EasyChair Preprint

№ 1583

Detection of Jammer enabled devices in the Wireless network

Dhruv Gajjar and Aditya Ranjan

October 6, 2019

Detection of Jammer enabled devices in the Wireless network

Author: - **Dhruv Rohitbhai Gajjar**

Guided by: - **Aditya R. Ranjan**

ABSTRACT

As a result of escalation in the development of various types of wireless technologies, most of the research is now days being done with respect to security in the network. When we talk about jammer, we are in a way discussing about DoS (Denial of Service) attacks in which a harmful enforced cyber-attack is carried out by sending number of messages with wrong addresses to flood the system.

Since jammers can block the system by jamming the various kinds of incoming signals like Bluetooth, or signals used for cell phones, GPS signals, etc. This might cause hindrance in your routine work. Therefore, it becomes necessary to search for the devices which are meant to jam the frequencies, and locate their position in the network. We need to either workout to turn off the jammer itself or a mechanism to notify the respective authorities to disable it.

Since, jamming is used to disorder the current wireless system by introducing signals of higher frequency to cause disturbance in the network at the physical layer. As jammer works opposite of data link layer to disconnect physical layer and network layer. Our location detector should be strong enough to detect at very first instance the strength of the Jammer enforced in the network. In order to find and locate the jammer, we need to know about the radio transmitter power, location where it is placed and the targeted network or system.

Jammers are usually undetectable in the system as users might have poor reception in case of mobile network jammers. Only after careful checking of the network they can be detected.

It sends the signals of various strengths in order to confuse the receptors. To trace and disable the enforced jammer in the network, we have managed to implement ways to detect such jammers by finding their location using the system MAC address and mapping it with the relative IP Addresses.

Objective: -

Solution to types of network devices, especially to wifijammer and international mobile sim card identification number (imsi) catcher desvice.

A low power jammer is dangerous as it can remain undetected in the network and can cause bigger harm than the powerful jammer which can be detected easily due to their harmful effects in the network.

For this we need to understand various types of jammers and the techniques that can be used to trace them in the network at the locations where they will work with utmost efficiency.

Introduction: -

What is Wi-Fi: -

Wi-Fi is a family of radio technologies that is commonly used for the wireless local area networking (WLAN) of devices which is based around the IEEE 802.11 family of standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing.

What is Wifijammer: -

Radio jamming is the deliberate jamming, blocking or interference with authorized wireless communications. In the United States, radio jamming devices are known as jammers. In some cases, jammers work by the transmission of radio signals that disrupt communications by decreasing the signal to noise ratio.

What is IMSI catcher device: -

An international mobile subscriber identity catcher, or IMSI-catcher, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. Essentially a fake mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man in the middle (MITM) attack.

IMSI number = MCC + MNC + LAC + Cell Id

MCC: - Mobile Country Code, it could be random 3-digit number. For Ex: - 405 & 404 is India Country Code.

MNC: - Mobile Network Code, it could be random 2 to 3-digit number. For Ex: - 24 is Gujarat State Idea company Number.

LAC: - Local Area Code, it could be random 1 to 5-digit number. For Ex: - 12345.

Cell Id: - Phone Id, it could be random 1 to 5-digit number. For Ex: - 23456.

Simulation: -

1) **Possible solution: -**

   a. **Mobile Telephone Switching Office (MTSO): -**

      Explanation: -

      The MTSO contains the switching equipment or Mobile Switching Center (MSC) for routing mobile phone calls. It also contains the equipment for controlling the cell sites that are connected to the MSC.

The system in the MTSO are the heart of a cellular system. It is responsible for interconnecting calls with the local and long distance landline telephone companies, compiling billing information (with the help of its CBM/SDM), etc. It also provides resources needed to efficiently serve a mobile subscribe such as registration, authentication, location updating and call routing. Its subordinate BSC/RNC are responsible for assigning frequencies to each call, reassigning frequencies for handoffs, controlling handoffs so a mobile phone leaving one cell (formally known as BTS)'s coverage area, can be switched automatically to a channel in the next cell.

All cellular systems have at least one MTSO which will contain at least one MSC. The MSC is responsible for switching calls to mobile units as well to the local telephone system, recording billing data and processing data from the cell site controllers.

