14th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 14 – May 24 - 26, 2011, Email: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel: +(202) 24025292 –24036138, Fax: +(202) 22621908

Preventing Information Leakage Caused by War Driving Attacks in Wi-Fi Networks

M.E. Elhamahmy[*] and T.S. Sobh[†]

Abstract: The information leakage problem presents one big challenge in the Wi-Fi networks which are widely used nowadays. The War-Driving attacks that target the widely used wireless network hosts and resulted in information leakage present a real challenge. In this paper, a solution that provides a tailored tool based on the open source software is proposed to prevent the information leakage in Wi-Fi networks specially when using the War-Driving attack. It aims to prevent the information leakage on the node machine connected to a Wi-Fi network. It also provides statistical reports that include useful data about the file access on the user-machine. The statistical reports provide the machine-user with complete information about who, what and where in the user-machine a remote user tries to have an access. It also provides the required user permissions to allow/block access of the files on the user-machine that used a client-version of MS-Windows which do not provide user permissions on the shared files. The experiments include the War-Driving attack are maintained through an attack scenario to test the effectiveness of the proposed tools. The host that is protected with the proposed tool success in detecting the war-driving attack through the defense scenario experiment. It also success in preventing the information leakage from the protected host as well.

Keywords—Wi-Fi networks, Information Leakage, War-Driving attacks, WEP cracking.

1. Introduction

The popularity of wireless networking is a function of convenience [1]. It provides the mobility which presents one of the most important features in the advanced computing technology. Wireless technologies may be categorized in a variety of ways depending on their function, frequencies, bandwidth, communication protocols involved, and level of sophistication (i.e., 1st through 3rd generation wireless systems) [2]. In this paper, it is emphasized on two categories: 1) Personal Area Network (PAN) and 2) Wireless Local Area Network (WLAN). PAN began as "workspace networks. Blue tooth, for example, is a desktop mobility PAN that was designed to support cable-free communication between computers and peripherals. WLAN is what most of us think of Wireless technology. It includes the now-ubiquitous 802.11 family of protocols, as well as a few others. While the fact that Wi-Fi technology has a few security vulnerabilities is not news, the extent of these vulnerabilities may be surprising.

[*] Egyptian Armed Forces, Egypt; mezzat1967@yahoo.com
[†] Egyptian Armed Forces, Egypt; tarekbox2000@gmail.com

War Driving Concept

It is an extension of the concept of War Dialing that deserves some explanation. The basic idea behind War Driving is to “sniff” 802.11 traffics with a wireless card set in “monitor” mode so that it accepts all traffic on frequency irrespective of intended target. The “War Driving” approach is considered as an example of attacks that exploit such Wi-Fi network vulnerabilities [3].

Piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks, particularly since people on average use only a fraction of their downstream bandwidth at any given time. Recreational logging and mapping of other people's access points has become known as war driving. It is also common for people to use open (unencrypted) Wi-Fi networks as a free service, termed piggybacking [4].

Wireless Network Security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking one must either gain access to a building (physically connecting into the internal network) or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus gaining wireless connectivity provides an attack vector, particularly if the network lacks encryption or if the intruder can defeat any encryption. Attackers who target the wireless networks may face the secured networks which use WEP keys. A common but unproductive measure to deter unauthorized users involves suppressing the access point's SSID broadcast, "hiding" it. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. But intruders can defeat this method because they can often (though not always) set MAC addresses with minimal effort (MAC spoofing). If eavesdroppers have the ability to change their MAC address, then they may join the network by spoofing an authorized address. Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping, but is now deprecated by using some open source tools [5].

In this paper a proposed solution is provided based on such open source tools. The proposed solution is a tool to be installed on the host (a machine) to be protected against the wireless network attacks such as War-Driving attack. In section 2, the related works to the wireless security issues are presented. In section 3, the proposed model to defend the victim host is presented. The experimental results are discussed in section 4. The conclusion is presented in section 5 and the references are presented in section 6.

