IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

TRACKING AND PREVENTING THE MULTIPLE SPOOFING ATTACKS IN WIRELESS NETWORKS

Dharmaji V. Manjrekar, Nita K. Dongare, Radhika R. Chavan
[*] Computer Department, Jaihind College of Engineering, India

ABSTRACT

Wireless Networks are more vulnerable to spoofing attacks which can be launched easily and considered as one of the most challenging, but these attacks have huge impact on the network performance. In this paper, we aim to propose a theory based on a physical property that cannot be altered, and does not depend on any of cryptographic approach, as medium for 1) Detection of spoofing attacks occurred in the network, 2) Determining the number of attackers present in the network 3) Localizing all adversaries and elimination them from the network and 4) Preventing these attackers from rejoining the network. We intend to use the spatial correlation of RSS readings that are acquired from wireless nodes to track down the attacker. Further, Cluster based mechanisms can be helpful in calculating the number of adversaries in the network. Distance-based Detection and Localization (DDL) will assist to accurately locate the attackers in the network while MAC address allocation scheme using MD5 hashing technique is applied to prevent the attacks. Hence, we can recover the network performance with high accuracy rate.

KEYWORDS: Wireless Spoofing Attacks, MAC address allocation, MD5 Hashing Technique, EPAM approach, Cluster-based Mechanisms.

INTRODUCTION

Wireless Networks that are based on IEEE 802.11, are used as a medium of transmitting data between two communicating nodes by means of radio waves in air. During the rise and advancement of mobile technology, the wireless networks were introduced to the world that created a revolution in technology and soon these network started to play a significant role for business organizations, native use and several enterprises. The main reason behind this was the appropriate release of IEEE 802.11 standard, smooth and simple installation, uplifted data rate and cheap wireless devices.

Due to increase in use of wireless networks in recent days, the risk of malicious attacks on the networks are also increased because in wireless networks, the transmission of data packets between two communication nodes continues as long as the network is establish. Thus, during sending and receiving of classified data packets, there is need of more guaranteed medium. The security flaws present in wireless medium grant an adversary to seize control of any system different platforms for launching numerous types of attacks. Identity-based spoofing attacks can be launched easily but also are considered to be one of the most challenging attacks. These attacks allows an adversary to gain illegal access in the network acting as a trusted user which has its huge impact on network performance.

Spoofing Attacks can further assist the progress of variation of traffic implanting attacks, such as rogue access points (AP), denial-of-Service (DOS) attacks, etc. Furthermore, in a massive network, numerous adversaries may costumize itself as trusted node identity and cooperate to launch vulnerable attacks like DOS attacks quickly with the use of cheap wireless devices and frequently available devices. Most of current approaches aim to address probable spoofing attacks operating cryptographic strategies, but their application requires dependable key distribution, management and maintenance techniques. These approaches are not always beneficial because of its excess requirements in framework, computation and management. Further, cryptographic methods are vulnerable to in compromisation of nodes. Hence, it is significant to 1) Recognize the existence of spoofing attacks in network; 2) Figure out and verify the number of attackers; 3) localize all adversaries and eradicate them from the network and 4) Avoid the attacks by allotting MAC address using MD5 hashing approach.

Thus, in this paper, we aim to propose a spatial correlation termed as Received Signal Strength (RSS), a physical attribute that cannot be faked which is linked with all wireless nodes and is not reliant on cryptography as medium for identifying spoofing attacks. Since, we are interested with adversaries with variable locations than authorized wireless nodes, using spatial information to intimate spoofing attacks has a unique power for not only detecting these attacks but also localizing the attackers and eliminate them. A major advantage of utilizing spatial correlation to identify spoofing attacks is that it does not depends on any additional expense or alteration to wireless devices.

The main benefaction of our work are: 1) GADE (Generalized Attack Detection Model) that can be used for identifying these attacks as well as to determine multiple adversaries present in the network using cluster-based mechanisms based on RSS among the wireless devices and attackers; 2) DDL (Distance-based Detection and Localization) algorithm for exact localizing the adversaries; and 3) Allotting MAC address via MD5 hashing approach to prevent the attack.

The remaining paper is systematized as follows. Section II consist of related work. Section III justifies the architecture of proposed work. Section IV gives brief explanations about algorithms used in paper. Section VI finalizes as conclusion and guidance for future work.

