International Journal of Technology and Engineering System (IJTES)
Vol 7. No.5 2015 Pp. 445-448

available at : www.ijcns.com
ISSN: 0976-1345

Spoofing Attack Detector Implementation for Wireless Spoofing using K-Implies Cluster Analysis

S. Prasanth[1], Dr. R. Indra Gandhi[2]
[1]PG Research Scholar, [2]Head of the Department
[1,2]Department of Master of Computer Applications
GKM College of Engineering and Technology, Chennai
[1]prasanthhari6@gmail.com, [2]shambhavi.rajesh@gmail.com

ABSTRACT

In today's wireless scenario, security place a prominent role and network administrator responsibilities plays a vital role to prevent attack , monitor access, misuse, modification, or denial of a and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Wireless systems are defenseless to spoofing attacks, which takes into consideration numerous different types of attacks on the systems. In this paper we propose a method for both detecting spoofing attacks, and spotting the positions of foes performing the attacks. We first propose an attack detector for wireless spoofing that uses K-implies cluster analysis. Next, we portray how we integrated our attack detector into a real time indoor confinement framework, which is additionally equipped for limiting the positions of the attackers. We show that the positions of the attackers might be confined utilizing either zone based or focus based confinement calculations with the same relative slips as in the ordinary case K-methods spoofing detector and also the attack localizer.

Keywords*:* Spoofing, Detection, k-methods, Spoofing Attacks, Spotting

I. Introduction

Device identity is perhaps one of the most challenging problems in any network for security. Localizing node is necessary for many higher level network functions such as tracking, monitoring and geometric-based routing and also used in broad area. It is easy to attack MAC addresses in IEEE 802.11 wireless network using publicly available tools. It is possible to implement many 802.11 attacks easily with the purchase of low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with a little effort. Spoofing attacks can further create a variety of traffic injection attacks.such as attacks on access control lists, rogue access point attacks, and eventually Denial-of- Service (DoS) attacks. Moreover, in a large-scale network, multiple adversaries may masquerade the same identity of the node and launch malicious attacks such as network resource utilization attack and DoS. Therefore, most of the approaches are introduced so for to prevent from spoofing attacks in wireless sensor network. It is important to detect the presence of spoofed in wireless network, determine the number of

attackers, and finding the location of multiple adversaries and defeat them. The presence of spoofing attack detection, count the number of attackers, identify the location of multiple adversaries in the network are challenging task in wireless sensor network. These problems are addressed by various authors by introducing different approaches. A number of traditional approaches are used in authentication application to address the problem of spoofing attacks.

II. Literature Survey

2.1. Identity-Based Attack Detection in Mobile Wireless Networks

Kai Zengi et al [1] approach in a Reciprocal Channel Variation-based Identification (RCVI) technique in 2006. Identity-Based Attacks (IBAs) are one of the most serious threats in wireless networks. The RCVI method is built based on RSS technique, to detect IBAs in mobile wireless networks.

RCVI takes advantage of the location de-correlation, randomness, and reciprocity of the wireless fading channel to decide whether all the packets come from a single sender or more. If the packets are only coming from the genuine sender, then RSS variations are reported by the sender that should be correlated with the receiver's observations. Otherwise, the correlation should be degraded and then an attack can be flagged. Results showed that RCVI achieved desirable performance under the tested scenarios and allows the user to tune the parameters to achieve strong security strengths.

2.2. Spoof Detection for Preventing DoS Attacks against DNS Servers

Fanglu Guo et al [2] expression against Spoof detection strategies for protecting Domain Name System (DNS) servers from DoS attacks. These strategies create some form of cookies for a DNS server to check whether each incoming request is from the source node or from other. Each DNS requester needs to obtain a unique cookie from a ANS (Authoritative Name Server). Spoofed requests cannot present correct cookie, thus it can be detected. The result showed that it can deliver up to 80K requests/sec to legitimate users in the presence of DoS attacks at the rate of 250K requests/sec.

2.3. Detecting and Localizing Wireless Spoofing Attacks

Yingying Chen et [3] proposed two approaches K-means cluster analysis and Area-based or Point-based Localization algorithms for wireless spoofing attack. The K-means is integrated as attack detector into a real-time indoor localization system, for localizing the positions of the attackers using either area based or point-based localization algorithms.

2.4. etecting 802.11 MAC Layer Spoofing Using Received Signal Strength

Sheng et al [4] attempt in spoofing detection approach based on Gaussian mixture models. The GMM is the mixture local statistics of a single AM, combining local results from AMs, and global multi-AM detection, respectively. The spoofing detection method is used for RSS profiling, and show how to use it to detect spoofing attacks.

