Novel Promising Algorithm to suppress Spoof Attack by Cryptography Firewall2014

Prof Hadadi Sudheendra
BE.,M.Tech.Ph.D
Bangalore, Karnataka, India

Dr. N Krishnamurthy B.E.,ME(IISc.,) India,
Ph.D (St Maris College, London ,UK)
Bangalore, Karnataka, India

ABSTRACT

Spoof attack suppression by the biometric information incorporation is the new and modern method of avoid and as well suppression the attack online as well off line. Wireless networks provide various advantages in real world. This can help businesses to increase their productivity, lower cost and effectiveness, increase scalability and improve relationship with business partners and attract customers. In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in face and voice recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities, such as fingerprint, face, or iris, to more marginal ones, such as signature or hand. Fingerprints cannot lie, but liars can make fingerprints". Unfortunately, this paraphrase of an old quote attributed to Mark Twain1 has been proven right in many occasions now. And not only for fingerprints, but also for many other biometric traits such as face, iris, voice or even gait. Every technology has its own time. Since the first pioneering works on automatic voice and face recognition over 40 years ago [1]–[2][3], steady and continuous progress has been made in the development of biometric technology. Driven by the very appealing new security biometric paradigm "forget about cards and passwords, you are your own key", researchers from many different fields such as image processing, computer vision or pattern recognition, have applied the newest techniques in each of these areas to improve the performance of biometric systems [4]. This path of technological evolution has permitted the use of biometrics in many

diverse activities such as forensics, border and access control, surveillance or on-line commerce.

This approach of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to spoofing. Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of antispoofing, with special attention to the mature and largely deployed face modality. The work covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the future of this very active field of research.

Communication in wireless network is critical and challenging issue. Wireless spoofing attacks are occurs easily and reduce the networks performance. Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. The flexibility and openness of wireless networks enables

an adversary to masquerade as other devices easily. The traditional approach to detect spoofing attacks is to apply cryptographic authentication. Here using spatial information, a physical property of each node, so hard to falsify and not depend on cryptographic security, on the beginning for (1)detecting spoofing attacks; (2) determining the number of attackers when multiple node pretend as a same node identity, (3) localizing multiple adversaries.

Here using the correlation between a signal's spatial direction and the average received signal gain of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. 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. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, also that can localize any number of attackers and eliminate them.

Keywords: *Spoofing Attack, Attack Detection, Localization, Attack suppression.*

INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless network provide an inexpensive and easy way to share a single Internet connection among several computers. The bases of wireless systems are radio waves, an implementation that takes place at the physical level of network structure. Wireless network are easy to add station as there are no cable required. There is less need for technical support signal can be sent through door and wall so station is mobile. Wireless networks are internet backbone for providing services to both mobile and stationary user. Spoofing in IT world refers tricking or deceiving computer users. When any person or program masquerades as another by falsifying data, gaining the advantage, in network security is called spoofing. Types of spoofing attacks includes IP spoofing, E-Mail spoofing, Web Spoofing.

Adversaries are a malicious entity whose aim is to prevent user from achieving their goal. Due to the openness of the wireless transmission medium, adversaries are able to monitor any transmission. 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. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. During passive monitoring it is easy to get MAC address for the attackers and modify its MAC address by using if config command to masquerade as another device. The traditional approach to detect spoofing attacks is to apply cryptographic authentication. Cryptographic authentication of devices introduces key management overheads that may not be practical for several commodity wireless networks.

Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Therefore it is important to 1. Detect presence of the spoofing attacks. 2. Determine the number of attackers. 3. Localizing multiple adversaries .4. Eliminate them. In practice, the channels between different antennas are often correlated and therefore the potential multi antenna gains may not always be obtainable. This is called spatial correlation as it can be interpreted as a correlation between a signal's spatial direction and the average received signal gain. To detect the attacks received signal strength (RSS) based special correlation which is physical property related to each wireless node will use. Here received signal strength (RSS) use to distinguish wireless devices for spoofing detection

The main contributions of our work are: 1) GADE: 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 2) IDOL: an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

RELAWireless Local Area Network (WLAN) is widely used today because of its mobility and ease of deployment. Providing complete security to the WLAN users is a challenge due to the open nature and undefined boundaries of the wireless networks. This paper is intended to protect the 802.11 WLAN

environments from Medium Access Control (MAC) layer Denial of Service (DoS) attacks especially, the deauthentication and disassociation attacks. This paper proposes an algorithm to detect and prevent deauthentication/ disassociation DoS attacks. These attacks are launched due to the vulnerability of the management frames which carries the MAC address of the client or Access Points (AP) that are not encrypted. So, there is an urgent requirement for a security mechanism to prevent MAC layer DoS attacks which does not require any change in the hardware or protocols. In this paper, an algorithm is proposed to detect and prevent MAC spoofing DoS attacks with an exchange of passkey values. The proposed algorithm, MAC Spoof Detection and Prevention (MAC SDP DoS) is compared with the existing algorithm which is used for MAC spoof detection. This algorithm is validated by NS2, a network simulator tool. The proposed algorithm improves the performance of WLAN by increasing the throughput and reduces the packet resend rates to a greater extend. The recovery time has also been reduced compared with the existing method.