RELATED WORK

The conventional techniques to anticipate spoofing attack is to use cryptographic-based authentication [5], [6], [10]. Wu et al. [5] proposed the theory of Secured and Efficient Key Management (SEKM) framework that builds a Public Key Infrastructure (PKI) by assigning a cryptic sharing scheme and crucial multicast server group. Wool [6] introduced a key management approach with periodic key refresh and host revocation to anticipate the composition of authentication keys. However, the cryptographic authentication may not be always desirable due to the finite resources on wireless devices, and flaws of a fixed key management infrastructure in the wireless transmission medium.

Recently, new techniques using physical properties linked with wireless transmission medium to battle attacks in wireless networks have been proposed. Based on the fact that wireless transmission medium acknowledgement is not associated quickly in space, a channel-based authentication scheme was introduced to distinguish between transmitters at different locations, and thus to detect spoofing attacks in wireless networks [11]. Brik et al. [12] intended on building fingerprints of 802.11b WLAN NICs by gathering radiometric signatures, like frequency magnitude, phase errors, and I/Q origin offset, to protect against identification attacks. However, there is added overhead linked with wireless medium response and radiometric signature eradication in wireless networks. Li and Trappe [4] introduced a security layer that used duplicate resistant relationships based on the packet traffic, including MAC address sequence number and traffic pattern, to detect spoofing attacks. The MAC sequence number has also been used in [13] to implement spoofing detection. Both the sequence number and the traffic pattern is manipulated by an attacker as long as it learns the traffic pattern under normal situations. The works [3], [7], [14] using RSS to protect against spoofing attacks are most likely related to us. Faria and Cheriton [3] imtroduced the use of comparing rules of signal prints for spoofing detection.

In this work, we select a group of algorithms using RSS to execute the task of localizing multiple adversaries and determine their performance in terms of localization accuracy. Our work differentiate from the previous study in that we use the spatial information to collaborate in attack detection instead of depending on cryptographic-based techniques. Moreover, our work is novel due to none of the existing work can figure out the number of adversaries when there are multiple attackers masquerading as the same node identity. In Addition, our technique can accurately localize all adversaries in network even when they vary their transmission power levels to deceive the system of their actual locations.

SYSTEM ARCHITECTURE

The system design of the proposed system is shown in figure 1. This architectural design consist of various components like traffic monitoring and analysis, mediod based cluster mechanism, multiclass formation and Dynamic MAC allocation with MD5 authentication.

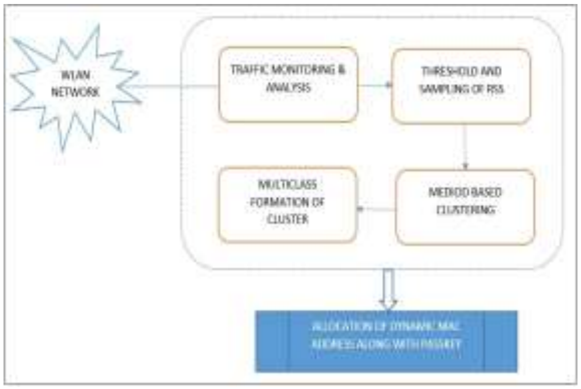

WLAN NETWORK
TRAFFIC MONITORING & ANALYSIS
THRESHOLD AND SAMPLING OF RSS
MEDIOD BASED CLUSTERING
MULTICLASS FORMATION OF CLUSTER
ALLOCATION OF DYNAMIC MAC ADDRESS ALONG WITH PASSKEY

Figure 1 – System Architecture

Depending on a node's identity, the network traffic was monitored and RSS (Received Signal Strength) is analyzed for identifying spoofing attack. Mediod based clustering mechanism is used for identifying multiple adversaries in the network. Because of limitations in PAM (Partitioning Around Mediod), a clustering technique is adopted, a cluster based mechanism is adopted maximizing criteria for average silhouette plot. Depending on traffic monitoring and analysis, a threshold has been set for identifying the occurrences of attacks in wireless networks. A multicast formation of cluster is used for identifying multiple adversaries present in the wireless mediums.

GADE Model

The Generalized Attack Detection Model consist of the phase. In first phase, the spoofing attack in the network is identified whereas in the second phase, the total number of adversaries in the network are determined.