The MSC is connected to a close telephone exchange by a trunk group. This provides an interface to the (Public Switched Telephone Network) (PSTN). It also provides connectivity to the PSTN. The region to be served by a Cellular Geographic Serving Area (CGSA) is split into geographic cells. These cells are ideally hexagonal in shape and they are initially laid out with their centers about 4 to 8 miles apart from each other. Other MTSO equipment, the cell site controllers provide control functions for a group of cell sites and actions of mobile phones through command and control data channels. To achieve this, there has to be a method of connectivity between the MTSO and the cell site. This may be by DS1, DS3, OCn or Ethernet circuits.

Therefore: -

Done by catching signals of imsi device or wifijammer.

We will try to catch by making base tower which also called MTSO.

If signals are weak so device, we are catching is far to us.

If signals are strong so device, we are catching is near to us.

b. Only possible solution for wifijammer: -

Carrier-sense multiple access with collision avoidance (CSMA/CA): -

Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple

access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be idle. When they do transmit, nodes transmit their packet data in its entirety.

It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.

Explanation: -

The jam signal or jamming signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations of the collision and that they must not transmit.

The maximum jam-time is calculated as follows: The maximum allowed diameter of an Ethernet installation is limited to 232 bits. This makes a round-trip-time of 464 bits. As the slot time in Ethernet is 512 bits, the difference between slot time and round-trip-time is 48 bits (6 bytes), which is the maximum jam-time.

This in turn means: A station noting a collision has occurred is sending a 4 to 6-byte pattern composed of 16 1-0 bit combinations. Note: The size of this jam signal is clearly beyond the minimum allowed frame-size of 64 bytes.

The purpose of this is to ensure that any other node which may currently be receiving a frame will the jam signal in place of the correct 32-bit MAC CRC, this causes the other receivers to discard the frame due to a CRC error.

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP. This leads to difficulties in medium access control sublayer since multiple nodes can send data packets to the AP simultaneously, which creates interference at the AP

resulting in neither packet getting through.

Although some loss of packets is normal in wireless networking, and the higher layers will resend them, if one of the nodes is transferring a lot of large packets over a long period, the other node may get very little goodput.

Practical protocol solutions exist to the hidden node problem. For example, Request To Send/Clear To Send (RTS/CTS) mechanisms where nodes send short packets to request permission of the access point to send longer data packets. Because responses from AP are seen by all the nodes can synchronize their transmissions to not interfere. However, the mechanism introduces latency, and the overhead can often be greater then cost, particularly for short data packets.

Therefore: -

Collision Avoidance: if another node was heard, we wait for a period of time (usually random) for the node stop transmitting before listening again for a free communications channel.

Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the shared the Access Point only issues a Clear to Send to one node at a time. However, wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions; they may turn it off completely, or at least not use it for small packets (the overhead pf RTS, CTS and transmission is too great for small data transfers).

Transmission: if the medium was identified as being clear or the node received a CTS to explicitly indicate it can send, it sends the frame in its entirety. Unlike CSMA/CD, it is very challenging for a wireless node to listen as the same time as it transmits (its transmission will dwarf any attempt to listen). Continuing the wireless example, the node awaits receipt of an acknowledgement packet from Access Point to indicate the

packet was received and check summed correctly. If such acknowledgement does not arrive in a timely manner, it assumes the packet collided with some other transmission, causing the node to enter a period of binary exponential backoff prior to attempting to re-transmit.

TOOLS: -

Wifijammer: -

https://github.com/DanMcInerney/wifijammer

IMSI catcher device: -

http://find-cell.mylinkov.org/

https://github.com/Oros42/IMSI-catcher

Software: -

http://ubuntuhandbook.org/index.php/2013/08/linssid-wifi-scanner-for-ubuntu-linux-mint/

Comparing CSMA/CA and CSMA/CD: -

1. **Carrier Sense Multiple Access with Collision Detection (CSMA/CD): -**

Process: -

The entire process of collision detection can be explained as follows: -

Step 1: - Start

Step 2: - K = 0

Step 3: - Apply one of the persistent methods (1-persistent, non-persistent, p-persistent)

Step 4: - Transmission done or Collision detected

If No: - Transmit and Receive

Else: -

Step 5: - Collision detected

If No: - Success

Else: -

Step 6: - Send a Jamming signal

Step 7: - K = K + 1

Step 8: - K > Kmax

If Yes: - Abort

Else: -

Step 9: - Choose a random number R between 0 and 2 ^ K – 1

Step 10: - Wait Tb time (Tb = R * Tp)

Step 11: - Back to Step 3

Notes: - K = number of attempts, Tp = max propagation time, Tb = Backoff time

Throughput and Efficiency: -

The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

For 1-persistent method throughput is 50% when G=1.

