ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Protecting MAC Address Spoofing in IEEE 802.11 Using MATLAB

Menal Dahiya
Assistant Professor, Dept. Of Computer Science
Maharaja Surajmal Institute
C-4, Janakpuri, Delhi, India

Dr Sumeet Gill
Assistant Professor (Computer Science)
Dept. Of Mathematics, M. D. University
Rohtak, India

Abstract: It is a proven fact that wireless local area networks are less secure as compared to fixed networks. Since, it is very easy for an intruder to learn the authorized addresses and change MAC addresses accordingly. MAC address spoofing is an easy task for hackers, as many tools available in the market that alter MAC addresses. In this paper, we propose a methodology based on the performance/result of different training functions using Backpropagation algorithm of ANN. The methodology does not require any change in IEEE 802.11 protocols and experience a small performance overhead.

Keywords: Authentication; ANN; Back Propagation Algorithm; MAC Address Spoofing; Training Functions; WLAN.

I. INTRODUCTION

Authentication is a two way process in which user confirms his or her identity to the computer system. Authentication plays vital role in providing security to the communication systems. Authentication schemes are mostly based on passwords, smart cards, biometrics and address based authentication techniques [1]. Authentication ensures that the services and system resources are used by the authentic person.

Address based authentication scheme verifies the identity of sender from which packets arrive. This address could be either IP address or MAC address. Both network addresses are equally important for the network. Therefore an intruder wishing to interrupt a wireless network using tools. Tools for IP Address spoofing and MAC address spoofing are easily available on the internet. Mostly all wireless routers use MAC address based authentication as a security scheme [2]. MAC address spoofing is easy in IEEE 802.11 wireless LANs. For example an intruder can disrupt the network connections by doing denial of service attack or performing Man-in-the-Middle attacks to nearby wireless stations. Existing security techniques for IEEE 802.11 are not sufficient for the authentication and primary mechanism. WEP, WPA OR WPA2 (802.11i) protocols protects only data frames. An attacker can still spoof management or control frames to cause damage. In wired LAN topology, point to point node connection link is configured with the MAC address of the node in each link [3]. But breaching the security using MAC address is not easy because learning MAC address through network traffic is difficult and secondly, an attacker needs to have a physical access to the port that MAC address is registered with. On the other hand, in wireless LAN it becomes easy for the unauthorized person to impersonating as an authorized user through MAC address spoofing. The Attacker uses any pocket capturing software, sniffs the network traffic and takes out the authorized MAC addresses. Another option is an alteration of MAC address with the authorized one. Basically, MAC address authentication is widely applicable for permitting or denying access to the wireless network. In this paper, our objective is to improve the security of IEEE 802.11 provided with MAC address authentication using Backpropagation Algorithm [4]. We propose a methodology for IEEE 802.11 to avoid unauthorized access or attacks through MAC address spoofing. The rest of the paper is organized as follows: Section II describes about the background on IEEE 802.11, Section III explains the MAC address Spoofing, In section IV we discussed the experimental work and then Section V concludes the result and discussion followed by a conclusion.

II. BACKGROUND ON IEEE 802.11

WLAN technology is experiencing tremendous growth which is due to increment in bandwidth made possible by the IEE 802.11 standard. Early WLAN technologies had several problems like they were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF technologies. The 802.11 project is initiated in 1990 by IEEE to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." In 1997, IEEE first approved the 802.11 international interoperability standards. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards whose goal were to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications [5]. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps. Motorola developed one of the first WLAN technology [6].

Wi-Fi can be used as various handheld devices. The handheld devices are connected to the internet by using the connection of Wi-Fi. The access of the Wi-Fi network is limited to a specific area and should not expand the network. This network is only for within the specified area only. And its established limited in some restricted place. Wi-Fi is not a technical term. However, Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other premises, can provide Internet access and internet working to all devices connected (wirelessly or by cable) to them. The connection was established from one system to another directly without any intermediate node. This mode of connection is known as an Adhoc Network. The connection establishment of the Wi-Fi is using some consumer electronic devices.