2. Related Works

Wi-Fi technology was built based on the IEEE 802.11 standards. The IEEE develops and publishes some of these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010, the Wi-Fi Alliance consisted of more than 375 companies from around the world. The most common wireless encryption-standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even when correctly configured. Wi-Fi

Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi access points typically default to an encryption-free (open) mode. Novice users benefit from a zero-configuration device that works out-of-the-box, but this default does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks connecting devices can monitor and record data (including personal information), but such networks may use other means of protection, such as a VPN or secure Hypertext Transfer Protocol (HTTPS) over Transport Layer Security [6]. The “War-driving” term was originated from “war-dialing”, a technique popularized by a character played by Matthew Broderick in the film “War-Games”, and named after that film. “War-dialing” in this context refers to the practice of using a computer to dial many phone numbers in the hopes of finding an active modem [7]. War-drivers are only out to log and collect information about the wireless access points (WAPs) they find while driving, without using the networks' services. Connecting to the network and using its services without explicit authorization is referred to as piggybacking. The terms have been interchanged in the press, however. For instance, an EETimes article with the headline "Wi-Fi user charged for not buying coffee" [8] refers to a user who "piggybacked off the shop's wireless Internet service for more than three months". When reposted by Engadget, the term "war-driving" was substituted, and the headline changed to "War-driver arrested for snagging coffee shop signal" [9]. Typical war-driving software actually takes control of the wireless radio, making it impractical, if not impossible, to war-drive and piggyback simultaneously.

The current version of Wi-Fi Protected Access encryption (WPA2) is considered secure, provided users employ a strong pass phrase. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video); and power saving mechanisms (WMM Power Save) improve battery operation. On the other hand, there is no mean to make the machine user has any permission on the shared files of his machine when he used the MS-Windows operating system for client. Thereby, the proposed tool provides add on function for securing this kind of circumstances. A commonly used operating system which has a well-known issue of the user permissions on the shared files when get into a workgroup. In the next section the proposed model to recover this issue is presented.

3. The Proposed Model

Figure 1 provides the proposed wireless protection against the “War-Driving” attack and data leakage as well. This project is composed of five main modules, Wi-Fi network manager module, Wi-Fi detailed packet sniffer module, alerts module, Wi-Fi packet filter module, and statistics & analysis reports module. In the next sections, these five modules should be explained.

3.1. Wi-Fi Packet Sniffer Module

In Fig. 1, the Wi-Fi traffics are sniffed by the Wi-Fi packet sniffer module. Packet sniffer module captures all the arrival Wi-Fi packets and provides total information about it. At first user has to choose a network device then press start capture to begin sniffing the packets. Then user can choose to stop sniffing and drop the sniffed packets into a “PCAP” file format (Logged Data) as shown in Fig. 1. Packet sniffer module identifies: Packet arrival time; Length; Source IP; Destination IP Protocol and Payload. The packet sniffer module provides multi panes so that the user can select a specific packet in one pane to display its data content in another pane view.