The traditional approach to prevent spoofing attacks is the use cryptographic-based authentication. Mathias Bohge et al. proposed a framework, called TESLA certificate, for the scalability problems in hierarchical ad hoc sensor networks [3].Wu et al. (2005) presented a secure and efficient key management (SEKM) framework. In this the data communication is done between the client and server.
They have introduced a secure and efficient key management (SEKM) framework [4]. A wool et al. presented Wired Equivalent Privacy (WEP), which provides key management with host revocation to existing IEEE 802.11 wireless LAN networks [5].
New approach is using physical property which is associated with wireless transmission. The MAC sequence number has also been used in [6] to perform spoofing detection. Liand Trappe [7] introduced a security layer that used forge resistant relationships

based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks. V. Brik et al. (2008) invented the concept of PARADIS server which is able to find the frequency error, I/ Q offset, SYNC correlation, phase error and magnitude error. In this the concept of fingerprinting is evolved into the PARADIS server [10]. RSS is the property closely correlated with location in physical space and is available in the exiting wireless network.
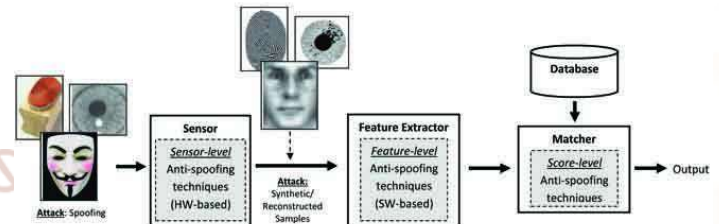
Block diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated (sensor-level, feature-level and score

PROPOSED SYSTEM
Network contains in different clusters. Each cluster contains different nodes. Our aim is to detect the spoofing attack from particular node which belongs to any cluster. Energy optimizer is used to calculate the energy of particular node to detect the spoofing attack. Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorrelates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations. When user sends the file to server then server will detect the attack & identify from which location it is by detection and localization of spoofing attack by Energy optimizer and the weight of the node
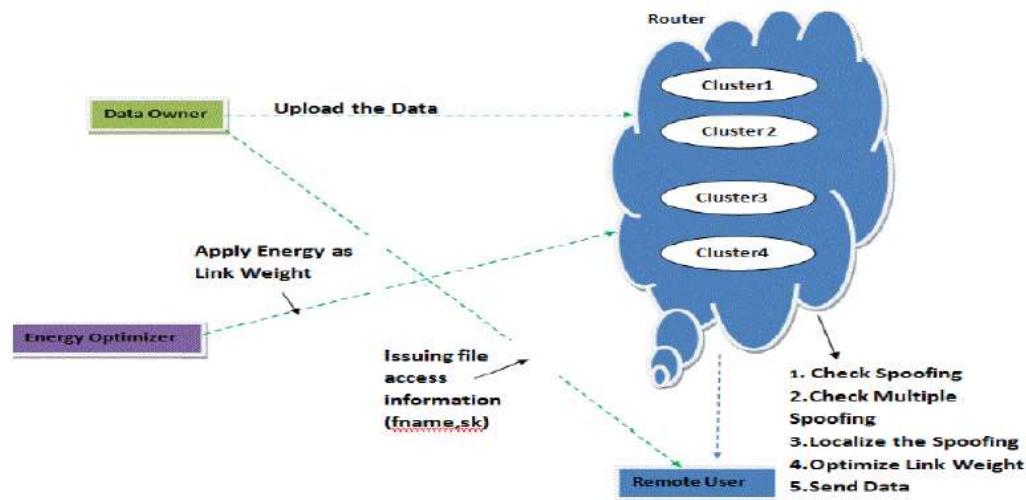
Fig 3.1 : System Architecture

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. The System Evolution is a new method to analyse cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is calculated as the average distance between elements in the border region of the twin clusters.

IP source address spoofing has plagued the Internet for many years. Attackers spoof source addresses to mount attacks and redirect blame. Researchers have proposed many mechanisms to defend against spoofing, with varying levels of success. With the defense mechanisms available today, where do we stand? How do the various defense mechanisms compare? This article first looks into the current state of IP spoofing, then thoroughly surveys the current state of IP spoofing defense. It evaluates data from the Spoofer Project, and describes and analyzes host-based defense methods, router-based defense methods, and their combinations. It further analyzes what obstacles stand in the way of deploying those modern solutions and what areas require further research.