For non-persistent method throughput can go up to 90%.

2. Carrier Sense Multiple Access with Collision Avoidance (CSNA/CA): -

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if collision occurs. It can't be used by station to sense collision. Therefore, CSMA/CA has been specially designed for wireless networks.

These are three type of strategies: -

1. InterFrame Space (IFS): - When a station finds the channel busy, it waits for a period of time called IFS time. IFS can also be used to define the priority of station or a frame. Higher the IFS is the priority.
2. Contention Window: - It is the amount of time divided into slots A station ready to send frames chooses random number of slots as wait time.
3. Acknowledgements: - The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

Process: -

The entire process of collision detection can be explained as follows: -

Step 1: - Start

Step 2: - K = 0

Step 3: - Idle channel

If No: - Back to Step 3

Else

Step 4: - Wait IFS time

If No: - Back to Step 3

Else: -

Step 5: - Still idle

If No: - Back to Step 3

Else: -

Step 6: - Choose a random number R between 0 and 2 ^ k -1

Step 7: - Wait R slots

Step 8: - Send frame

Step 9: - Wait time-out

Step 10: - ACK Received

If Yes: - Success

Else: -

Step 11: - K = K + 1

Step 12: - K > Kmax

If Yes: - Abort

Else

Step 13: - Back to Step 3

Notes: - K = number of attempts, Tp = max propagation time, Tb = Backoff time

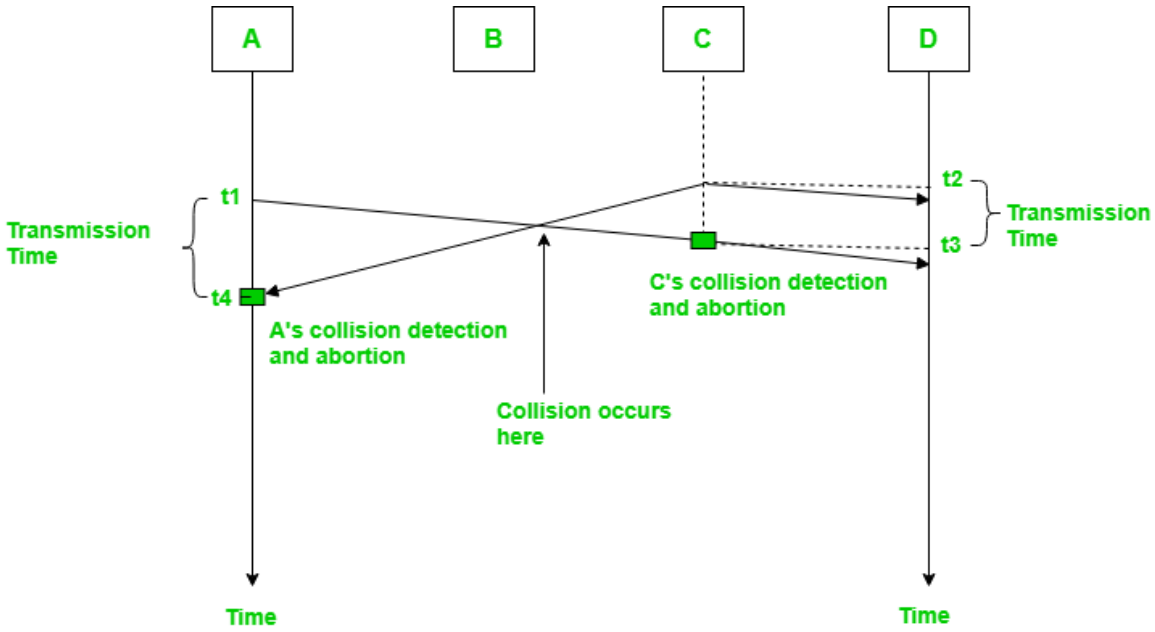
Earlier Work: -

Wifijammer: -

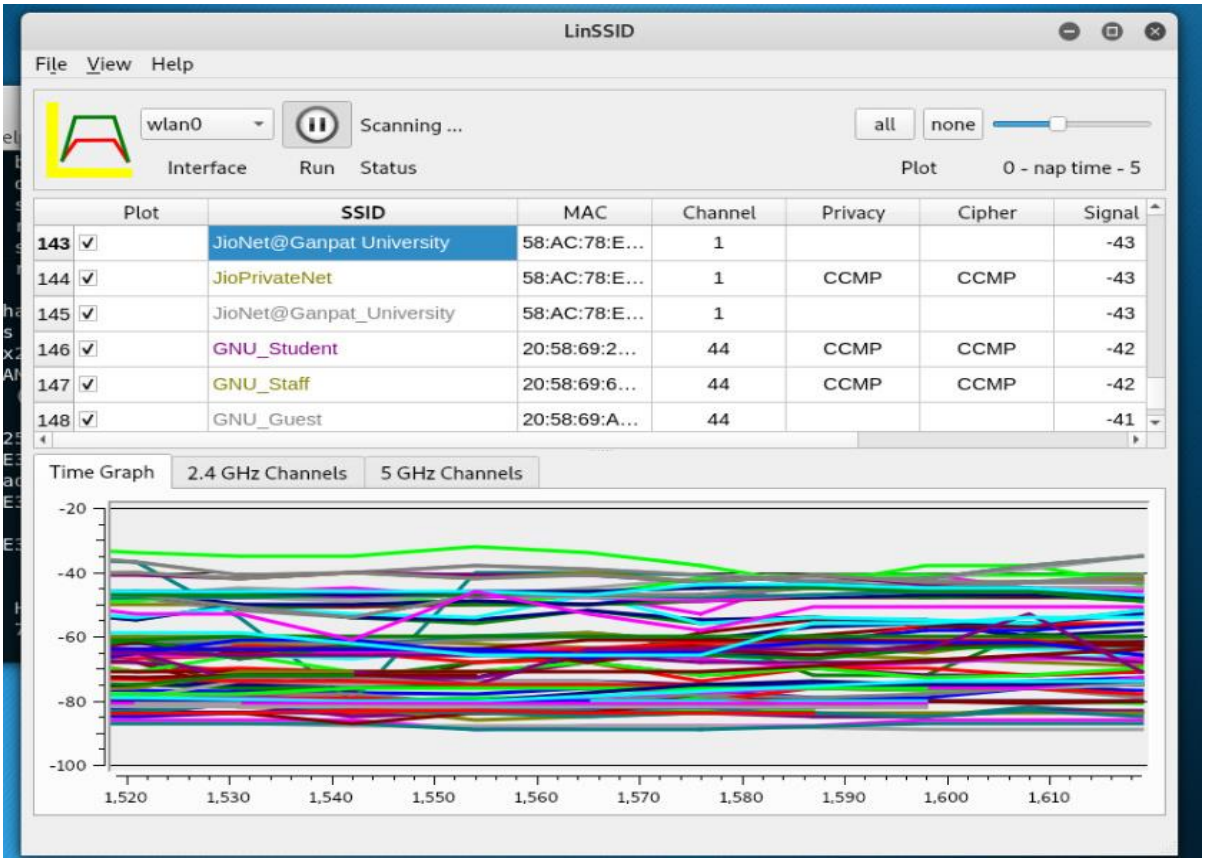
Raspberry Pie 3B Model with wlan adapter.