1. Identifying Attacks

The main challenge of in identifying the spoofing attack in wireless network is to implement the strategies that can use the unique behavior of this spatial correlation, as replacement of the location as the attacker's position is unknown at start because the attackers masquerade the victim node identity due to which there is a chance that the authorized user may also get eliminated.

Thus, we have used RSS (Received Signal Strength), a non-falsified property which is closely linked with the transmitter's physical location in the network space. Also, it can be easily available in any wireless mediums. The RSS readings will differentiate based on the locations i.e. it will be same for similar locations but may distinguish as the location of physical node changes.

2. EPAM Algorithm

After analyzing the RSS-based spatial correlation which is derived from wireless node theoretically as a medium to detect the identity-based spoofing attack, we came to a conclusion that the RSS reading over same physical space should belong to same cluster points whereas, the readings from different locations should be included in different clusters in n-dimensional signal space. While performing a spoofing attack, the victim or the authorized user and the adversary in the network make use of same identity to transmit data packet, and the RSS reading of that identity will be the mixture of readings measured from the spoofing node and victim node. Since, these readings are mixed together, we make use of Enhanced Partitioning Around Mediod (EPAM) method as traditional k-means clustering approach won't be able to give better accuracy when the resulting clusters are too small. The PAM method is a suitable and iterative decent clustering algorithm whereas EPAM method is concentrated and strong in the present of noise and outliers as it uses Euclidian distance for clustering of node. The aim of this method is minimizing the average contradiction of objects to their closest selected objects. Hence the EPAM method is more appropriate in estimating the clusters RSS of nodes, which can be affected by attacks. This method consists of two phases namely BUILD and SWAP. In the first phase "BUILD ", a collections of k objects are selected for initial set o. and the second phase "SWAP ", one tries to improve the quantity of clustering objects by exchanging selected object with unselected objects.

DDL algorithm

DDL adds the distance information between two nodes as additional parameter to the existing system, to accurately localize adversaries. For this, it uses lat-Iong (latitude-longitude) information about the nodes. The advantage of lat-Iong information is that they are more accurate and represents points in sphere using degree, minutes and seconds. As a result, the position of a node can be exactly found. Hence, DDL achieves accurate localization.

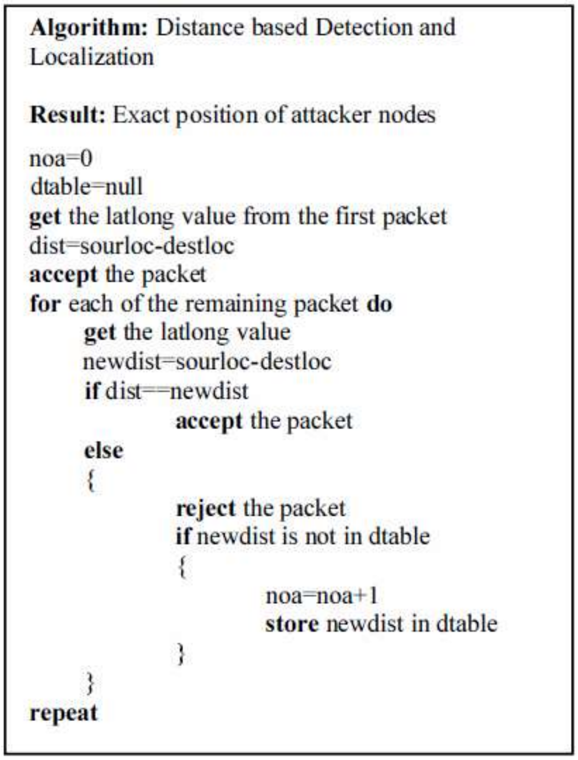
During the lifetime of a network, misbehaving nodes have to be identified and must not be allowed to remain connected to the network. Therefore, we need a detection mechanism. The DDL algorithm will be invoked for each transmission and performs packet-level localization, which means localization is performed for each packet received. The reason for performing packet-level localization is, identity-based spoofing attacks are active attacks. Any number of adversaries can interrupt the transmission at any time and cause damage to network perfonnance. By doing packet-level localization, the DDL algorithm can effectively detect identity-based spoofing attacks and accurately localizes multiple adversaries.

By changing the packet format, our approach uses the position of nodes to calculate the distance between source and destination. Whenever a node is deployed, the current location of that node (in lat-Iong format) will be automatically embedded in its packet.