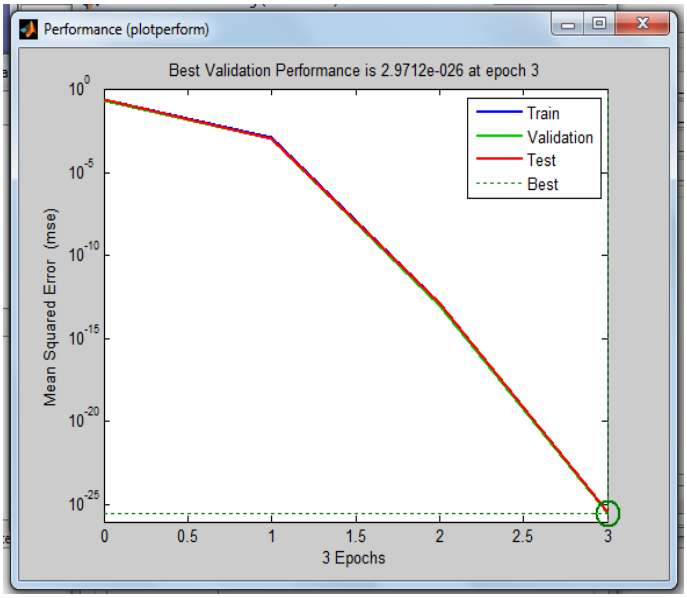
III. MAC Address Spoofing

MAC address spoofing means an attacker altering the MAC address assigned by the manufacturer to any other value and utilize the wireless facility for their own purpose, transmitting and receiving from the same source MAC. The MAC address is globally unique for all devices. Every network interface controller (NIC) has a unique MAC address "burned" into it [7]. By exchanging MAC addresses, Local area network computers identify each other. Each Ethernet interface includes the unique 48-bit media access control (MAC) address at the time of manufacturing. The MAC address is used as an authentication factor for granting services to a user. So, various attackers targeting wireless LANs through MAC address spoofing technique. MAC spoofing is a computer identity theft, to prevent MAC address spoofing one needs to harden the system and access points or to detect MAC spoofing [8]. There are various methods for spoofing detection like Transceiver Fingerprinting, Sequence-Number Analysis, 802.11 Spoofing Based Attacks, etc..

IV. Experimental Setup

Table 1: Weights for Trainlm Function.

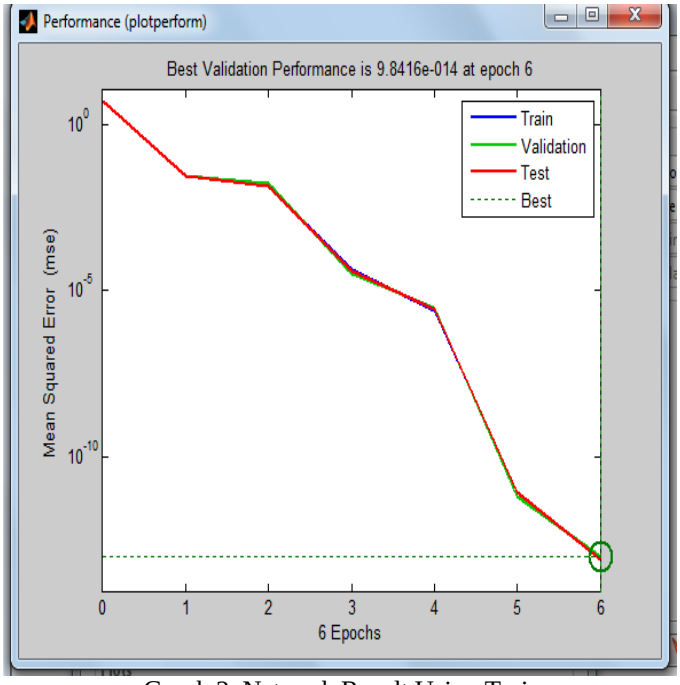
	Initial Weights			
Between Input Layer to Hidden Layer	0.7257	0.4743	0.2578	0.9217
	0.5413	0.1008	0.9807	0.0087
	0.2467	-0.0128	0.5421	0.8965
	0.3765	0.9001	0.0008	0.1032
	0.0024	-0.0124	0.0089	0.3412
	0.01765	0.8912	0.0012	0.0306
Between Hidden Layer to Output Layer	0.5461	0.5273	-0.0025	0.9862
	0.3421	0.1004	0.3564	0.6581
	0.4452	0.0202	0.1265	-0.9816
	-0.0027	0.0206	0.1034	0.2341
	0.5461	0.1278	-0.6732	0.3452
	0.6413	0.1033	0.0198	0.0192



Graph 1. Network Result Using Trainlm

Table 2: Weights for Trainscg Function.

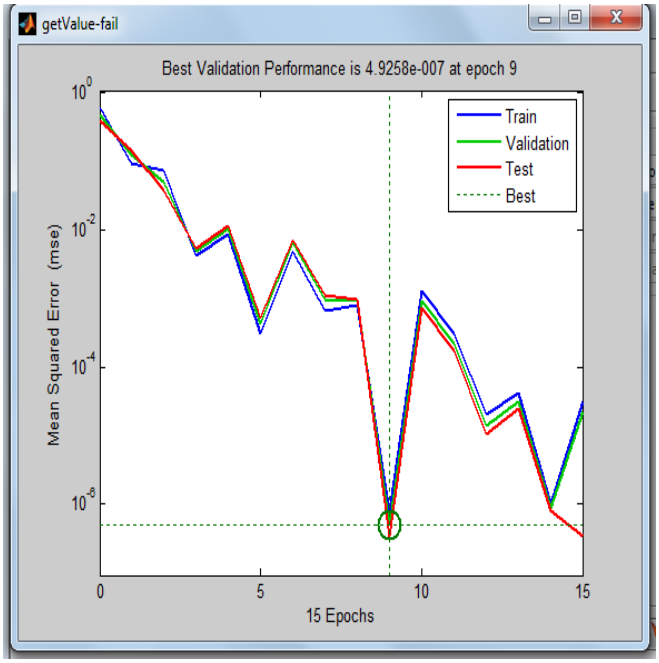
	Initial Weights			
Between Input Layer to Hidden Layer	-0.6893	0.7507	0.5464	0.7854
	0.4532	-0.0016	0.9852	0.8743
	0.0112	0.0202	-0.3010	0.1276
	0.2341	0.0061	0.0876	0.5101
	0.3113	0.2183	-0.0298	0.9926
	0.2351	0.5423	0.7821	0.7722
Between Hidden Layer to Output Layer	0.4321	0.4433	-0.1221	0.2434
	0.1113	0.3667	0.4521	0.6121
	0.2144	0.3443	0.2112	0.8429
	0.0033	0.4421	0.2312	0.2242
	0.3322	0.8195	0.8009	0.0203
	-0.6381	0.2556	0.2115	0.0406



