IJMETMR
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Discovering Identity Theft (Spoofing) Using the Spatial Correlation of Received Signal Strength in Wireless Networks

Duggudurthypujyavenkata Rama Vivek
M.Tech,
Department of CSE,
Adikavinannaya University, Rajamahendravaram,
Andhra Pradesh, India.

Mrs.Voola Persis
Assisatnt Professor
Department of CSE,
Adikavinannaya University, Rajamahendravaram,
Andhra Pradesh, India.

Abstract:

In the context of network security, 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. Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message. In wireless networks, Spoofing attacks are relatively simple to launch as result it degrades the overall performance of the networks.

To identity an attacker node, it can be verified through cryptographic authentication, authentication is always not possible because it requires key management and additional infrastructural overhead. The proposed approach is used for 1) Detecting spoofing attacks 2) Determining the number of attackers when multiple adversaries masquerading the same node identity and 3) Localizing multiple adversaries. The proposed system uses spatial correlation of received signal strength (RSS) to detect the spoofing attacks. Cluster-based mechanisms are introduced to determine the number of attackers.

In this paper, K-Nearest-Neighbor classifier (KNN) is proposed to improve the performance of determining the number of attacks. Finally, An Integrated Detection and Localization system is used to localize the positions of multiple attackers.

Keywords:

Wireless network security, Spoofing attack, Localization, Detection,

Introduction:

Wireless security is just an aspect of computer security, however organizations may be particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) brings in a wireless router and plugs it into an unsecured switchport, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer via an open USB port, they may create a breach in network security that would allow access to confidential materials.

However, there are effective countermeasures (like disabling open switchports during switch configuration and VLAN configuration to limit network access) that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices. Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e.g. M2M communication in industrial applications.

Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. An evaluation of these vulnerabilities and the resulting vulnerability catalogues in an industrial context when considering WLAN, NFC and ZigBee can be found here. Identity theft (or MAC spoofing) occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires, and the hacker can easily get around that hurdle.

MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

RELATED WORK:

J. Bellardo and S. Savage worked on 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. 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.

F. Ferreri, M. Bernaschi, and L. Valcamonici, worked on Access Points Vulnerabilities to Dos Attacks in 802.11 Networks.They 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.

D. Faria and D. Cheriton worked on Detecting Identity-Based Attacks in Wireless Networks Using Signalprints. 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 they 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.

They 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, they 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. Y. Chen, W. Trappe, and R.P. Martin worked on Detecting and LocalizingWireless Spoofing Attacks. 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 they propose 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, they describe how they integrated attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. They 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. They have evaluated their methods through experimentation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. Their 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.

EXISTING SYSTEM:

•Ingress / Egress Filtering:

•Ingress – An ISP prohibits receiving from its stub connected networks packets whose source address does not belong to the corresponding stub network address space

•Egress – A router or a firewall which is the gateway of a stub network filters out any packet whose source address does not belong to the network address space.

DISADVANTAGES OF EXISTING SYSTEM:

•Allows Spoofing within a stub network

•Not self defensive

•Effective only when implemented by large number of networks

•Deployment is costly

•Incentive for an ISP is very low

PRPOSED SYSTEM:

•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.

ADVANTAGES OF PROPOSED SYSTEM:

•Damage Reduction under SPM Defense is high

•Client Traffic

•Comparing to other methods the benefits of SPM are more.

•SPM is generic because their only goal is to filter spoofed packets.

System Architecture:

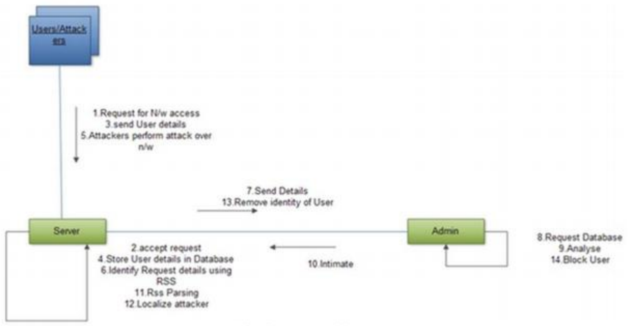


Fig. System Architecture

MODULES:

•Blind & Non-Blind Spoofing

•Man in the Middle Attack

•Constructing Routing Table

•Finding Feasible path

•Constructing Inter-Domain Packet Filters

•Receiving the valid packets

MODULES DESCRIPTION:

Blind & Non-Blind Spoofing:

•Spoofing detection is to devise strategies that use the uniqueness of spatial information.

•In location directly as the attackers' positions are unknown network RSS, a property closely correlated with location in physical space and is readily available in the wireless networks.

•The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive.

•The number of attackers when there are multiple adversaries masquerading as the same identity.

Man in the Middle Attack:

•Localization is based on the assumption that all measurements gathered received signal strength (RSS) are from a single station and, based on this assumption, the localization algorithm matches a point in the measurement space with a point in the physical space.

•The spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node.

•RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

Constructing Routing Table:

•The channel frequency response is sensitive to each multipath. An impulse in the time domain is a constant in the frequency domain, and thus a change to a single path may change the entire multiple tone link of Network.

•In wireless networks classes that provide automatic reconfiguration of APs, adjusting power levels and channel assignments to optimize coverage while minimizing contention between neighbors.

•The RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space.

Finding feasible path (Attack Computation):

•Converting the large dataset into medium format for the computation purpose.

•In this medium the rows consists of http request and columns consists of time for a particular user (IP address).

•Received Signal Strength Indicator Formula,

$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right)$$

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•The RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations.

Constructing Inter-Domain Packet Filters:

•The clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions and fake RSS clusters caused by outliers and variations of the signal strength.

•The minimum distance between two clusters is large indicating that the clusters are from different physical locations.

•The minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers.

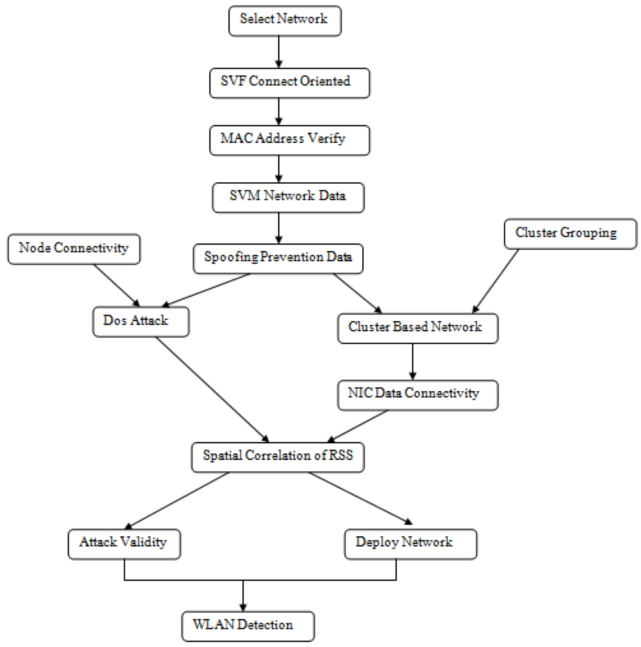
Receiving different Transmission Power:

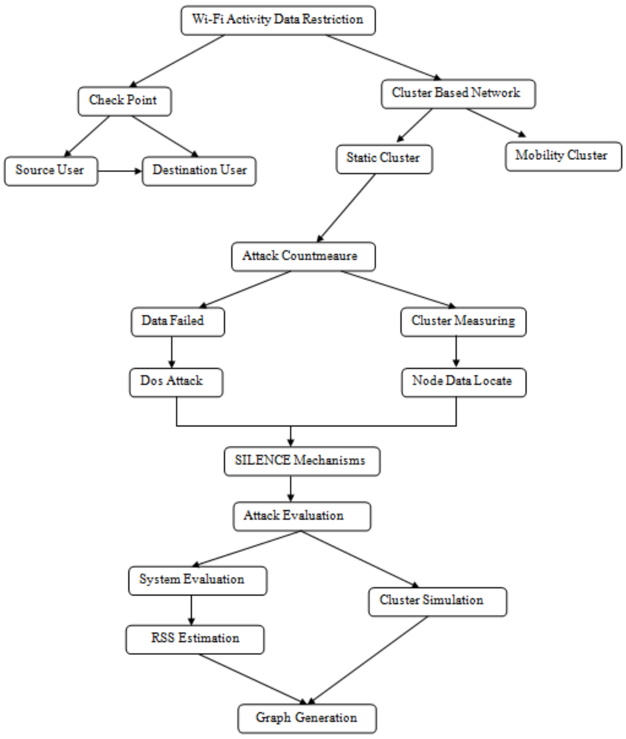
•The transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately.

•The CDF of localization error of RADAR-Gridded and ABP when adversaries using different transmission power levels.

•In detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of network.

Data Flow Diagram:





Conclusion:

This project 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. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that can localize any number of attackers and eliminate them. In addition, a zone-based node compromise detection scheme is proposed using the Sequential Probability Ratio Test (SPRT). Furthermore, several possible attacks are described against the proposed scheme and proposed counter-measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy zones with a small number of zone-trust reports.

REFERENCES:

[1]. Jie Yang, Yingying Chen, and Jerry Cheng, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks” in IEEE 2012.

[2]. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.

[3]. F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabilities to dos attacks in 802.11 networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.

[4]. 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.

[5]. Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in Proc. IEEE SECON, 2006.

[6]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in Proc. IEEE IPDPS, 2005.

[7]. A. Wool, “Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677–686, 2005.

[8]. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC layer spoofing using received signal strength,” in Proc. IEEE INFOCOM, April 2008.

[9]. J. Yang, Y. Chen, and W. Trappe, “Detecting spoofing attacks in mobile wireless environments,” in Proc. IEEE SECON, 2009.

[10]. Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wirelss spoofing attacks,” in Proc. IEEE SECON, May 2007.

[11]. 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, pp. 79–87.