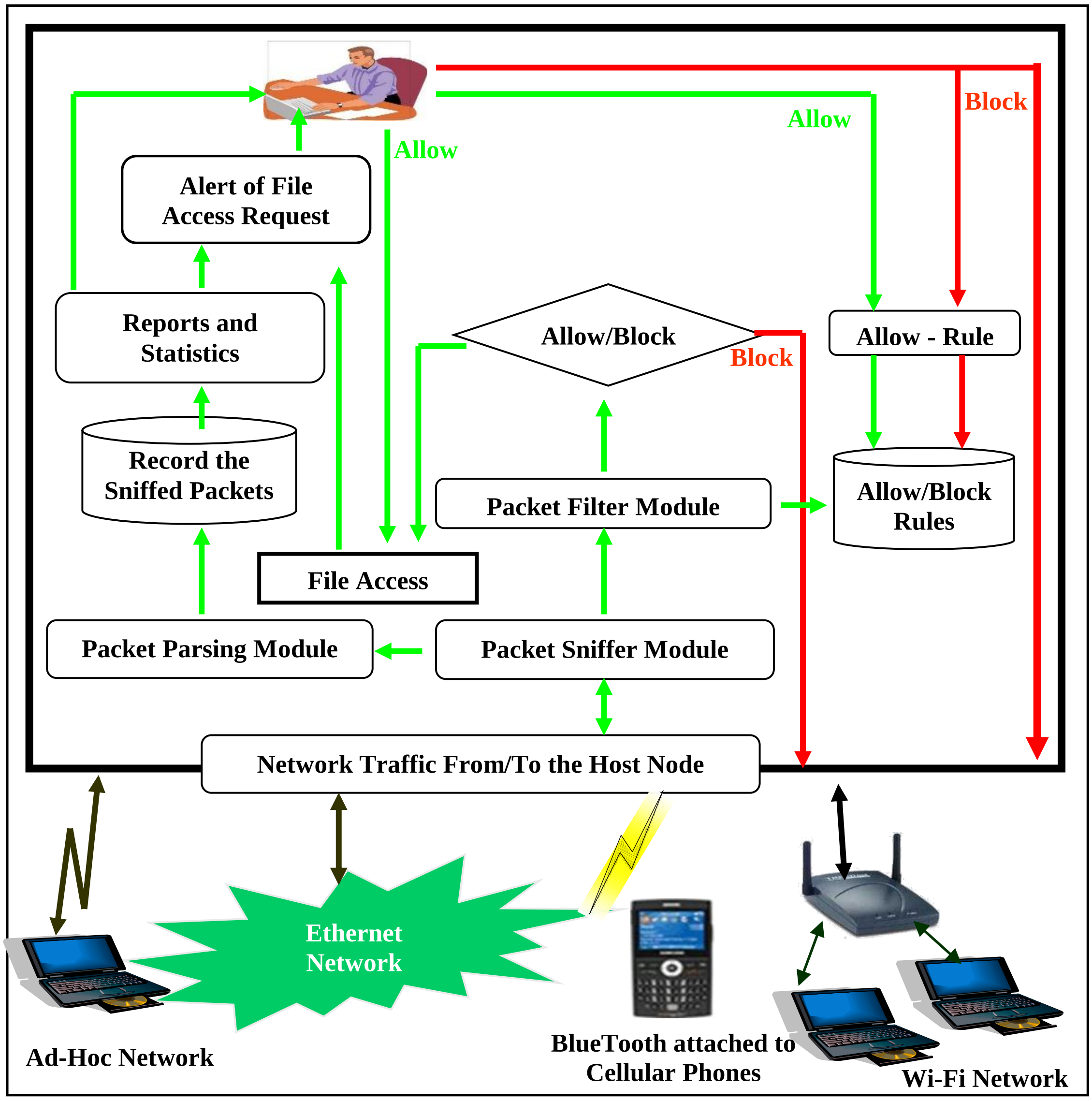


Fig. 1 The proposed model for defending against the data leakage in wireless networks

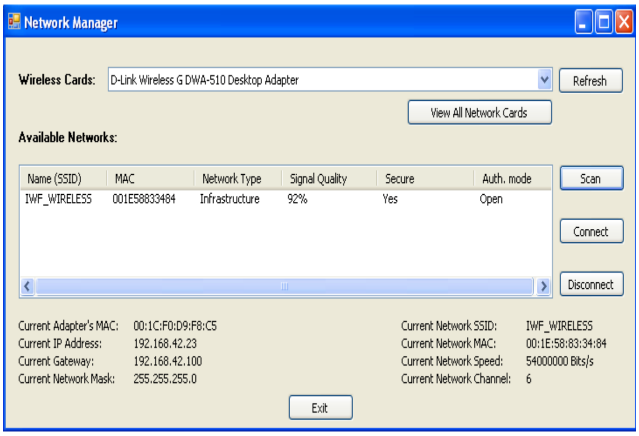
3.2. Wi-Fi Network Manager Module

Wi-Fi Manager module provides information about the available wireless networks for the user machine includes as shown in Fig. 2: Network card type, Network name, MAC, Signal quality, Security and Authentication. User can do “scan process” at any time to be informed with the available wireless networks and their data.

As shown in the Fig. 2., the SSID is “IWF_Wireless” its MAC address is presented as well. The signal quality for this detected network is 92% and it is secured WLAN. The “Scan” option can be selected more and more to detect the detected Wi-Fi networks.

3.3 Alerts Module

The Alerts module arise alerts when policy violation detected. Such as a file/directory on the host machine is required to be illegal accessed by a network user.



