International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 6, November – December 2013 ISSN 2278-6856

# A Review on Spoofing Attack Detection in Wireless Adhoc Network

**Mukesh Barapatre[1], Prof. Vikrant Chole[2], Prof. L. Patil[3]**

[1] Department of CSE, GHRAET,RTM Nagpur University,
[2] Department of CSE, GHRAET,RTM Nagpur University,
[3] Department of CSE, PIET,RTM Nagpur University.

**Abstract:** ***Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities. Although the identity of a node can be verified through cryptographic security, conventional security approaches these are not always desirable. we propose to use spatial information, a physical property of each node, so hard to forge or alter fraudulently , and not depend on cryptographic security, on the basis for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple node pretend as a same node identity, and (3) localizing multiple adversaries. We propose to use 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. In this paper enlist the various methods of spoofing attack detection using spatial correlation between wireless nodes. And cluster based mechanisms to determine the number of attakers in network. , we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. We evaluated techniques through two wireless adhoc networks using both an 802.11 (WiFi) network and some other wireless network standard.***

**Keywords:** — Wireless network security, spoofing , attack detection, localization, AP-Access Point.

## 1. INTRODUCTION

Device identity is perhaps one of the most potential challenges in any network security solution. Localizing node is necessary for many higher level network functions such as tracking, monitoring and geometric-based routing and can be used in broad areas . 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 with easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. example, an attacker can masquerade as a legitimate access point to disrupt network connections such as attacks on access control lists, access point attacks, and Denial-of-Service (DoS) attacks, or to advertise false services to nearby wireless stations, Therefore, it is important to

- detect the presence of spoofer in wireless network,
- determine the number of attackers, and
- find location of multiple adversaries and defeat them.

The traditional approach is to use authentication application to address spoofing attacks. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often require significant human management costs on the network. In this paper,[1][2] we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. For that we propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes. By analyzing the RSS from each MAC address using cluster algorithm, we have found that the distance between the access point in signal space is a good test for effective attack detection. We then use adverseries data to locate spoofers ie. Localization system.

In this paper, in section 2 some earlier related work is explained In section 3 the disadvantages of the existing systems are enlisted named as problem definition. In section 4, the objectives are given which may be satisfied in future. Finally in section 5, the conclusion with some future work is given.

## 2. RELETED WORK

There are number of advantages of wireless access networks which are based on 802.11 access in the military and industrial sectors. However, the usage of these access is predicted on the basis of availability and confidentiality assumption. The 802.11 is able to maintain the confidentiality in the data which is to be transferred. The 802.11 is prone to denial-of-service(DoS) attacks at high extent that target to the media access protocols and its management. Jie Yang, Yingying (Jennifer) Chen and Wade Trappe [1] introduce use of spatial correlation of (RSS) received signal strength of wireless nodes to sense the spoofing attacks. Then determining the number of attackers. By Cluster-based mechanisms are used to determine the number of attackers. Training data set are explore using the Support

Vector Machines(SVM) to further improve the accuracy of determining the number of attackers. To localize the attacker they build the an integrated detection and localization system that can localize the positions of multiple attackers.

In the paper of Bellardo and S. Savage[2] have done the experimental analysis and identification of the attacks which are 802.11 specific. In this paper the authors suggested some steps to identify the attacks and same steps to remove that attacks. In this, there is communication between client & AP in which the client is sending the authentication request to the AP. Also the AP is sending the response to client. In next step the client is sending the association request to the AP, and AP is sending the reply to client. After the connection establishment the data exchange is done by client and AP. During this communication some attacker may get access to this communication in such a way that the IP address of attacker appears same as that of the source that is client. But at the time of data sending the de-authentication message is sent to the AP, and then AP again sends that de-authentication message to client also. In this way the attacker can be identified. All these kind of attacks are practical to implement .

In this paper, F. Ferreri, M. Bernaschi, and L. Valcamonici[3] described the number of possible denial-of-service attacks that are carried out on the 802.11 access networks. The attacks are carried out that lead to denial-of-service and the impacts are observed. In this paper also the communication is done between client and AP. The connection is established by sending the request and responses of authentication and association between client and AP. While communication if attacker attacks the communication then de-authentication message is sent to both client and AP. To achieve this communication the finite state machine is used here. To be safe from the attacks, the FSMs provides the three frames that are active when the attack is there. There are total three frames. The first frame is 'probe request flood' that scans the network area. The client and AP sends the probe request and response to each other to get the current information about the network. The second frame is 'authentication request flood' which also scans the network and gets the information about the authenticated users. If any unauthenticated user found then immediately the message is sent to the client and AP. The third frame 'association request flood' which identifies the illegal access to the communication in the network. So using these frames the network may be free from the attacks.

