IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.126107

Detection and localization of multiple spoofing attackers in wireless network

Mr.R. Ambikapathy, MCA. M.Phil[1], D. Dhanalakshmi[2]

Asst.Prof. Department of MCA & Krishnasamy College of Engineering & Technology[1]

Department of MCA & Krishnasamy College of Engineering & Technology[2]

Abstract: Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In this paper, we propose 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 a same node identity; and (3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multi-class detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When 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 addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. We evaluated our techniques through two testbeds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90% Hit Rate and Precision when determining the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

I. 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 if config 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), 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.

II. LITERATURE SURVEY

This paper presents Privacy Grid - 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 PrivacyGrid 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.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.126107

III. PROPOSED 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 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

Module 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 assumes 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). 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

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.126107

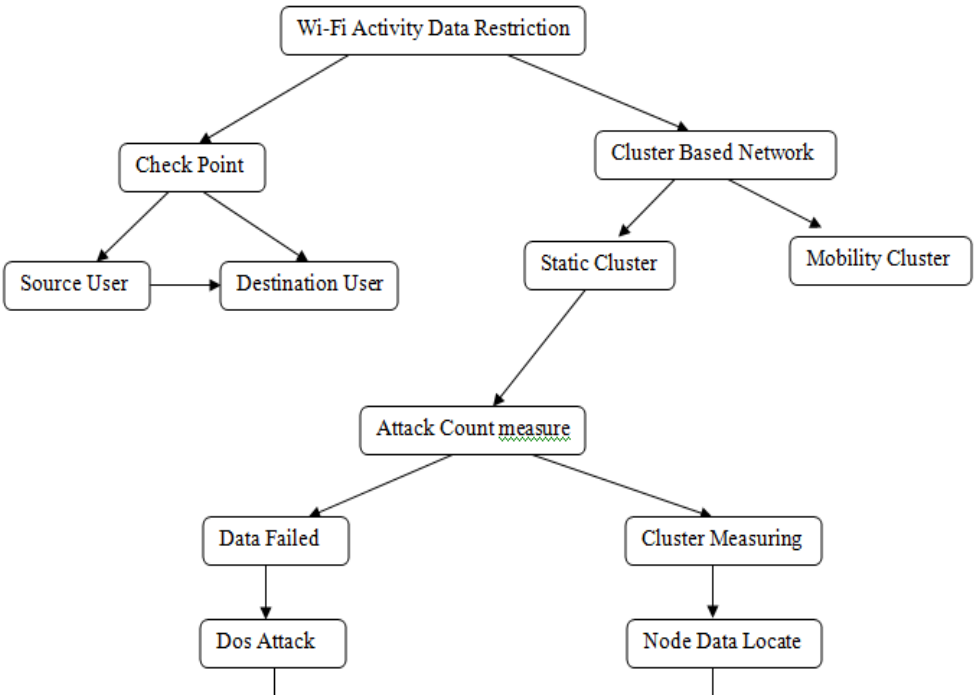
Packet Filters:

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.

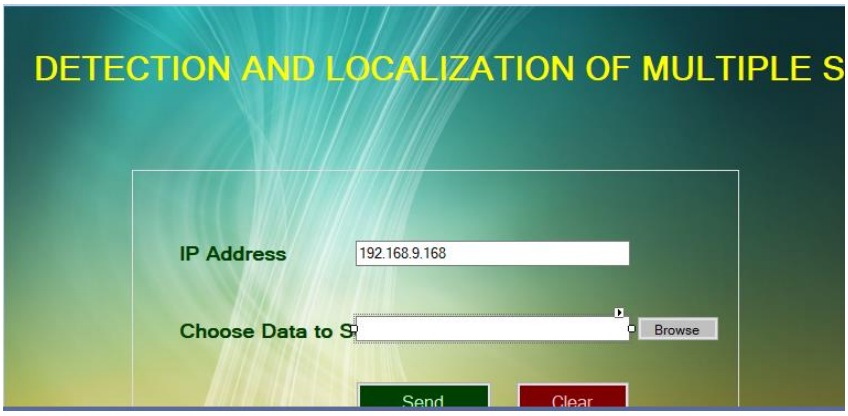
Receiving different Transmission Power:

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.

IV. WORK FLOW DIAGRAM FOR ANDROID



V. SCREEN SHOT



DOI: 10.17148/IJARCCE.2023.126107

VI. 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.

VII. FUTURE ENHANCEMENT

To validate our approach, we conducted experiments on two testbeds through both an 802.11network (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

[1] 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.
[2] 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.
[3] 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.
[4] Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in *Proc. IEEE SECON*, 2006.
[5] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in *Proc. IEEE IPDPS*, 2005.