The Face recognition is an unique efficient method of avoid spoof attack which is widely used biometric approach. Face recognition technology has developed rapidly in recent years and it is more direct, user friendly and convenient compared to other methods. But face recognition systems are vulnerable to spoof attacks made by non-real faces. It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. A secure system needs Liveness detection in order to guard against such spoofing. In this work, face liveness detection approaches are categorized based on the various types techniques used for liveness detection. This categorization helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of the latest works regarding face liveness detection works is presented. The main aim is to provide a simple path for the future development of novel and more secured face liveness detection approach.

Y. Sheng et al. [11] describes that MAC spoofing attacks in 802.11 networks. They propose to use Gaussian Mixture Modeling (GMM) for RSS profiling, and show how to use it to detect spoofing attacks.The GMM is the mixture local statistics of a single AM, combining local results from AMs, and global multi-AM detection, respectively.

Sang et al. [12] proposed to use the node's "spatial signature, "including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. However, none of these approaches are capable of determining the number of attackers and they do not have the ability to localize the positions of the adversaries after attack detection.

Chen et al. [8] created a system that both detects spoofing attacks and localizes the attacker. Yang et al. [9] proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. Choosing a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy.

J.Yang et al., [13] proposed a technique DEtecting Mobile Spoofing aTtacks in wireless Environments (DEMOTE). They 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

In 2009 Gyathri Chandrasekaran et al. [14], proposed architecture to robustly detect identity spoofing attacks under varying operating conditions. In 2010, Jeong Heon Lee et al. [15] address issues associated with location spoofing attack detection by examining relative location error rather than its absolute value.

Liang Xiao et al.,[16] proposed a PHY-authentication protocol to detect spoofing attacks in wireless networks, exploiting the rapid-decorrelation property of radio channels with distance

F.A. Barbhuiya et al. [17] presented an IDS to detect ARP spoofing attacks using active state-transition framework called "active DES". Ali Broumandan et al. [18] proposed a spoofing detection method based on a single moving antenna. Test measurements have been performed by combining authentic signals received from a rooftop antenna with spoofing signals radiated from an indoor directional antenna and received by a spatially translated single antenna

Jie Yang et al. [19] 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.

Our work differs from the previous study in that we use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, our work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations. The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology and it is more direct, user friendly and convenient compared to other methods. Therefore, it has been applied to various security systems. But, in general, face recognition algorithms are not able to differentiate 'live' face from 'not live' face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. In order to guard against such spoofing, a secure system needs liveness detection.

III PROPOSED SYSTEM

Network contains in different clusters. Each cluster contains different nodes. Our aim is to detect the spoofing attack from particular node which belongs to any cluster. Energy optimizer is used to calculate the energy of particular node to detect the spoofing attack. Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorrelates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations. When user sends the file to server then server will detect the attack & identify from which location it is by detection and localization of spoofing attack by Energy optimizer and the weight of the 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. The System Evolution is a new method to analyse cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is

calculated as the average distance between elements in the border region of the twin clusters.

Generalized Attack Detection Model : In public key cryptography the security of private keys is vital importance. If private key is ever compromised can be used t0 sign forge documents decrypt secret messages. Conventional methods such as password-based encryption that are used for safe custody of private keys do not provide adequate security due to very low entropy ?n user chosen passwords. In order to enhance the security of private keys we propose ? novel biometric-based method that dynamically regenerates the private key of the user rather than storing ?t directly ?n ?n encrypted form. Our proposed algorithm is capable of regenerating key lengths that can meet the current security requirements? f any public key algorithm and is more secure than conventional methods ?f protecting private keys using password-based encryption.

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.

Cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker.

3.2 Localization of Attackers:
Identify the positions of multiple adversaries even when the adversaries vary their transmission power levels. The main contribution is as follows

➤ To effectively detect the presence of spoofing attack

➤ To count the number of attackers

➤ To identify the location of multiple adversaries in the network

➤ To provide solution to identify adversaries in the network where in there is no additional cost or modification to the wireless devices themselves

➤ To avoid authentication key management

➤ To avoid overhead

3.3 Attack Detection Using Cluster Analysis:
The RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that 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.

For RSS reading vectors of three landmarks (i.e., n = 3) from two different physical locations. 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).

Advantages:
➤ 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.

➤ The Hit Rate is lower when treating four attackers as errors than treating two attackers as errors. This indicates that the probability of misclassifying three attackers as four attackers is higher than that of misclassifying three attackers as two attackers.
➤ The proposed system validates the effectiveness, efficiency, and robustness of the scheme through analysis.