During transmission the source sends packet to the destination. The destination first checks the MAC address and extracts the lat-Iong value from the source packet. It then computes the distance between source and the destination and accepts the packet. For the next packet, the destination will check the MAC and again compute the distance by extracting the lat-Iong value from it and compare it with the distance already computed for the first packet. If both are same it accepts the current packet. In this way, the destination accepts the remaining packets from the source.

If the distance computed by the destination for the current packet is different but the MAC is same, it ensures that the packet is coming from the attacker, rejects the packet and sends the lat-Iong value to the server for localization process.

In this way, the proposed system detects the presence of spoofmg attacks, accurately localizes multiple adversaries and eliminates them.



```
Algorithm: Distance based Detection and
Localization

Result: Exact position of attacker nodes

noa=0
dtable=null
get the latlong value from the first packet
dist=sourloc-destloc
accept the packet
for each of the remaining packet do
      get the latlong value
      newdist=sourloc-destloc
      if dist==newdist
                accept the packet
      else
      {
                reject the packet
                if newdist is not in dtable
                {
                          noa=noa+1
                          store newdist in dtable
                }
      }
repeat
```

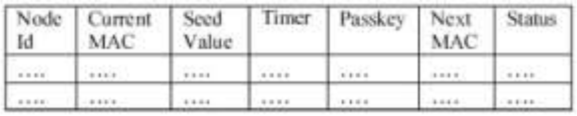
The above pseudo code will determine the distance between the source and destination and between the attacker and destination. If the distances are different, then the system will declare the presence of spoofmg attacks, return the nwnber of attackers and their corresponding locations and eliminates them from the network.

Dynamic MAC Address Allocation

In order to prevent MAC address spoofing attacks, a novel dynamic MAC address allocation technique has been implemented. Each MAC address has been used for one session and periodically updated in the DAM table (refer table I) Node Id refers to the unique identification given to every communicating node. Current MAC field give the MAC address of the node. The seed value field is the concatenation of passkey value and the current MAC value. Timer helps us to update the seed value and proceed to the node having next MAC address. Status gives details about whether it has undergone attack or not.

Whenever a node requests for authentication through their MAC address, it has been check verify from this register table. If the authentication success then MAC address of node would be changed dynamically with the help of DAM table.

Table 1: Dynamic Allocation MAC table



Node Id	Current MAC	Seed Value	Timer	Passkey	Next MAC	Status
.....	.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....	.....

The format of the DAM table as shown table 1 shows the following fields such as Node id, Current MAC address, Seed value, timer for expiry time, Passkey of the node, Next dynamic MAC address and status this node. The table shows the structure of DAM table.

The steps involved in Dynamic MAC allocation as follows.

Steps:

1. Initialize a seed value of each node which is compromised i.e. seed value could be 128 bit long. Seed has been generated through MDS digest code of concatenation of old MAC address and random value which is generated from CryptGenRandom.

2. Derive virtual MAC address from the seed value. The new MAC address is the first 48 bit of seed value which is generated from step I.

3. After generation of new MAC address, the seed value has been changed. The new Seed value would be the MDS digest code of the old seed value.

4. The newly created seed value would be updated in the DAM table for next assignment of MAC address. Go to step 2 until connections lost.

To improve the security of the node, passkey verification scheme has been proposed in this prevention mechanism. Initially the passkey value of each node would be generated and maintained along with MAC address in the DAM table. Whenever a node transmits packets, the passkey value is verified for authentication. The node will allow for transmission only if the passkey of node matched with passkey stored. Otherwise, the node will not be the part of the networks.

RESULTS AND DISCUSSION

This section discuss about the experiments carried out based on the proposed methodology. The analysis of detection and prevention of spoofing attacks in wireless networks is discussed further. The received signal strength of nodes would be gathered from the simulation environment.

Then the EPAM algorithm is evaluated using the same simulation values. Figure 2 shows that packet delivery ratio for normal and EPAM. Threshold values have been set by varies test statics in the simulation and then

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

carried out clustering algorithm to detect attacks. Table 2 show the detection accuracy which shows that the detection rate of spoofing attacks and false positive rates. The detection rate of exiting works has been compared with the proposed work of detection of attacks. Hence it concludes that detection rate has been increased.