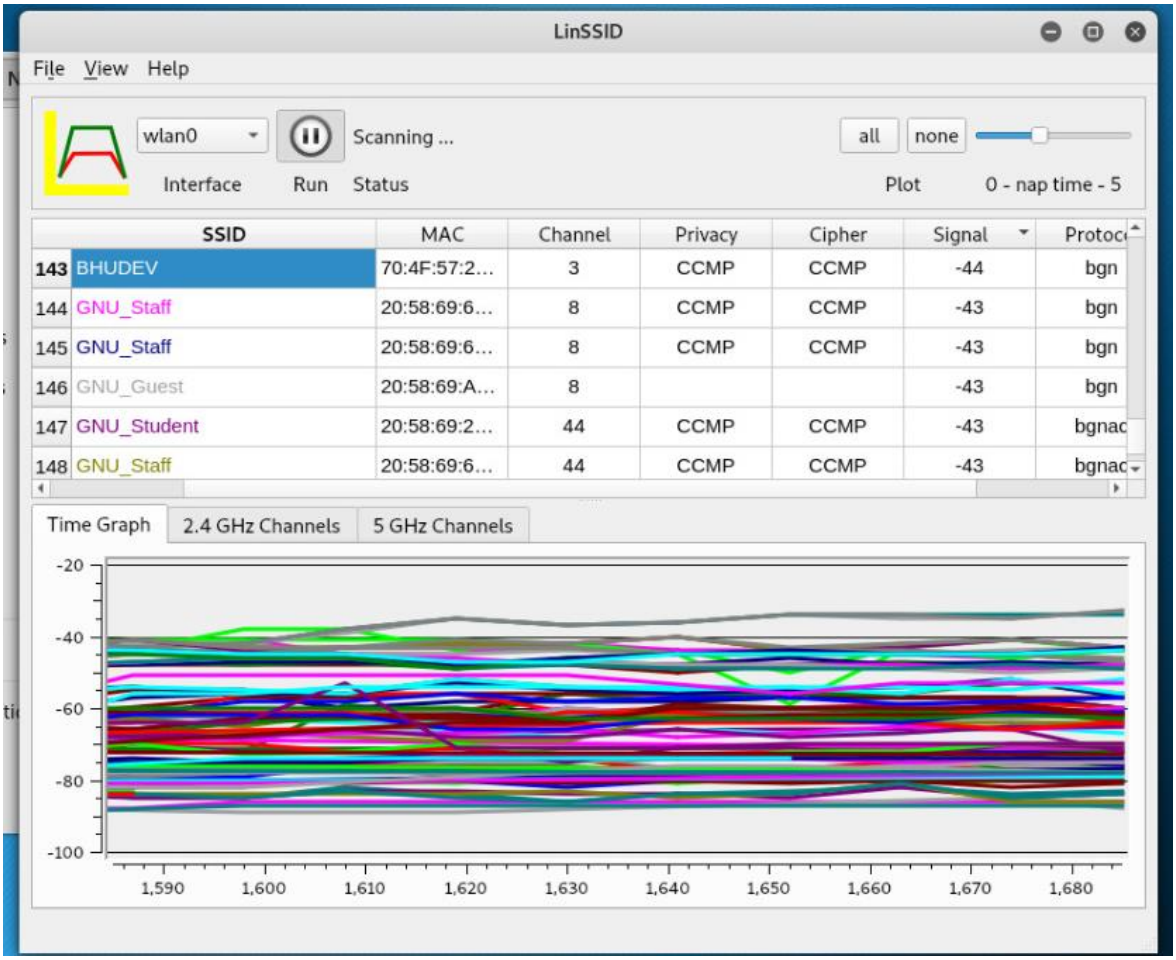
IMSI catcher device: -

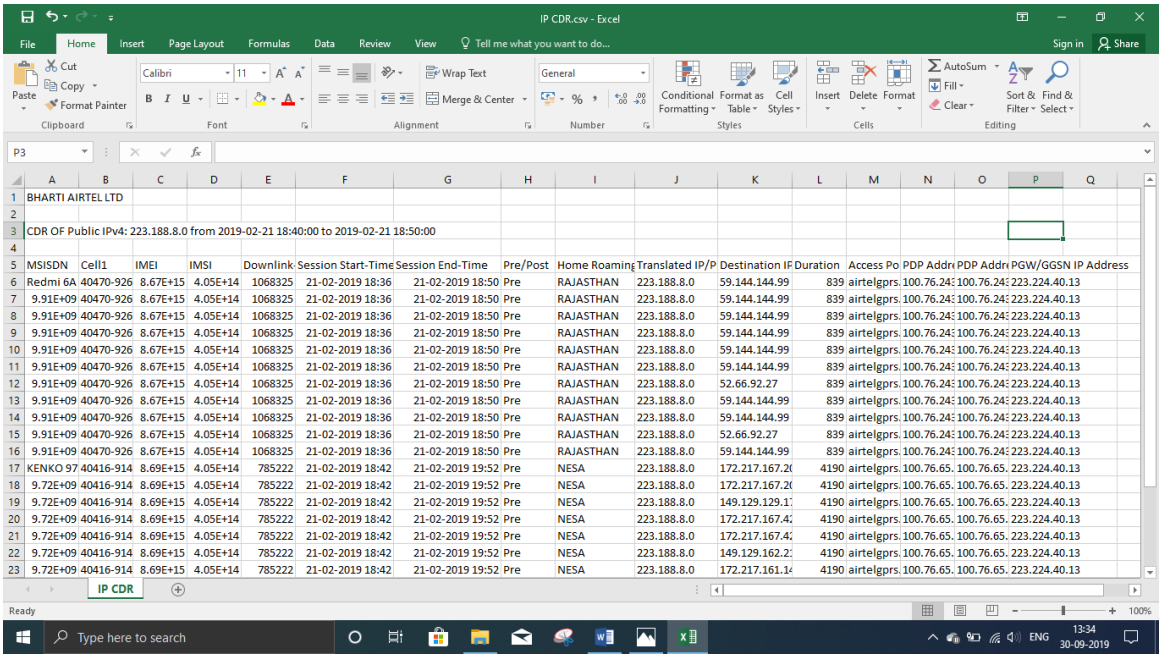
Done using websites and softwares.



In the diagram, A starts send the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is therefore collision detection and abortion and for A's frame is collision detection and abortion. So, the frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp). This can be deduced when two stations involved in collision are maximum distance apart.


LinSSID
File View Help
wlan0
Scanning ...
all
none
Interface
Run
Status
Plot
0 - nap time - 5
Plot
SSID
MAC
Channel
Privacy
Cipher
Signal
143 JioNet@Ganpat University 58:AC:78:E... 1 -43
144 JioPrivateNet 58:AC:78:E... 1 CCMP CCMP -43
145 JioNet@Ganpat_University 58:AC:78:E... 1 -43
146 GNU_Student 20:58:69:2... 44 CCMP CCMP -42
147 GNU_Staff 20:58:69:6... 44 CCMP CCMP -42
148 GNU_Guest 20:58:69:A... 44 -41
Time Graph
2.4 GHz Channels
5 GHz Channels
-20
-40
-60
-80
-100
1,520
1,530
1,540
1,550
1,560
1,570
1,580
1,590
1,600
1,610


LinSSID
File View Help