Wireless Cards: D-Link Wireless G DWA-510 Desktop Adapter

Available Networks:

Name (SSID)	MAC	Network Type	Signal Quality	Secure	Auth. mode
IWF_WIRELESS	001E58833484	Infrastructure	92%	Yes	Open

Current Adapter's MAC:	00:1C:F0:D9:F8:C5	Current Network SSID:	IWF_WIRELESS
Current IP Address:	192.168.42.23	Current Network MAC:	00:1E:58:83:34:84
Current Gateway:	192.168.42.100	Current Network Speed:	54000000 Bits/s
Current Network Mask:	255.255.255.0	Current Network Channel:	6

Fig. 2 The Proposed Tool Interface on Successful Attack

3.4 Wi-Fi Packet Filter Module

This module is a host-side filter to allow/deny the connections to the user machine. It is different from windows firewall as it is designed to provide more options which allow user to:

- Prevent the connections by all other network nodes on the same network from connect to the user host.
- The user also has an option to identify some legible machine IP(s) to allow them to connect to his host machine. So that, the user has the ability to connect to the network, while all other network nodes will be denied

3.5 Statistics and Analysis Report Module

This module allows the user to get a statistical and analysis charts of network activities captured by the system. These charts can give the user information about the most active IPs with the user's machine in the last session, the most active source and destination ports in the last session and the most active IPs through a specific period of time determined by the user as well.

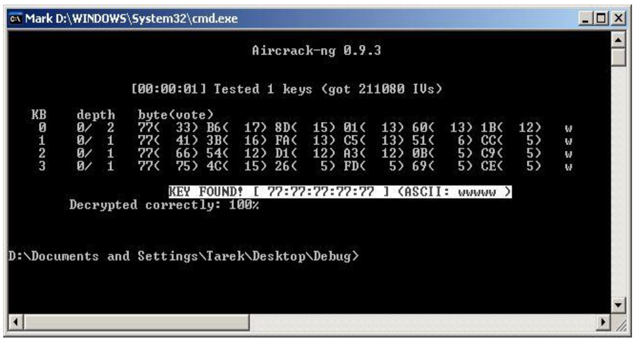
4. The Experimental Results

To match the mentioned objectives, the experiments are included in two scenarios. One is the attack scenario. It is maintained to imitate the attack like actions to get into a wireless network and get data out of one host (data leakage). The second is the defense scenario that presents using of a proposed tool to countermeasure the vulnerabilities found by the attack scenario and specify prevention of the data leakage.

4.1 The attack Scenario

The “Aircrack-ng” is an 802.11 WEP and “WPA-PSK” keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like “KoreK” attacks. Thereby all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools. The “Aircrack-ng” is a network software suite consists of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless card whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and MS-Windows operating system as well. The “Aircrack-ng” software suite includes “Airodump-ng” which is used for packet capturing of raw 802.11

frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with “Aircrack-ng” tool. Additionally, “Airodump-ng” writes out several files containing the details of all access points and clients seen. Airodump-ng will display a list of detected access points, and also a list of connected clients (“stations”). Features can be detected using the “Airodump-ng” tool. To speed up the cracking process, we run “Aircrack-ng” while running the “Airodump-ng” tool. The “Aircrack-ng” will periodically reread the captured data so it is always working with all the available IVs. Figure 3 shows the success of cracking the WEP protection of the victim machine and gets the key in ASCII format as well as in HEX format.



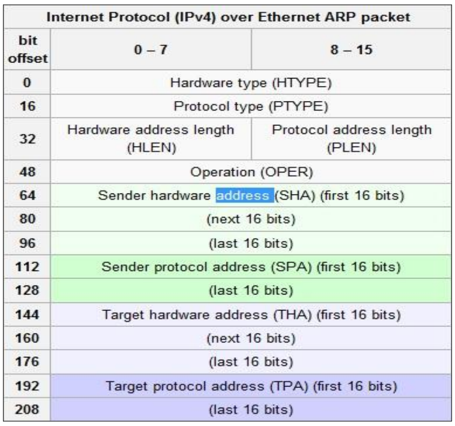
```
                         Aircrack-ng 0.9.3

                 [00:00:01] Tested 1 keys (got 211080 IVs)

   KB    depth   byte(vote)
    0    0/  2   77(  33) B6(  17) 8D(  15) 01(  13) 60(  13) 1B(  12)   w
    1    0/  1   77(  41) 3B(  16) FA(  13) C5(  13) 51(   6) CC(   5)   w
    2    0/  1   77(  66) 54(  12) D1(  12) A3(  12) 0B(   5) C9(   5)   w
    3    0/  1   77(  75) 4C(  15) 26(   5) FD(   5) 69(   5) CE(   5)   w

                   KEY FOUND! [ 77:77:77:77:77 ] (ASCII: wwwww )
        Decrypted correctly: 100%


D:\Documents and Settings\Tarek\Desktop\Debug>
```

