A Comparative Study of Various Wireless Network Monitoring Tools

Rajinder Singh
Deptt. Of Computer Science & Applications
Panjab University SSG Regional Centre,
Hoshiarpur, Punjab (India)
rajinderid@gmail.com

Satish Kumar
Deptt. Of Computer Science & Applications
Panjab University SSG Regional Centre,
Hoshiarpur, Punjab (India)
satishnotra@yahoo.co.in

***Abstract*—Nowadays wireless networks are growing very rapidly. Similarly, number of users which are using wireless network are also growing daily. With the development and popularity of the wireless network, it is important for the network administrators to keep the network efficient and smooth. It is very important to monitor the network traffic. Packet sniffer tools help in network monitoring and troubleshooting the network problems. At present a number of packet sniffer tools are available in the market. In this paper a number of wireless network monitoring tools are discussed. It focuses on basics of various wireless sniffer tools and their working under different operating environment. This paper also focuses on the capability of these tools to troubleshoot wireless network problems.**

Keywords—sniffer, wireshark, kismac, tcpdump, kismet

I. INTRODUCTION

Nowadays wireless networks are growing very rapidly. With the development and popularity of wireless network, management, monitoring and troubleshooting of the wireless network is also important [1]. It is important for wireless administrators to monitor the activities of users to keep the network efficient and smooth. Wireless sniffers are used for this purpose. Packet sniffing is used by the network administrators to keep the log of network activities of users [2]. Currently a number of packet sniffer tools are available in the market, which can be used for network sniffing. It is important for network administrators to troubleshoot and analyze the behavior of 802.11 standard to check the performance, functioning and security of the wireless network. In the network all data travels in the form of packets. Downloading a file, accessing a web page reading or sending an email, all these communication between the two nodes is done in the form of packets [2]. Network sniffer tools are used to capture the network traffic and analyze it. A sniffer tool sometime is also called network analyzer, a protocol analyzer or packet analyzer [3].

According to Wikipedia a sniffer tool is a computer program or a piece of computer hardware that can be used to capture the network traffic [4]. Using a sniffer is very helpful for the network analyzers and network administrators for troubleshooting network problems, maintaining network traffic, detecting intrusion, controlling the traffic, and supervising the network contents.

Many enterprise level tools are available in the market for monitoring Wi-Fi network but these simple freeware tools are also very handy for troubleshooting wireless network. These sniffing tools provide basic detail about the Wi-Fi signal such as signal strength, SSID, security status, MAC address and channel.

Today main operating systems dominating the world are i) Windows ii) Linux iii) Mackintosh operating system. In this paper a number of sniffer tools available in these different operating environments are discussed. Their role in case of troubleshooting network problems is also discussed.

II. WORKING OF A NETWORK MONITORING TOOL

A Wi-Fi sniffer tool can find the nearest wireless connection. It can also tell us about the strength of the wireless signal. Wireless sniffer tools are supported by many wireless cards. Wi-Fi sniffers are written in the C++ programming language.

First wireless card is put into the monitor mode or promiscuous mode. This mode allows wireless network card to receive all the packets from the network and send to operating system. In this mode network card can only receive wireless traffic and it cannot transmit data. Then the sniffer tool further decodes or analyzes received packets with the help of a protocol sniffer or dissector. Useful information is fetched from the captured packets and then presented to the user.

There are two parts of a sniffer [5]. i) Packet Analyzer Module ii) Packet Capturing Module

Packet capturing module captures all the packets from the network and packet analyzer tool is used to analyze the packets.

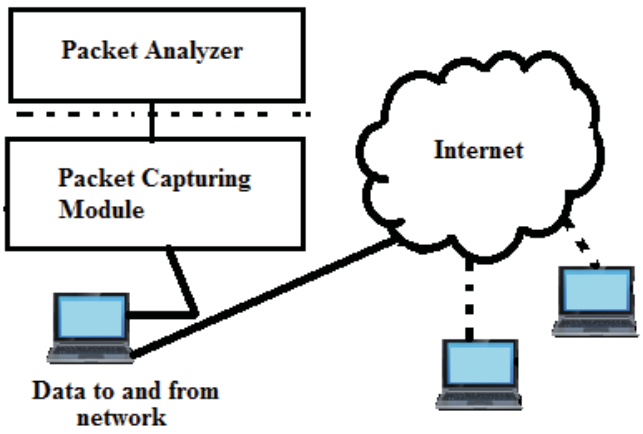

Fig. 1. Structure of a Wireless Sniffer.