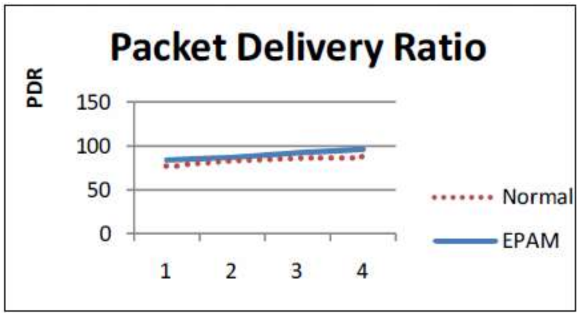
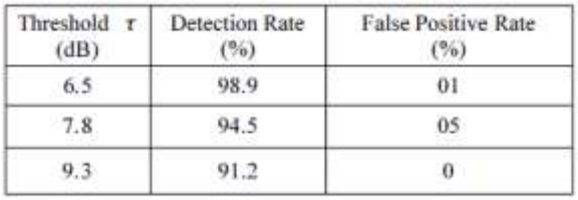


Figure 2 : PDR for EPAM

Table 2: Attacks detection - Detection and False Positive Rate Threshold r Detection Rate False Positive Rate



Threshold τ (dB)	Detection Rate (%)	False Positive Rate (%)
6.5	98.9	01
7.8	94.5	05
9.3	91.2	0

Figure 3 shows that comparison of energy consumption for both normal and attacker node in the simulation. From the graph it shown that energy consumption of adversary would be more compared to legitimate user. Increase in energy level for the adversary is due to their additional attacks. The normal behavior along with their attacks behavior increases the energy dissipation for adversary.

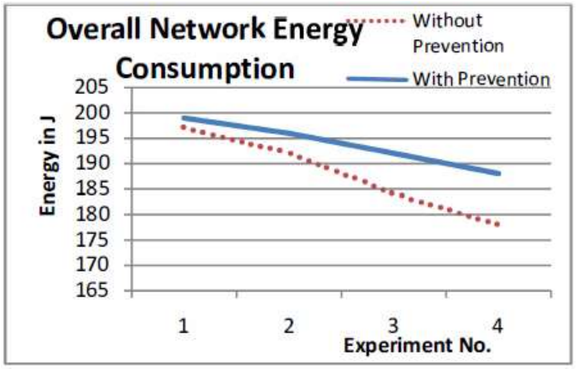


Figure 3: Energy comparison

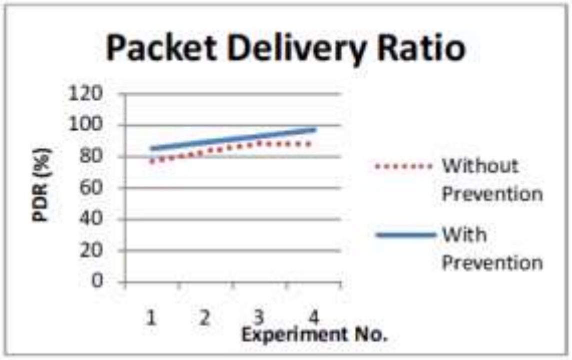


Figure 4: Packet Delivery Ratio for prevention

The overall throughput of the traffic is calculated for both the normal and spoofing behavior. The experiment was conducted for both normal and EPAM traffic and without prevention mechanism and with prevention mechanism. Based on result, shown in Table 3 were the throughputs of the network of both with and without prevention mechanism. The throughputs between normal and EPAM shows in Figure 5.Throughput Analysis

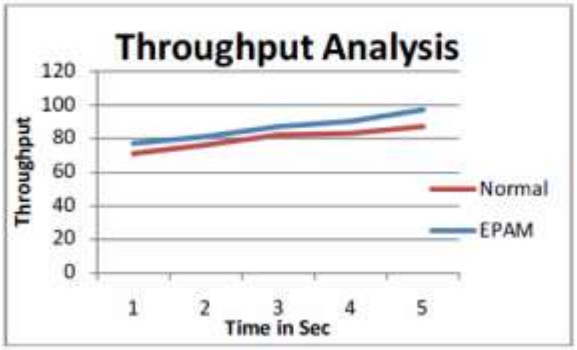
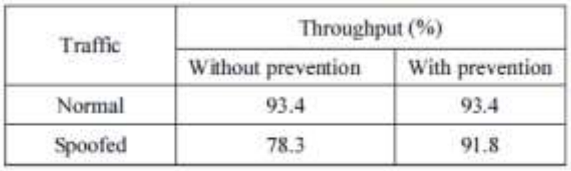