➤ The System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters.

Fig. 3.2 presents an example of using the System Evolution method to determine the number of attackers in the 802.11 network. It shows the energy calculation versus the number of clusters. The Koptimal is obtained when K = 4 with Ep(4) > Em(4) and Ep(5) < Em(5) indicating that there are four adversaries in the network using the same identity to perform spoofing attacks.

Determining The Number Of Attackers
Number of Attacker Determination:
A Silhouette Plot is a graphical representation of a cluster. To determine the number of attackers, we

---

construct Silhouettes in the following way: the RSS sample points S= {s1,...,sN}(with N as the total number of samples) are the data set and we let C=(c1,...,cK)be its clustering into K clusters, as shown in Fig. 8. Let d(sk,sl)be the distance between skand sl. Let cj=(sj1,...,sjmj)be the jth cluster, j =1,...,K , where mj=|cj|.

image

4.2 Support Vector Machine Based Mechanism

Several statistic methods available to detect the number of attackers, such as System Evolution and SILENCE, we can combine the characteristics of these methods to achieve a higher detection rate. Using Support Vector Machines to classify the number of the spoofing attackers. The advantage of using SVM is that it can combine the intermediate results (i.e., features) from different statistic methods to build a model based on training data to accurately predict the number of attackers.

4.2.1 Experimental Evaluation

Table 1, shows experimental results of using SVM-based mechanism when the attacker number i ={2,3,4} for the 802.11.Here observation is that when the number of attackers equals to 2, the SVM-based method achieves the highest Hit Rate (above 99 percent) and the highest F-measure value, over 98 percent. In the case of four attackers achieves the highest Precision, above 99 percent, which indicates that the detection of the number of attackers is highly accurate, the Hit Rate decreases to about 90 percent.

image

By comparing the results of SVM to those of Silhouette Plot, System Evolution and SILENCE methods, here observation is that there is a significant increase of Hit Rate, Precision and F measure for all the cases of the number of attackers under study. These results demonstrate that SVM-based mechanism, a classification approach that combines training data and different statistic features is more effective in performing multiclass attacker detection when multiple attackers are present in the system.

4.3 Idol: Integrated Detection And localization Framework

IDOL: an Integrate Detection and Localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

CONCLUSION

This project proposed to use received signal strength mechanism and implement the clustering, SVM to identify the attack, 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, also that can localize any number of attackers and eliminate them.

References

1. P. Bahl and V. N. Padmanabhan, "RADAR: An in- Building RF- Based User Location and Tracking System," Proc. IEEE INFOCOM, vol. 2, Page(s): 775 – 784, 2000

2. Modern Promising Algorithm to avoid Spoof Attack by Cryptography: - **Murthy, K. N. B.; Sudheendra, H**. PUB. DATE August 2008 SOURCE Proceedings of World Academy of Science: Engineering & Technolog; Aug2008, Vol. 44, p690.

3. Daniel B. Faria and David R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," In Proceedings of the First ACM Workshop on Wireless Security (WiSe'02), September 2002

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

5. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile AdHoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (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.

7. 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.

8. Xiao L and Trappe W, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proceedings of IEEE International Conference on Communications (ICC), pp. 4646-4651, 2007

9. Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in SECON'07: Proceedings of the 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.

10. Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

11. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008

12. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength, "Proc. IEEE INFOCOM, Apr. 2008.

13. Lifeng Sang and Anish Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," proc. IEEE INFOCOM, page 2137-2145, 2008.

14. 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.

15. Gayathri Chandrasekaran, John-Austen Francisco, Vinod Ganapathy, Marco Gruteser and Wade Trappe, "Detecting Identity Spoofs in IEEE 802.11e Wireless Networks," proc. IEEE GLOBECOM, 2009.

16. Jeong Heon Lee and R. Michael Buehrer, "Location Spoofing Attack Detection in Wireless Networks," proc. IEEE GLOBECOM,2010

17. Liang Xiao, Alex Reznik, Wade Trappe, Chunxuan Ye, Yogendra Shah, Larry Greenstein and Narayan Mandayam, "PHY Authentication Protocol for Spoofing Detection in Wireless Networks," proc. IEEE Global Telecommunications Conference (GLOBECOM), 2010.

18. F. A. Barbhuiya, S Biswas and S Nandi, "An Active DES based IDS for ARP Spoofing," IEEE International Conference on Systems, Man, and Cybernetics (ICSMC), Page(s): 2743 – 2748, 9 Oct 2011.

19. Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen and Gérard Lachapelle, "GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation," IEEE/ION PLANS April 24-26, 2012

20. Jie Yang, Yingying Chen and Wade Trappe, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transaction on parallel and distributed system, Vol. 24, NO. 1, January 2013