III. Wireless Monitoring tools in case of Windows

Main wireless monitoring tools in case of Windows operating system are given below.

A. *Wireshark*

It is a very popular network troubleshooting tool available in the market. It allows the network administrators to put the wireless card in promiscuous mode, allowing it to monitor all the wireless traffic. This tool is very helpful to understand the structure of various network protocols. This tool can also be used for capturing the wireless traffic. Captured data can be used by the network administrators for troubleshooting the network problems [6].

B. *Cain and Able*

Although it is basically a password recovery and password cracking tool, but it can also be used for sniffing wireless traffic. It can also be used for penetrating testing. It is also used for cracking applications. This tool supports monitor or promiscuous mode for capturing wireless traffic. This tool has a simple and older GUI. Top of the GUI contain an old-style toolbar with different icons for showing different utilities. The wireless tab can be used to display the wireless network information. It can display SSID, signal information and connected clients. Like Acrylic Wi-Fi tool it can also reveal hidden SSIDs. Network traffic captured with this tool can be exported to a text file [7].

C. *Homedale*

Homedale is a simple and portable stumbler tool. It supports both command line interface and GUI. Its GUI consist of multi-tabbed dialog box. Its adapter tab can display all the network adapters. Its access point tab can be used to display essential information about the network. It can display the supported data rates. This tool can not reveal hidden SSIDs but it can display other network details of hidden SSIDs [8].

D. *Acrylic Wi-Fi Home 3.1*

It comes in both commercial as well as home edition. Acrylic Wi-Fi Home Free is a very good Wi-Fi stumbler tool for basic needs. Its interface shows both textual and graphical details. The free edition has a simple and attractive Graphical user interface. This tool can display SSIDs, RSSI values, 802.11 standards with a name, and multiple channels [9].

E. *Wi-Fi Network Monitor*

It is a free tool which can be used by the administrators for checking and discovering all the devices connected to the network. Its ARP technique can detect all the connected devices in very less time. Main features of this tool are it can detect RAP. It detects IP address, Device name and MAC address. Captured network traffic can be saved in HTML/XML/TEXT and/or in the CSV file. It has a very good GUI. It can run on any Windows operating System [10].

F. *WirelessNetView*

It is a small tool which can display SSID, MAC Address, Channel Frequency, RSSI values, Channel Number, and more [11].

IV. Wireless Monitoring tools in case of Linux

In case of Linux Operating System a number of wireless tools are included itself in the operating system to troubleshoot the wireless network. Commands like iwconfig, iwlist, iwspy, iwpriv etc. with proper parameters can be used to manipulate the Wireless activities. Other tools which can be used for the said purpose are given below.

A. *tcpdump*

It is an open source tool that is automatically installed on various UNIX distributions. tcpdump tool uses libpcap library for capturing wireless traffic. This tool is also used for capturing data of other users of network. This tool has one limitation that it is a command line tool and it does not contain user friendly GUI [12].

B. *Kismet*

It is most widely used open source tool for wireless network. This tool can collect packets passively and can also detect hidden networks. It can detect both wireless clients as well as access points. It can capture the wireless traffic in a format which can be read with Wireshark, tcpdump and Airsnort tools. Multiple channels can be found out with the help of its channel hopping feature [13].

C. *AirSnort*

It is a popular wireless password cracking tool. This tool passively monitors the wireless traffic. It is free and open source tool for both Linux and Windows operating systems. It can be used for cracking the WEP key [14].

D. *Aircrack-ng*

Aircrack-ng tool can be used to find out the detail of a wireless network. The main use of this tool is to check the wireless network security. It can be used for wireless traffic capturing, checking Wi-Fi cards and also for checking the password strength [15].

V. Wireless Monitoring tools in case of Mac

Quality wireless monitoring tools in case of MAC operating system help users to choose suitable wireless network. Various wireless monitoring tools for MAC operating system are given below.