Fig. 3 Using of an open source tool to crack the WEP key

Sometimes we watch”<length :?>” as the SSID on the “Airodump-ng” display. This means the SSID is hidden. The”?” is normally the length of the SSID. For example, if the SSID was “test123” then it would show up as”<length: 7>” where 7 is the number of characters. When the length is 0 or 1, it means the AP does not reveal the actual length and the real length could be any value. To obtain the hidden SSID there are a few options. We wait for a wireless client to associate with the AP. When this happens, Airodump-ng will capture and display the SSID. Authenticate an existing wireless client to force it to associate again. The point above will apply. Use a tool like mdk3 to brute force the SSID. We choose to use “Wireshark” combined with one or more of these filters to review data capture files.

4.2 The Defense Scenario

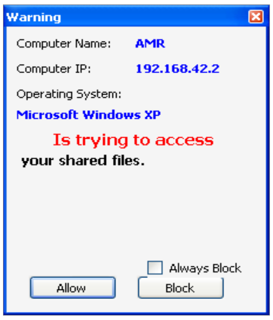
When discovering a new machine appeared in the network an appropriate alert should be raised to the user. The alert should has some details about the new node appeared such as the machine IP, machine Mac address and the machine name. The idea is that when a new machine joins the network it broadcasts ARP packets to all machines in the network because ARP is used as a simple announcement protocol. This is useful for updating other host's mapping of a hardware address when the sender's IP address or MAC address needs to be updated in all machines. By detecting ARP packets as shown in Fig. 4, reaching to the user’s machine.



Internet Protocol (IPv4) over Ethernet ARP packet		
bit offset	0 – 7	8 – 15
0	Hardware type (HTYPE)	
16	Protocol type (PTYPE)	
32	Hardware address length (HLEN)	Protocol address length (PLEN)
48	Operation (OPER)	
64	Sender hardware address (SHA) (first 16 bits)	
80	(next 16 bits)	
96	(last 16 bits)	
112	Sender protocol address (SPA) (first 16 bits)	
128	(last 16 bits)	
144	Target hardware address (THA) (first 16 bits)	
160	(next 16 bits)	
176	(last 16 bits)	
192	Target protocol address (TPA) (first 16 bits)	
208	(last 16 bits)	

Fig. 4 ARP Packet Structure

If the details of this machine already exist in the user’s database, it means it’s already known machine. If not it means it’s a new machine joined the network. The system will alert the user about this new machine. From IP address, Mac address and machine name the user can know if this machine is trusted or it’s not trusted (may be attack machine) and he must take action with it to protect the network. The Alerts module raised the following alert as shown in Fig. 5, when policy violation detected. Without this alert, the machine user should not know that a network user trying to access his machine. Now, the machine user has to decide whether to allow or deny this trial.



Warning

Computer Name: AMR

Computer IP: 192.168.42.2

Operating System:
Microsoft Windows XP

Is trying to access
your shared files.

Fig. 5 The Alert Message on Illegal Access Trial

This module is a host-side filter to allow/deny the connections to the user machine. The machine user can select the “Always Block” option which prevents this user from accessing this machine from now on. The user can also select the “Block” option which means to block this request one time only. The reaction of the machine user should be logged to be statistically analyzed later.

The statistical analysis of the machine activities can be viewed by charts representing the most frequent used files or IPs. Fig. 6 shows an example of the machines with the shown IPS 192.168.42.23 and 192.168.42.51 that have accessed the secured machine.

