Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Localization of Multiple Spoofing Attackers

Shyam Jadhav, Yogesh Katke, Vaibhav Joshi, Sagar Thore
Department of Computer Engg. Dr. D.Y. Patil College of Engg, Pune,
Savitribai Phule Pune University, India

Abstract: ***Wireless network are openness in nature and it is easy for spoofing attacker to launch wireless spoofing attackers which causes threat for data security and impact performance of a network. In conventional security cryptographic authentication is used to verify the nodes which are not desirable because of network overhead requirement. In this paper I use special information, that is a physical property associate with each node, which is very hard to falsify, and it does not depend on cryptography. This physical property can used for detecting spoofing attacker present in the network, determining the number of attacker when multiple adversaries masquerade as the same node identity as that of other node and localizing multiple adversaries. Then the problem of determining the number of attackers as multiclass detection problem is formulated. Cluster-based mechanisms are developed to determine the number of attackers. When the training data is available, Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers. In addition, integrated detection and localization system is used to localize the positions of multiple attackers.***

Keywords: Wireless network security, Spoofing attack, Attack detection, Localization

I. INTRODUCTION

In wireless network it is very difficult to identify multiple spoofing attacks because wireless network has openness in nature and each and every node have their own node identity which is very essential to recognize and differentiate one node from other node. As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is very easy for an attacker to purchase a low price wireless device and can use these commonly available platforms to launch various type of wireless spoofing attack. There are different types of attacks which can be performed by attackers, among this attacks identity-based attacks are easy to launch and cause significant damage to network performance. Therefore, it is important to detect the presence of spoofing attackers, determine the number of attackers and to localize multiple adversaries ant eliminate them. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational poor associated with distributing, and maintaining cryptographic keys. Due to the limited, poor and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network. In this paper, I take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, I propose a scheme for both detecting spoofing attacks, as Ill as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) and a physical property associate with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Using spatial information to address spoofing attackers has the unique power to not only identify the presence of these attackers but also localize adversaries. It does not require additional cost or modification to wireless device to identify spoofing attacks. In this I proposed to use a general attack detection module (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis and an integrated detection and localization system (IDOL) which can detect both attacker as well as position of multiple attacker even when the attacker vary their power level.

The scope of this paper is to detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries If an intruder comes during transaction, then server discover and localize that specific system. So that the data transmitted by the sender can be receive only by authenticated receiver not by the attacker who masquerades as the same identity of original node and to eliminate the attack to make data transmission secure.

In the proposed system I proposed to use 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; and an integrated detection and localization system (IDOL) that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. In GADE, the Partitioning around Medoids (PAM) cluster analysis method is used to perform attack

detection. After that I formulate the problem of determining the number of attackers as a multiclass detection problem and then I applied cluster-based methods to determine the number of attacker. To improve the accuracy of determining the number of attackers a mechanism called SILENCE, when the training data are available, Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers. Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries.By this method it is possible to detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries without causing overhead in wireless network.

ARCHITECTURE:

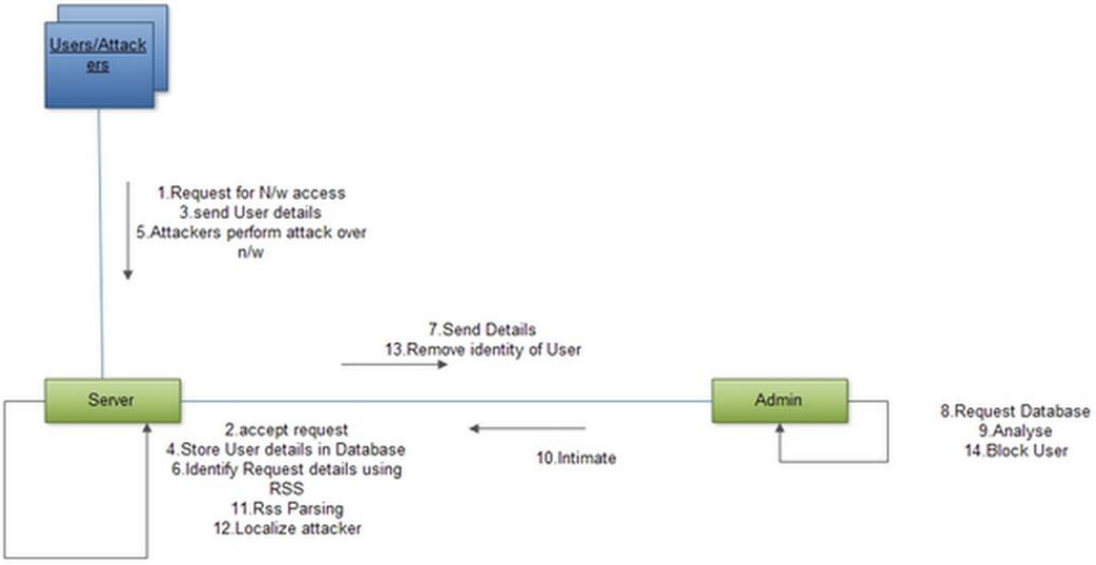

Fig. System Architecture

II. RELATED WORK

Real Vulnerabilities and Practical Solutions: The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols This paper provides an experimental analysis of such 802.11-specific attacks their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.[1]