A. *KisMAC*

KisMAC is an open source Wi-Fi analyzer tool for Mackintosh operating system. This tool has many features similar to those of kismet. It can be used to display the information related to wireless network and this information can be used to troubleshoot the wireless network. KisMAC is supported by many cards like Apple's Airport, Airport extreme. It is also supported by the cards which support Mac OS. Main features of KisMAC are:

a) It can reveal hidden/closed/cloaked SSID.

b) It also supports import and export of pcap files.

c) It can be used to find out the de-authentication attack.

d) It support 802.11b/g wireless network.

e) It can also display the information about the clients which are logged in [16].

B. *NetSpot Mac OS X*

This tool can quickly find out the nearby network. This tool can reveal the information about the channel. It can also reveal network name, SSIDs, signal strength and security settings of the network. NetSpot works in two modes: Discover and Survey. In Discover mode this tool can detect all the nearby networks. It can check the security settings of the network, channel number, signal and the operating band. In Survey mode, this tool can tell where the signal in the network is weak and where the signal is strong [17].

C. *WiFi Scanner*

It is a powerful wireless diagnostic tool in Mac OS. It can also tell about the networks which are not broadcasting their name. It can reveal wireless network name, channel number, SSID, protocols and network security. It can also be used for capturing the wireless traffic [18].

D. *WiFi Explorer*

This tool has a simple and user friendly interface. It can reveal SSID, BSSID channel number, security information, band, country code and much more. With the help of this tool users can easily identify the channel conflicts and signal overlapping problems. It is a very handy tool for small offices and homes. It can also display information about the hidden networks [19].

VI. Analysis and Discussion

Packet sniffers are valuable tools for network administrators. They can be used for the following purposes a) to investigate and analyze the network problems b) detection of misuse of the network by both internal and external users c) monitoring network bandwidth utilization and network usage d) filtering the network traffic *e*) investigating network bottlenecks.

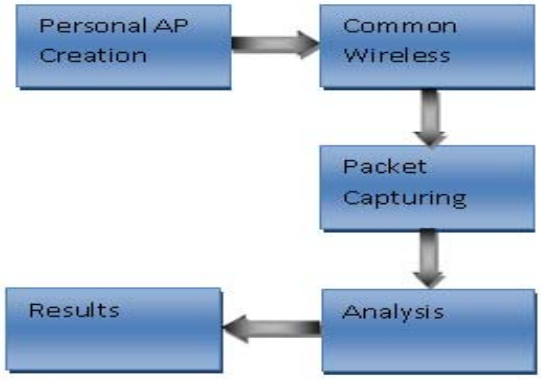

Fig. 2. Research Methodology Steps

A. *Research Methodology*

Main steps which are used are:

1) Personal AP creation for testing
2) Common Wireless Attacks conducted on this network
3) Traffic Capturing during various attacks
4) Analysis of Captured Packed
5) Findings of the Results

B. *Network Troublshooting*

Network operators often troubleshoot wireless issues related to wireless network, users and their devices. The main concerns are:

- Wireless connectivity problems of users
- Wireless connectivity problems related to AP
- Network Monitoring for checking wireless usage
- Performance checking of the wireless network

In this paper the following troubleshooting issues are checked with the help of the above discussed tools.

i) Signal Strength(Client Connectivity Problem)

Signal strength means signal power received by a wireless client. In majority of the tools signal strength is displayed in dBm and is expressed in negative values. Some of the tools discussed above use RSSI value to show the signal strength.After checking these values, a network administrator can find out if a client is receiving weak signal or strong signal and can make the proper adjustment so that client is able to receive the proper signal. Pictures given below show the Signal strength by different tools.