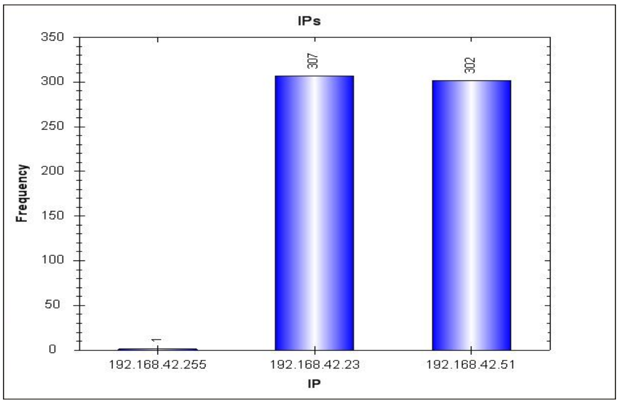


Fig. 6 The frequency of the IP usage

5. Conclusions

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. Attackers who have gained access to a Wi-Fi network can use DNS spoofing attacks very effectively against any other user of the victim network. They can see the DNS requests made, and often respond with a spoofed answer before the queried DNS server has a chance to reply. Recreational logging and mapping of other people's access points has become known as “War-Driving”. It is also common for people to use open (unencrypted) Wi-Fi networks as a free service, termed piggybacking. Once the target Wi-Fi network is compromised, a data leakage may be occurred without feeling of the leaked machine user. The attacker may also try the passive sniffing once he got cracking the WEP key. In this paper, a solution of such issues is proposed based on the open source tools such as “Wireshark”, “Aircrack-ng” and “Airodump-ng”. Two scenarios are maintained, the attack scenario and the defense scenario. These tools are used in the attack scenario to crack the WEP key of the experimental network which protected using the WEP encryption. The attack scenario is accomplished successfully against the experimental network. The proposed tool is designed to detect the both of active and passive attacks of the Wi-Fi networks and enforce the security policy against these attacks. In the defense scenario, the same attack trials are repeated with the same network after using the proposed tool. The alerts are generated when the attack trials take place. The passive eavesdropping attacker is hard to be detected. When discovering such attacker machine the proposed tool arise an alert to the proposed tool’s user along with some details about this machine such as (the machine IP, machine Mac address and machine name). The idea is that when a new machine joins the network it broadcasts ARP packets to all machines in the network because ARP is used as a simple announcement protocol. This is useful for updating other host's mapping of a hardware address when the sender's IP address or MAC address needs to be updated in all machines. By detecting ARP packets, reaching to the user’s machine. If the details of this machine is already exists in the user’s database, it means it’s already known machine. If not it means it’s a new machine joined the network. The system will alert the user about this new machine. From IP address, Mac address and machine name the user can know if this machine is trusted or it’s not trusted (may be attack machine) and he must take action with it to protect the target network. The proposed tool could protect the Wi-Fi networks against the “War Driving” attacks and enforce the security policy. The both of WPA and WPA-2 encryption techniques are more secured than WEP. However they are not tried in this paper and may be studied with the proposed tool on the future.

6. References

[1] LaRoche, P. and Zincir-Heywood, A.N., “Genetic Programming Based Wi-Fi Data Link Layer Attack Detection”, “*In Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR 2006)*”, IEEE Press, May 24–25, 2006, pp. 8–15.

[2] Balachandran, S., Dasgupta, D. and Wang, L., “A Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks”, “*In Symposium on Information Assurance*”, New York, USA, June 14–15, 2006.

[3] Mishra, A. and Arbaugh, W. A., “An Initial Security Analysis of the IEEE 802.1x Standard”, University of Maryland, Tech. Rep. CS-TR-4328, 802.11, IEEE 802.11 Standard, 2005. Available at: http://grouper.ieee.org/groups/802/11/ [accessed 24 Mar, 2010]

[4] Borisov, N., Goldberg, I. and Wagner, D., “Intercepting Mobile Communications: the Insecurity of 802.11”, “*In 7th Annual International Conference on Mobile Computing and Networking*”, 2001.

[5] Fluhrer, S., Mantin, I. and Shamir, A. “Weaknesses in the Key Scheduling Algorithm of RC4”, “*In 8th Annual International Workshop on Selected Areas in Cryptography*”, 2001.

[6] Rager A. T., “WEP Crack and Airsnort”, SourceForge, (2005). Available at: http://wepcrack.sourceforge.net/ [accessed 24 May, 2010]

[7] "Securing Wi-Fi Wireless Networks with Today’s Technologies". Wi-Fi Alliance. Available at: http://www.wi-fi.org/files/wp_4_Securing%20Wireless%20Networks_2-6-03.pdf [Accessed Nov. 2009].

[8] "WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks". Wi-Fi Alliance. Available at: http://www.wifi.org/files/wp_6_WPA%20Deployment%20for%20Public%20Access_10-28-04.pdf [Accessed 27 Nov. 2009].

[9] Kumari, L., Debbarma, S. and Shyam R., “Security Problems in Campus Network and Its Solutions”, “*International Journal of Advanced Engineering & Application*”, Vol. 1, Issue 1, pp. 98-101, Jan, 2011.