Graph 2. Network Result Using Trainscg

Table 3: Weights for Trairp Function.

	Initial Weights			
Between Input Layer to Hidden Layer	-0.5534	0.0065	0.7888	0.7749
	0.7698	0.6107	0.3481	0.0047
	0.9229	0.8746	0.1745	0.2690
	0.8895	0.4309	0.6399	0.4485
	0.8460	0.6924	0.4867	0.0034
	0.1570	0.6101	-0.1388	0.1705
Between Hidden Layer to Output Layer	-0.0034	0.9889	0.1252	0.3434
	0.0606	0.0058	0.1049	0.2020
	0.1212	0.1003	0.0005	0.3008
	0.0023	0.4548	0.4477	0.6632
	0.3286	0.8736	0.8877	0.5920
	0.3402	0.0037	0.1284	-0.7503



Graph 3. Network Result Using Trainrp

V. RESULT AND DISCUSSION

Three experiments are performed on a Feed Forward Neural Network by taking three training functions. The three training functions are taken from three training algorithms respectively one from each. The above graph 1 to 3 shows the network result of the architecture (48-24-48). If we compare the training function based on below parameters:

A. Based on Epochs

Table 4: Results Based on Epochs.

S.No.	Training Functions	Epochs
1	Trainrp	15
2	Trainscg	6
3	Trainlm	3

The above summary of results in table 4 shows that trainrp takes 15 epochs for training and trainscg takes 6 epochs. Results/Performance of Trainlm is best if we take epochs as a priority for training.

B. Based on MSE

Table 5: Results Based on MSE.

S.No	Training Functions	MSE
1	Trainrp	0.612
2	Trainscg	0.157
3	Trainlm	0.259

The results in table 5 show that maximum error is shown by trainrp function followed by trainlm. Trainscg shows the minimum error of 0.157.

C. Based on Time

Table 6: Results Based on Time.

S.No.	Training Functions	Time
1	Trainrp	0.007 Sec
2	Trainscg	0.003 Sec
3	Trainlm	0 Sec

The results in table 6 show that all three training functions take different times for completing the convergence. Trainlm takes negligible time and proves best in term of training time.

VI. CONCLUSION

The above results and calculation concludes that which training function is suitable for training the MAC address in a better way. One of the most used supervised ANN model is a Backpropagation learning algorithm. Here, we train the network by using BPNN with MAC address as an IP and store the MAC address in the form of network parameters. This methodology prevents the MAC address spoofing as the network parameters are not easily understandable by intruders. Our methodology provides authentication and privacy too. Not any third party can connect different communication link of the same user by monitoring MAC addresses. Attackers cannot change the MAC address as they are stored in the form of network parameters.

VII. REFERENCES

[1] Kemal Bicakci and Yusuf Uzunay, "Pushing the Limits of Address Based Authentication: How to avoid MAC Address Spoofing in Wireless LANs," International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Volume.02, Issue.06, 2008, pp. 1092-1101.

[2] C. Kaufman, R. Perlman and M. Speciner, Network Security Private Communication in a Public World, Prentice Hall, Second Edition, 2002.

[3] Infoexpress, "Detecting and Preventing MAC Spoofing," https://infoexpress.com/content/practical/142.

[4] Shrikant Ramesh, "How to Spoof MAC address on Android Phone," 2017, https://www.gohacking.com/spoof-mac-address-on-android-phones/.

[5] Wireless LAN Security Paper, 2003, available http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf.

[6] Chapter 1 Introduction 1.1 Wireless Technology, http://shodhganga.inflibnet.ac.in/bitstream/10603/34313/10/09_chapter-1.pdf.

[7] J. Wright, "Detecting wireless LAN MAC address spoofing," technical document, 2003, http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.

[8] Yong Sheng, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," 27th IEEE Conference on Computer Communications, 13th-18th April 2008, DOI: 10.1109/INFOCOM.2008.239.