2.5. Detecting Identity Spoofs in IEEE 802.11e Wireless Networks

Gayathri Chandrasekaran et al [5] proposed an architectural detection algorithm to detect the identity spoofing attacks robustly in 2009 [37]. Identity spoofing allows an attacker to avail network services that are normally restricted to legitimate users. Several techniques that rely on physical properties of transmitting devices are ineffective for the mobile attacker.

III. Implementation

In this form first we develop the access point module. In WSN, these access point module acts as an intermediate between the sensor node and sink node. Then browse a file to find particular folder and transform the status of the

receiver node to create txt node refer Figure 1 for the same.

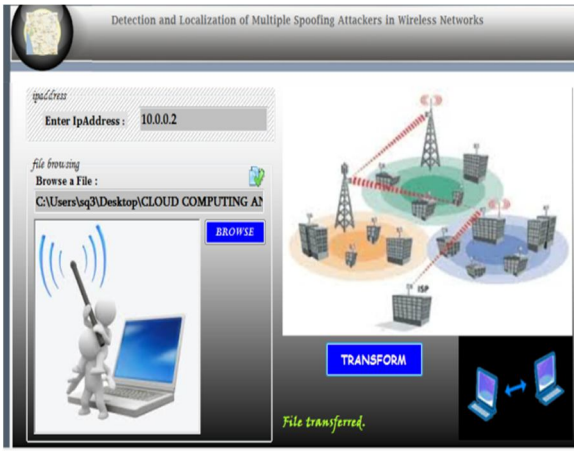

Figure 1. Localization of Attackers

In this module (refer figure 2),

- ✓ Its shown how we seen intermediate person while transformation was done.
- ✓ To identify the same node/ name and to identify the attackers from which signal it was routed and reachable from the sending file.
- ✓ The results of the proposed system helps in analyzing various performance metrics such as False positive rate, detection rate, delay metric energy level and hit rate.

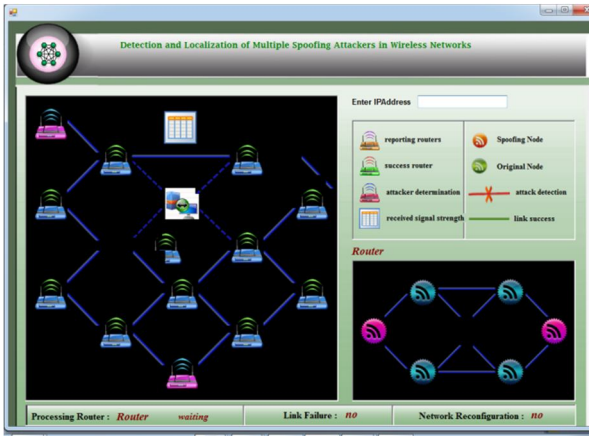

Figure 2. Detection of Multi Spoofing Attack

- ✓ In this form we will receive a new folder with message by creating a folder in the before form.
- ✓ The same message will be displayed on the new folder in this form.
- ✓ After receiving the folder with messages the status will be displayed as file received. (refer figure 3)

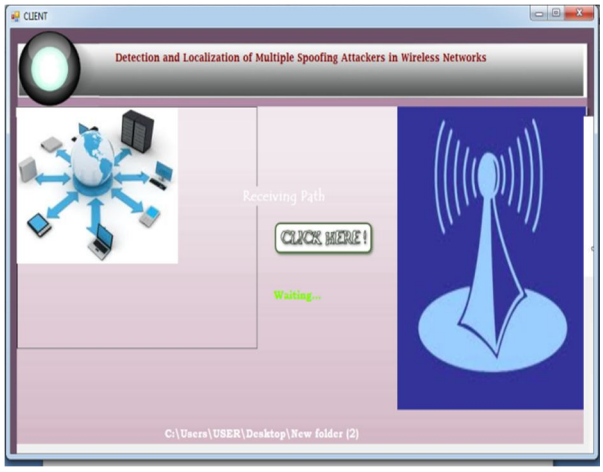

Figure 3: Receiving signal and path

IV. Issues in Spoofing Attack Detection

Based on the identified spoofing attack three major issues are listed below Detect the presence of spoofing attacks,

1. Determine the number of attackers,
2. Localize multiple adversaries and eliminate them.
3. Localization of Attackers

V. Conclusion

The proposed approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it can localize any number of attackers and eliminate them. Determining the number of adversaries is particularly challenging problem. This 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. Further, based on the number of attackers determined by the 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 wireless spoofing attacks, determining the number of attackers and localizing adversaries.

VI. 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 signal prints," 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. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.
6. 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.