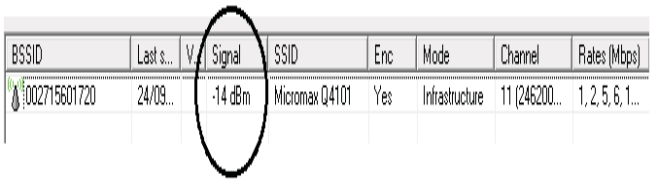

Fig. 3. Signal strength shown by Cain and Able

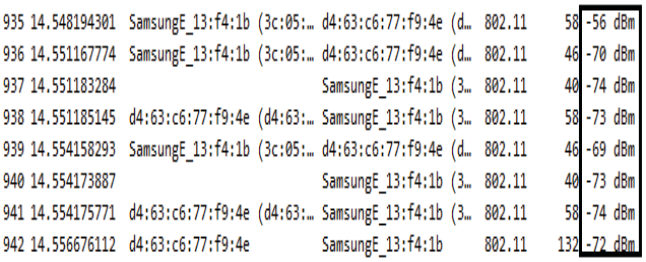

Fig. 4. Signal strength shown by Wireshark

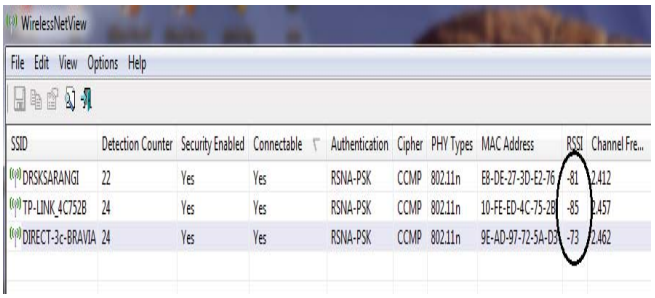

Fig. 5. Signal strength shown by WirelessNetView

Fig. 6. Signal strength shown by Aircrack-ng

ii) Capacity of the channel(Slow DaTransferProblem)

The capacity of the channel means speed of data transmission. With the help of these tools, network administrators can find out which users are communicating slowly and the reasons behind it. Most of the routers work in 2.4 GHz band. Channel 1, 6 and 11 are popular channel for this band because they do not overlap with each other. If many wireless clients and APs are working in the same channel, then there is interference. So using the above tools, we can find the channel where there is less interference. NetSpot's visualization feature [17] can display the channels with active networks.

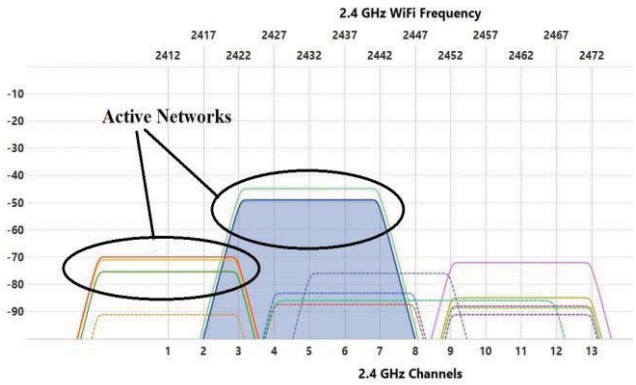

Fig. 7. Channel Capacity Shown by NetSpot tool

Figure shown below shows different BSSID's are working in different channel.

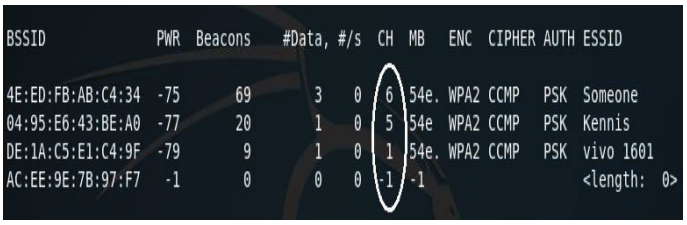

Fig. 8. Channel Number Displayed by Aircrack-ng Tool

Different channels shown by Kismet tool:

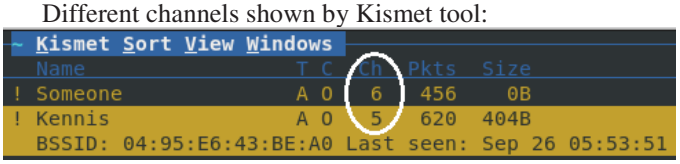

Fig. 9. Kismet tool

iii) Congestion Checking(Appearing/Disappearing of Wi-Fi signal continuously)

These tools can also be used to find out the congestion on the channels. As shown in the picture there are two devices which are working on channels number 1 and 11. In case if there are more clients working in the same channel, then this will lead to the congestion problem in the network. The picture given below shows two different BSSIDs is working in different channels.

