposed the use of matching rules of singalprints such as differential values, max-matches, and min-matches to detect identity-based spoofing. [3] implemented a spoofing detector by utilizing K-means cluster analysis in the signal space. Further, [12] captured the effects of antenna diversity and used Gaussian Mixture Modeling (GMM) for RSS profiling to detect spoofing attacks. Although these methods have varying detection and false alarm rates, none of these approaches can detect spoofing attacks in mobile wireless environments.

An authentication framework for hierarchical, ad hoc sensor networks is proposed in [13] and a hop-by-hop authentication protocol is presented in [13]. Additional infrastructural overhead and computational power are needed to distribute, maintain, and refresh the key management functions needed for authentication. [10] has introduced a secure and efficient key management framework (SEKM). SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. [4] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. In addition, binding approaches are employed by Cryptographically Generated Addresses (CGA) to defend against the network identity spoofing [5], [6]. Due to the limited resources in wireless and sensor nodes, and the infrastructural overhead needed to maintain the authentication mechanisms, it is not always desirable to use authentication. Recently new approaches have been proposed to detect the spoofing attacks in wireless networks. [7], [8] have introduced a security layer that is separate from conventional network authentication methods. They developed forge-resistant relationships based on packet traffic by using packet sequence numbers, traffic interarrival, one-way chain of temporary identifiers, and signal strength consistency checks to detect spoofing attacks. [3] proposed a lowerlayer approach that utilizes properties of the wireless channel at the physical layer

to support high-level security objectives such as authentication and confidentiality. [7], [8] have introduced a security layer that is separate from conventional network authentication methods. They developed forge-resistant relationships based on packet traffic by using packet sequence numbers, traffic interarrival, one-way chain of temporary identifiers, and signal strength consistency checks to detect spoofing attacks. [3] Proposed a lower layer approach that utilizes properties of the wireless channel at the physical layer to support high-level security objectives such as authentication and confidentiality. Although these methods have varying detection and false alarm rates, none of these approaches provide the ability to localize the positions of the spoofing attackers after detection.
This work differs from the previous study in that we use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore they explore methods for spoofing attack detection as well as prevention when wireless devices are moving around.

IV. Noteworthy Contribution

[1] Yingying Chen, Wade Trappe, Richard P. Martin in 2008 - Proposed a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks. They first propose an attack detector for wireless spoofing that utilizes K-means cluster analysis. Next, describe how integrated attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. Then show 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.
[2] Jie Yang, Yingying Chen, and Wade Trappe in 2010- Proposed a method for detecting spoofing attacks in the mobile wireless environment that is when wireless devices are moving. They develop the 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. 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 by using algorithm alignment prediction (ALP). Their approach does not require any changes or cooperation from wireless devices other than packet transmissions. Through experiments from an office building environment, we show that DEMOTE achieves accurate attack detection both in signal space as well as in physical space using localization and is generic across different technologies including IEEE 802.11 b/g and IEEE 802.15.4.
[3] Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, and Jerry Cheng in 2013- Proposed 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. They propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. They 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, they explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers, also developed an integrated detection and localization system that can localize the positions of multiple attackers.

V. Summary

As wireless networks are integrated with our daily social lives, there is an increasing need to support emerging mobile wireless applications. One serious class of threats that will affect the successful deployment of mobile wireless applications is spoofing attacks. In this work, we discuss a method for detecting spoofing attack in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, our RSS based approach does not add additional overhead to the wireless devices and sensor nodes. Also about system, which utilizes an optimal thresholding scheme to partition the RSS readings and further reconstruct the RSS traces over time for attack detection. Further, we discuss noteworthy contribution in spoofing detection and prevention methods.

Prof. A.Jaiswal
G,H,R.I.E.T.W , Nagpur University
MH. India.

Prof. S.J.Karale
YCCE, Nagpur University
MH. India.

Acknowledgment

We would like to express our deepest of gratitude to our project guide, Prof. S.J. Karale, Associate Professor, Department of Computer Science and Engineering, YCCE, Nagpur for giving us this wonderful opportunity to work under him and to provide us with valuable guidance and the necessary support throughout the course of this project.

We would also like to express our sincere thanks Prof. A.Jaiswal G.H.R.I.E.T.W , Nagpur for helping me throughout the development of this paper.

References

[1] Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, and Jerry Cheng, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks,” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013.

[2] 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.

[3] Y. Chen, W. Trappe, and R.P. Martin, “Detecting and Localizing Wireless Spoofing Attacks,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[4] T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J. Sievanen, “Wireless Information Networks,” International Journal of Parallel and Distributed Processing, 2007.

[5] Yingying Chen, Jie Yang, Wade Trappe, and Richard P. Martin, “Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks,”IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 59, NO. 5, JUNE 2010.

[6] Manusankar, C. ; Karthik, S. ; Rajendran, T., “Intrusion Detection System with packet filtering for IP Spoofing,” International Conference on Communication and Computational Intelligence, 2010.

[7] Fanglu Guo, Jiawu Chen, and Tzi-cker Chiueh,“Spoof Detection for Preventing DoS Attacks against DNS Servers,” IEEE International Conference on Distributed Computing Systems, 2006.

[8] Jeong Heon Lee, Buehrer, R.M., “Location Spoofing Attack Detection in Wireless Networks,“IEEE Conference on Global Telecommunications , 2010.

[9] Y. Chen, W. Trappe, and R. Martin, “Attack Detection in Wireless Localization,” IEEE International Conference on Computer Communications, Apr. 2007.

[10] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2005.

[11] D. Faria and D. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.

[12] Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), September 2006.

[13] M. bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003.

Pratibha R. Thakre:

Discussing far-reaching information which will detect the IP spoofing attack and prevent it using received signal strength (RSS) in contrast to traditional identity-oriented authentication methods.