ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

# Multiple Spoofing Attackers Detection and Localization in Wireless Networks

R.Tamilarasi (Assistant professor, CSE Department, MVJCE, Bangalore)
Jaharlal Sarkar (PG- Student, CSE Department, MVJCE, Bangalore)

***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.***

***Index Terms*—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.

## II. SCOPE OF THE PAPER

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.

## III. EXISTING SYSTEM

In the existing system cryptographic scheme is used for node identification, as number of nodes increase in an wireless network it is very difficult to provide security to each and every nodes because it require reliable key distribution, management, and maintenance mechanism. It is not always desirable to apply these cryptographic methods [1], [2] because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

most wireless nodes are easily accessible, allowing their memory to be easily scanned. In a wireless network such as 802.11 networks attacker can easily attack to gather useful MAC address information during passive monitoring and then modifying its MAC address by simply issuing an*" ifconfig "*command to masquerade as another device. In spite of existing 802.11 security such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or 802.11i (WPA2) security. This type of security can only protect data frames but identity of the node cannot be protected. Various spoofing attacks such as attack [1], [2] on access control list, rogue access point (AP) attack and Denial of-Services (Dos) attack affect wireless network performance and security and in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly.

## IV. PROPOSED SYSTEM

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.

### *A.* ARCHITECTURE

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.

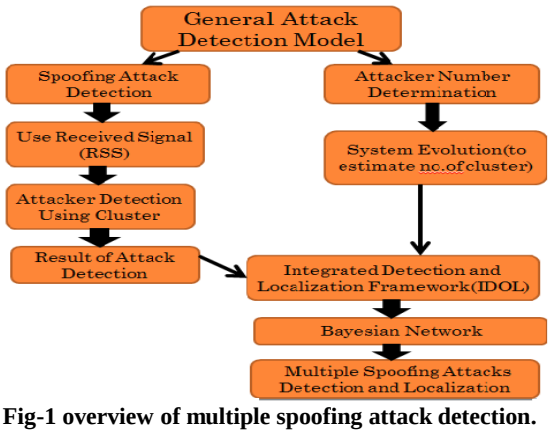


**Fig-1 overview of multiple spoofing attack detection.**

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.

## V. ATTACKERS IN EXISTING SYSTEM

### *A. Resource Depletion Attacks*

This is essentially a DoS attack. The attacker floods the network with unnecessary requests, thereby consuming large amount of network bandwidth, computational power and memory.[8] The attacker goes one step ahead and attempts to mask its identity by spoofing its IP or MAC address. Therefore, security mechanisms based on IP or MAC addresses will fail to identify the DoS attack. However, as signal prints are hard to spoof, a mechanism based on signal prints can detect such an attack.

### *B. Masquerade Attacks*

In a masquerade attack, the attacker poses as a valid member node. Most techniques involve spoofing IP or MAC address, so as to acquire the privileges of another valid member node.[3] This allows the attacker to enter and access a network to which he is not authorized. Identity-based security mechanisms that use IP or MAC address – or any information that the sender sends as a part of data – cannot detect such security violations. However, owing to the properties of signal prints (described in Section III) it is very difficult for the attacker to defeat a security mechanism based on signal prints.

## VI. SURVEY ON EXISTING SYSTEM

The following chapter routes us on the theoretical background that is required in studying the different ways in which the current problem has been deal with in the past. It goes on to give a brief outline of the various protocols that have been used in the existing system, the architectures that are used. Finally deals with ideas which are most related to the proposed project.

### *1. Detecting Identity-Based Attacks in Wireless Networks Using Signal prints.*

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.[3] 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.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

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.

***2. 802.11 Denial-of-Service Attacks: 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[4].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.

***3. Detecting Spoofing Attacks in Mobile Wireless Environments:***

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.[5] 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. Further, 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

## VII. GENERALIZED ATTACK DETECTION MODEL (GADE)

In this section, we describe our Generalized Attack Detection Model, which consists of two phases: attack detection, which detects the presence of an attack, and number determination, which determines the number of adversaries.

### *A. Received Signal Strength (RSS):*

RSS is the power of the signal at the receiver. During propagation of the signal from the sender to receiver, multiple environmental phenomena modify the transmitted signal strength. For example, in a closed room a transmitted signal will be reflected off the walls. This reflected signal can then interfere with the original signal constructively or destructively resulting in modified signal intensity. Similarly an obstacle in the path may create a shadow region of low signal power on the side of the obstacle away from the sender. Transmitted signals also suffer from absorption and attenuation which further reduce signal strength. The combined effect of all this is that the RSS values reduce exponentially with distance. In fact, as we move away from the sender, the RSS values drop rapidly initially. However, after some distance, the signal to noise ratio decreases to the sensitivity of the receiver and, hence, the RSSI values appear fairly constant to the sender. Therefore, the RSS values are highly dependent on environment phenomena. This dependence of RSS values on the environmental phenomena makes it extremely difficult for the intruder to spoof RSS values.