We describe possible denial of service attacks to infrastructure wireless 802.11 networks. To carry out such attacks only commodity hardware and software components are required. The results show that serious vulnerabilities exist in different access points and that a single malicious station can easily hinder any legitimate communication within a basic service set. [2]

Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a septic client or to create multiple illegitimate identities. For example, several link-layer services in IEEE 802.11 networks have been shown to be vulnerable to such attacks even when 802.11i/1X and other security mechanisms are deployed. In this paper we show that a transmitting device can be robustly indentured by its signal print, a topple of signal strength values reported by access points acting as sensors. We show that, deferent from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce. Moreover, using measurements in a tested network, we demonstrate that signal prints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity. By tagging suspicious packets with their corresponding signal prints, the network is able to robustly identify each transmitter independently of packet contents, allowing detection of large class of identity-based attacks with high probability. [3]

Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. In this paper we propose a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks. We first propose an attack detector for wireless spoofing that utilizes K-means cluster analysis. Next, we describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. We 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. We have evaluated our methods through experimentation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. Our results show that it is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer. [5]

The flexibility and openness of wireless networks enables an adversary to masquerade as other devices easily. Identity-based spoofing attacks are serious network threats as they can facilitate a variety of advanced attacks to undermine the normal operation of networks. However, the existing mechanisms can only detect spoofing attacks when the victim node and the spoofing node are static. In this paper, we propose a method for detecting spoofing attacks in the mobile wireless environment that 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. Fur ther, our 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. Our 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. [6]

Hierarchical architectures are more and more widely adopted for organizing wireless sensor networks. In such architectures, middle-tier nodes take important roles, and preventing a malicious node from impersonating a middle-tier node and injecting falsified messages becomes critical. In this paper, we propose an energy efficient, distributed scheme to secure the multicast messages from the middle-tier nodes. Our scheme does not require a priori knowledge about the hierarchical relation between middle-tier nodes and lowest-tier nodes, and is adaptive to changes of this relation. Extensive simulations are conducted to evaluate our scheme, and the results show that the scheme is energy efficient. [4]

The IEEE 802.11 Wireless LAN standard has been designed with very limited key management capabilities, using up to 4 static, long term, keys, shared by all the stations on the LAN. This design makes it quite difficult to fully revoke access from previously-authorized hosts. A host is fully revoked when it can no longer eavesdrop and decrypt traffic generated by other hosts on the wireless LAN. This paper proposes WEP∗, a right weight solution to the host-revocation problem. The key management in WEP∗ is in the style of pay-tv systems: The Access Point periodically generates new keys, and these keys are transferred to the hosts at authentication time. The fact that the keys are only valid for one re-key period makes host revocation possible, and scalable: A revoked host will simply not receive the new keys. Clearly, WEP∗ is not an ideal solution, and does not address all the security problems that IEEE 802.11 suffers from. However, what makes WEP∗ worthwhile is that it is 100% compatible with the existing standard. And, unlike other solutions, WEP∗ does not rely on external authentication servers. Therefore, WEP∗ is suitable for use even in the most basic IEEE 802.11 LAN configurations, such as those deployed in small or home offices. A WEP∗ prototype has been partially implemented using free, open-source tools. [7]

TABLE:

Ref.No	Reference Name
[1]	802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions
[2]	Access Points Vulnerabilities to Dos Attacks in 802.11 Networks
[3]	Detecting Identity-Based Attacks in Wireless Networks Using Signal prints
[4]	An Authentication Framework for Hierarchical Ad Hoc Sensor Networks
[5]	Detecting and Localizing Wireless Spoofing Attacks
[6]	Detecting Spoofing Attacks in Mobile Wireless Environments
[7]	Lightweight Key Management for IEEE 802.11 Wireless Lans with Key Refresh and Host Revocation

III. CONCLUSION

In this work, I 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. I provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. I 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 I can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. I 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. Additionally, when the training data are available, I explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system. 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 levels. Our approach can detect multiple wireless Spoofing attacks and can also, determining the number of attackers and localizing adversaries.

REFERENCES

[1] J. Bellardo and S. Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions Proc. USENIX Security Symp. pp. 15-28, 2003.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,Proc. IEEE Wireless Comm. and Networking Conf., 2004.

[3] D. Faria and D. Cheriton, Detecting Identity-Based Attacks in Wireless Networks Using Signalprints,Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[4] M. Bohge and W. Trappe, An Authentication Framework forHierarchical Ad Hoc Sensor Networks, Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

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

[6] 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.

[7] A. Wool, Lightweight Key Management for IEEE 802.11 WirelessLans with Key Refresh and Host Revocation,ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