D. Faria and D. Cheriton[4] introduce the client and server communication is established. This connection is developed in some wireless network like wi-fi wireless internet connection. The request is sent to some wireless appliance(WA), then that signal is transferred to the server. Here whenever the communication is held within client and server, the signals are sent to each other as it is wireless network. The strength of each signal is calculated and it is stored. The value of each signal is near about in same range. This value is called as the 'signalprint value'. This value totally depend on the physical location of the client. If the value of the signalprint is in same range then that signal is sent by the authenticated user but if that range of signalprint value changes that means some attacker may be accessing the data communication between client and server .

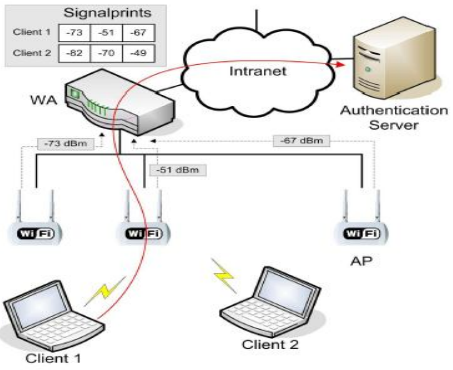


**Figure 1 :** Signalprint Creation

Q. Li and W. Trappe[5] described about the number of algorithms to calculate the signal strength measurement to check the susceptibility to the attacks. There are some ways to localization algorithms such as, 'range-based' which calculates the distance between the client and server and the landmarks. 'Point-based' way gives the estimated point as a result just like RADAR. There are some 'range-based' localization algorithms such as,

- "Simple point matching" in which the received signal strength(RSS) range matching is done.
- "Area-based probability" in which Baye's rule is applied in matching RSS and the area confidentiality is calculated in percentage.
- "Bayesian network " in which the most secure and confidential area is returned for secure communication.

There are some 'point-based' localization algorithms such as,

- "RADAR" gives the closest point at which the security is maintained.
- "Averaged RADAR" gives the average of the top two closest points at which the confidentiality is maintained.
- "Gridded RADAR" calculates the closest point using the interposed grid signal map.
- "Highest Probability" applies the highest range of received signal strength value to the received signal.
- "Averaged Highest" gives the average of two same range values of received signal.
- "Gridded Highest Probability" applies the two same range values of received signal strength to an interposed grid signal map [5].

B. Wu, J. Wu, E. Fernandez, and S. Magliveras [6]focused on the concept of 'cryptography'. In this also

the data communication is done between the client and server. For that again the connection establishment is done. Here the data attacker is not identified but the data is done free from any attack. Means that when the client is sending the data, some key is provided for that data to the server. Using that key only the data can be accessed. That infrastructure may be called as 'public key infrastructure'. So if any attacker gets the data, he cannot access that data as that data is in encoded format. Decoding of the data is done on the server side as the server contains the key to decode data which is provided by the client. So in this way the data is safe and the security is provided to the data. That key management is done by both the client and servers. Server group is developed safely and keeps attached. The certificate keep informing apply for is processed by server group in a ticket based concept. The system confidentiality held by each server is restored from time to time in a reasonable and well-organized way. New joining server with outdated contribute to could be renewed. Node's misbehaving is supervised and could be blamed by network nodes. A certificate can be invalidated by server group. Nodes with expired or invalidated certificate necessitate off-line reconfiguration .

A. Wool proposes WEP*,[7] a way out to the host-invalidation difficulty. The key management in WEP* is important tool. The Access Point time to time creates new keys, and these keys are sent to the hosts at the time of validation. The actuality that the keys are only applicable for one re-key episode creates host invalidation achievable, and balanceable. A invalid source will not collect the new keys. obviously, WEP* is not solution, and does not reach all the protection difficulties that IEEE 802.11 undergoes from. However, what makes WEP* worthwhile is that it is 100% companionable with *existing* standard. And, dissimilar to other solutions, WEP* does not depend on outside substantiation servers. So, WEP* is appropriate for use in the most basic IEEE 802.11 LAN arrangements also, such as those positioned in miniature or home offices. A WEP* trial product has been partially implemented using free, open-source tools.

Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell,[8] In this article authors proposed a technique for in cooperation discovering burlesquing bouts, as well as pinpointing the locations of challengers accomplishing the bouts. They first invented a bout indicator for wireless satirizing that uses K-means cluster investigation. After that, they described how they combined their bout finder into a real-time internal localization system, which is also proficient of localizing the locations of the invaders. After that they found that the locations of the invaders can be localized using either area-based or point-based localization algorithms. They had appraised the ways through practical session using both an 802.11 network and an 802.15.4 network. Their consequences showed that it is conceivable to find wireless taking off with both a high recognition amount, thereby giving durable indication of the activeness of the K-means taking off finder and the about localizer .

After that, the authors V. Brik, S. Banerjee, M. Gruteser, and S. Oh[10] 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. When two networks are connected, the routers are used to connect them. There are number of access points that are connected with the PARADIS sensor. Through that sensor the unauthorized user can be identified. They practically demonstrated that the usefulness of the PARADIS is differentiating in more than hundred similar IEEE 802.11 nics with accurate results. The PARADISE servers are also feasible in the changing characteristics of the wireless channel .

In the next paper, the authors P. Bahl and V.N. Padmanabhan [12] demonstrated the concept of identifying the location of attacker using RADAR. This concept is based on the physical location of the authorized as well as unauthorized users. The RADAR is having all information about the authorized users into the client-server communication. So, if any outer user is accessing the data then that information is with RADAR. So, it is easily identifiable the attacker .

C. Hsu and C. Lin[15] proposed again the new concept of 'Support vector machine'. It is having the characteristics as,

- Best differentiating Hyper plane.
- Formulation as an Optimization difficulty.
- Only Sustenance Vectors are Appropriate (Scarceness)
- Representing in High-dimensional Spaces
- Kernel Trick
- It may be a replacement for Neural Networks.

## 3. PROBLEM DEFINITION

Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device. The problems with the existing systems are,

- Not self defensive
- Effective only when implemented by large number of network.
- Implemented on static network
- Deployment is costly.

There are some problems in the existing systems, such as the systems are not able to defense if some attackers are attacking on the data. They are only able to identify the attacker. Some systems are not are not able to work well in one network, means their working is better if they are applied in large network. Some systems are very costly to

deploy. Some systems are having low performance due to some disadvantages.

## 4. OBJECTIVES AND FUTURE SCOPE

Due to the severe problems into the existing system, the more work can be done on this specific area. The additional work may include,

- Spoofing attack detection in dynamic network.
- Determining adversaries network access pattern
- Determining number of attackers when multiple adversaries masquerading as the same node identity.
- localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks.

For accuracy purpose we can use multi vector support vector machine.so that our experimental results could achieve over 90 percent Hit Rate and Precision when determining the number of attackers.

It does not mean that all these work was not done in the existing systems but there are some disadvantages. So by applying some new techniques, algorithms it may be possible to recover this problem.

## 5. CONCLUSION

Fetching and the removing the attacks in the client-server communication is a topic getting attention because there is high requirement of the secure communication and the data security.

In the existing system, there are number of the disadvantages with their techniques and the algorithms. The future scope is to invent the new algorithms and the techniques that are able to identify the attacker as well as to remove or to disable the attacker by overcoming the problems existing into the existing systems. Because of this the problem of data security into the client-server communication will be decreased.

## References

**[1]** Jie Yang, Yingying (Jennifer) Chen and Wade Trappe, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transection on parallel and distributed system, Vol. 24, NO. 1, January 2013.

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

**[3]** 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

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

**[5]** 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

**[6]** 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.

**[7]** 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.

**[8]** 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.

**[9]** 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.

**[10]** 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.

**[11]** 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

**[12]** P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

**[13]** E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

**[14]** J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

**[15]** C. Hsu and C. Lin, "A Comparison of Methods for Multiclass Support Vector Machines," IEEE Trans. Neural Networks, vol. 13, no. 2, pp. 415-425, Mar. 2002.