Figure 5: Throughput analysis for EPAM

Table 3: Throughput Analysis



Traffic	Throughput (%)	
	Without prevention	With prevention
Normal	93.4	93.4
Spoofed	78.3	91.8

Traffic throughput at various time intervals are shown in Figure 6. This Figure shows that the throughputs of the network with prevention and without prevention. Accuracy of spoofing attack detection ratio is based on the number of attacker changed dynamically. Accuracy of attacks detection compared and plotted in graph which is shown in Figure 7. From this, concludes that proposed work has more accuracy rate compared to existing work. Through Analysis

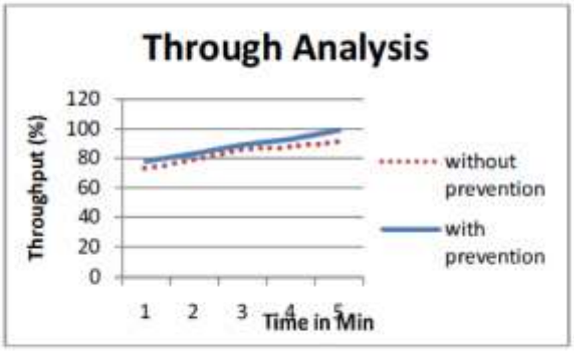


Figure 6: Throughput analysis for prevention

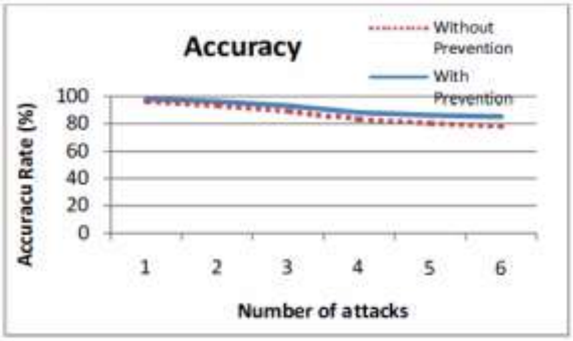


Figure 7: Accuracy of attack detection

CONCLUSION

In this proposed work, EPAM technique is used as mediod based clustering of RSS-based spatial correlation is used for identifying the presence of spoofing attacks in networks. The introduced approach has not only identified the presence of attacks, but also it has determined the number of adversaries in the network, who spoofed an authorized node identity. Further, localizing these attackers and prevent the nodes from the attack can be done. The proposed work has the higher detection rate compared to existing technology. 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.An unique MAC address allocation technique has been implemented for preventing the spoofing attacks in the networks. Change in MAC address is done dynamically with the help of MD5 approach. In Addition, provide high security by authentication of node using Passkey value. Thus the proposed work can identify the multiple spoofing attacks as well as anticipate those multiple spoofing attacks with higher accuracy rate.

ACKNOWLEDGEMENTS

The Author Mr. Dharmaji Vinayak Manjrekar would like to take this opportunity to express gratitude to and deep regards to his fellow co-authors, Miss Nita Dongare and Miss Radhika Chavan for their caluable assistance and help in completion of this article. The Author would further like to thamk his Project Guide Mr. Vaibhav U. Phulwade for his exemplary guidance and suggestions till completion of my work. Working under him was a good and knowledgeable experience for me.

REFERENCES

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

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.

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

[4] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[5] 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.

[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] Jie Yang, Yingying (Jennifer) Chen, Wade Trappe and Jerry Cheng, "Detection and Localization of Multiplr Spoofing Attackers in Wireless Networks" in Proc. IEEE Parallel and Distributed Systems, Vol.24, pp. 44 - 58, January 2013.

[8] Maivizhi. R and Matilda. S, “Distance Based Detection and Localization of Multiple Spoofing Attackers for Wireless Networks”, ICCPEIC 2014.

[9] R. Vijayakumar, K. Selvakumar, K. Kulothungan, A.Kannan, “Prevention of Multiple Spoofing Attacks with Dynamic MAC Address Allocation for Wireless Networks”, ICCSP, April 3-5,2014, India.