### *B. Attack Detection Using Cluster Analysis:*

Cluster analysis is to be done after getting the signal strength from the nodes. RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection.[6] But the RSS readings from a wireless node may fluctuate and should cluster together. In particular, the RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. Under 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 (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

## VIII. RESULT OF ATTACK DETECTION

### *A. Impact of Threshold:*

The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a threshold t enables the attack detector to be robust to false detections.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

Figures show the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. We observed that the curve of Dm shifted greatly to the right under spoofing attacks. Thus, when Dm > t, we can declare the presence of a spoofing attack.

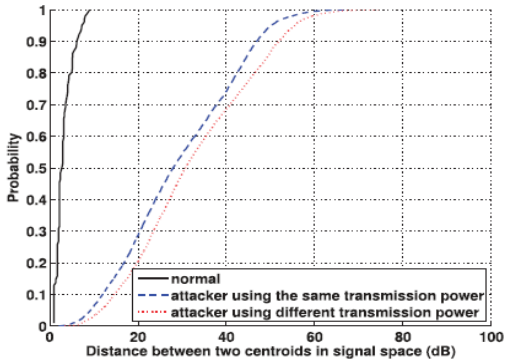


**Fig-2: Different transmission power. [7]**

### *B. Impact of Distance between the Spoofing Node and the original node:*

We further study how likely a spoofing device can be detected by our attack detector when it is at various distances from the original node in physical space.[7] We found that the further away Pspoof is from Porg, the higher the detection rate becomes. In particular, for the 802.11 network, the detection rate goes to over 90 percent when Pspoof is about 15 feet away from Porg. While for the802.15.4 network, the detection rate is above 90 percent when the distance between Pspoof and Porg is about 20 feet.

## IX. SYSTEM EVOLUTION

The System Evolution is a new method to analyse cluster structures and estimate the number of clusters [6]. The System Evolution method uses the twin-cluster model, which are the two closest clusters (e.g., clusters a and b) among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy Ep(K) denotes the border distance between the twin clusters, whereas the Merging Energy Em(K) is calculated as the average distance between elements in the border region of the twin clusters. The basic idea behind using the System Evolution method to determine the number of attackers is that all the rest of clusters are separated if the twin clusters are separable

## X. INTEGRATED DETECTION AND LOCALIZATION FRAMEWORK (IDOL)

In IDOL, we present our integrated system that can detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

### *A. RADAR-gridded:*

The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR returns the x, y of the nearest neighbour in the signal map to the one to localize, where "nearest" is defined as the euclidean distance of RSS points in an N-dimensional signal space, where N is the number of landmarks.

### *B. Area-based probability:*

ABP also utilizes an interpolated signal map. Further, the experimental area is divided into a regular grid of equal-sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector s.

### *C. Bayesian networks:*

BN localization is a multi lateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. The vertices X and Y represent location; the vertex si is the RSS reading from the ith landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of si follows a signal propagation model $s_i = b_{0i}+b_{1i}\log D_i$, where $b_{0i}$, $b_{1i}$ are the parameters specific to the ith landmark.

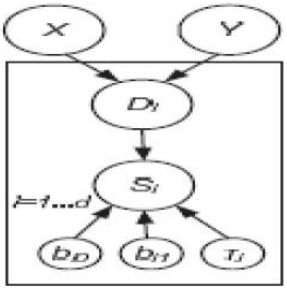


**Fig 3: Bayesian graphical models. [7]**

in our study The distance $D_i=\sqrt{(X-x_i)^2+(Y-y_i)^2}$ in turn depends on the location (X, Y ) of the measured signal and the coordinates ($x_i$, $y_i$) of the ith landmark.

## XI. 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 both 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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

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] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[2] 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.

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

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

[5] 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.

[6] K. Wang, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China, 2007.

[7] 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.

[8] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

## AUTHOR'S PROFILE

**R.Tamilarasi** is a Computer Science Engineer, presently working as an Assistant Professor in the department of Computer Science & Engineering of MVJ College of Engineering, Bangalore. She pursued her MTECH from PEC, Anna University, and B.E., from MEC Anna University.

**Jaharlal Sarkar** completed B.E (CSE) from Sathyabam University, Chennai, Tamilnadu in 2012 and pursuing M.Tech (CSE) in MVJ College of Engineering Bangalore, Karnataka. His main research interests include Network Security, Networking and Mobile Computing.