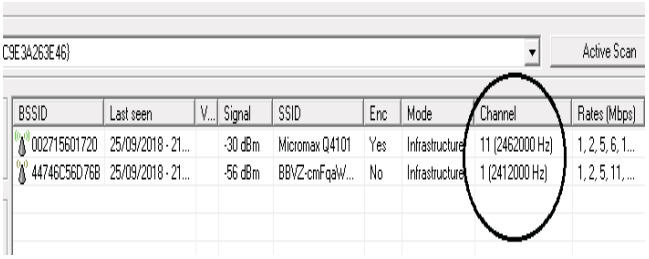

Fig. 10. Cain and Able

Snapshot shown below shows two wireless client devices are working on the same frequency band in case of kismet tool.

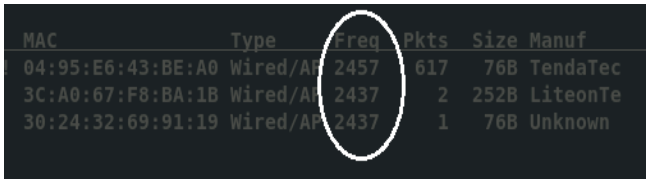

Fig. 11. Kismet tool displaying different frequency band

iv) Finding Overlapping Channels(Performance Problem)

Some of the tools discussed above can also be used to find out the overlapping channels in a given network. If wireless clients are working on the overlapping channels, then there is a decrease in the throughput of data transfer and performance of the networks will be dropped.

v) Wireless Authentication

With the help of these tools, network administrators can check whether there is proper authentication or not.

Network authentication in case of WirelessNetView tool is shown below:

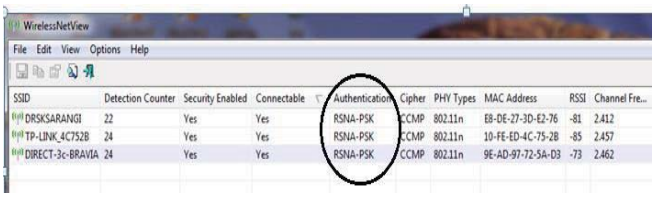

Fig. 112. WirelessNetView tool showing Authentication

Authentication in case of Cain and Able tool is shown below:

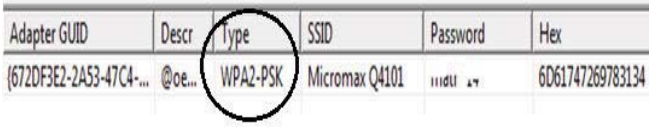

Fig. 12. Cain and Able tool showing Authentication

Aircrack-ng tool displays authentication as shown below:

Fig. 134. Authentication as shown by Aircrack-ng tool

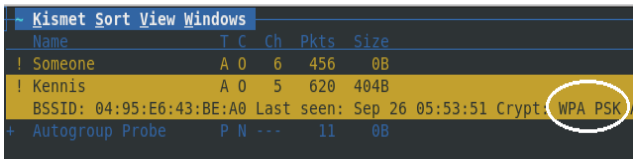

Fig. 145. Authentication in case of Kismet tool

vi) Proper Encryption of Data

These tools can also check whether the data is encrypted or not encrypted. Open air transmission of the data can be sniffed by the hacker and they can read it. But if the data is encrypted, it is still can be sniffed by the hackers but it cannot be read.

C. Wireless Threat Detection

Some of the tools discussed above can also be used to find the some common wireless threats. Main threats in case of wireless network are shown below in the Table I given below.

TABLE I. .LAYERWISE THREATS

Name of OSI Layer	Common Attacks
APPLICATION Layer	SQL Injection, Malware, Cross Site Scripting Attack
TRANSPORT Layer	TCP flooding, UDP flooding
NETWORK Layer	IP spoofing
MAC Layer	MAC Spoofing, MITM, Injection
PHY Layer	Eavesdropping, Jamming

Table II given below shows some common wireless threats. Network administrators can take the help of these tools to identify these threats.

TABLE II. DIFFERENT TOOLS FOR IDENTIFYING THE WIRELESS THREATS

S.N.	Name of Wireless Threat	Tools which can be used to detect them
1	RAP	Kismet, Wireshark, Acrylic, Network monitor
2	MITM	
3	DoS	
4	Replay Attack	
5	Jamming	

The picture given below shows the DoS attack with the help of de-authentication frames.

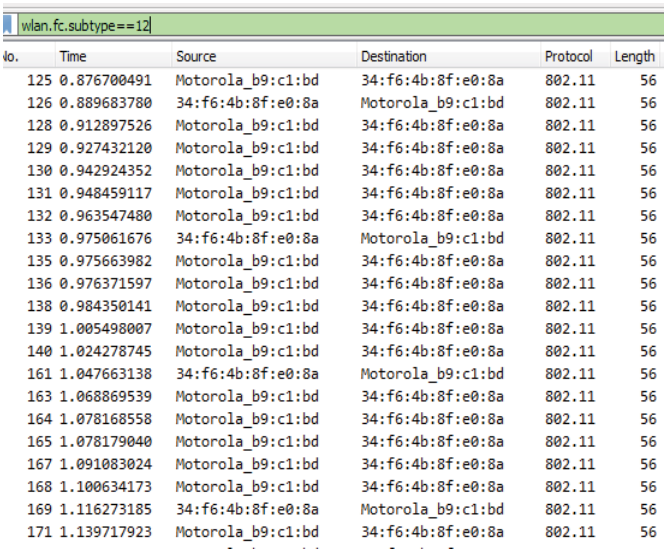

Fig. 156. Wireshark tool showing De-authentication frames.

VII. CONCLUSION

In this paper a number of packet sniffing tools are discussed. The majority of these tools are open source tools and freely available on the internet. With the help of these tools we can troubleshoot many network problems and we can also use them to identify wireless threats. In this paper wireless troubleshooting problems like internet connectivity problem, slow speed of the internet and congestion problems are discussed. A normal user can also take the help of these tools to rectify some of these problems. With respect to

wireless threats, these tools can be used to identify them and then proper measurements can be done to reduce them.

REFERENCES

[1] Li, Harry, and Guangjing Chen. "Wireless lan network management system." Industrial Electronics, 2004 IEEE International Symposium on. Vol. 1. IEEE, 2004.

[2] Oluwabukola, Otisule, et al. "A Packet Sniffer (PSniffer) application for network security in Java." Proceedings of the Informing Science and Information Technology Education Conference. Informing Science Institute, 2013.

[3] 'MargarateRouse,NetworkAnalyzer', [Online] Available: https://searchnetworking.techtarget.com /definition/network-analyzer

[4] 'Packetanalyzer', [Online]. Available: https://en.wikipedia.org/wiki/Packet_analyzer

[5] Gandhi,Charu,etal."Packet sniffer–a comparative study." International Journal of Computer Networks and Communications Security 2.5 (2014):179-187

[6] 'Wireshark', [Online]. Available: https://www.wireshark.org/

[7] 'Cainandabel', [Online]. Available: https://en.wikipedia.org/wiki/Cain_and_Abel_(software)

[8] 'Windows'[Online].Available: https://homedale.en.uptodown.com/windows

[9] 'Acrylicwifi',[Online].Available:https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/

[10] 'Wifi network monitor',[Online]. Available: https://securityxploded.com/wifi-network-monitor.php

[11] 'Wirelessnetworkview', [Online]. Available: https://www.nirsoft.net/utils/wireless_network_view.html

[12] 'Tcpdump', [Online]. Available: http://www.tcpdump.org/

[13] 'Kismetwireless.' [Online] Available: https://www.kismetwireless.net/

[14] 'Sourceforge', [Online]. Available: https://sourceforge.net/projects/airsnort/

[15] 'Aircrack', [Online].Available: https://www.aircrack-ng.org/

[16] 'Kismac', [Online].Available: https://en.wikipedia.org/wiki/KisMAC