wlan0
Interface
Run
Scanning ...
Status
all
none
Plot
0 - nap time - 5
SSID MAC Channel Privacy Cipher Signal Protoc
143 BHUDEV 70:4F:57:2... 3 CCMP CCMP -44 bgn
144 GNU_Staff 20:58:69:6... 8 CCMP CCMP -43 bgn
145 GNU_Staff 20:58:69:6... 8 CCMP CCMP -43 bgn
146 GNU_Guest 20:58:69:A... 8 -43 bgn
147 GNU_Student 20:58:69:2... 44 CCMP CCMP -43 bgnac
148 GNU_Staff 20:58:69:6... 44 CCMP CCMP -43 bgnac
Time Graph
2.4 GHz Channels
5 GHz Channels
-20
-40
-60
-80
-100
1,590
1,600
1,610
1,620
1,630
1,640
1,650
1,660
1,670
1,680


IP CDR.csv - Excel
BHARTI AIRTEL LTD
CDR OF Public IPv4: 223.188.8.0 from 2019-02-21 18:40:00 to 2019-02-21 18:50:00
MSISDN Cell1 IMEI IMSI Downlink Session Start-Time Session End-Time Pre/Post Home Roaming Translated IP/P Destination IF Duration Access Po PDP Addr PDP Addr PGW/GGSN IP Address
Redmi 6A 40470-926 8.67E+15 4.05E+14 1068325 21-02-2019 18:36 21-02-2019 18:50 Pre RAJASTHAN 223.188.8.0 59.144.144.99 839 airtelgprs. 100.76.24 100.76.24 223.224.40.13
9.91E+09 40470-926 8.67E+15 4.05E+14 1068325 21-02-2019 18:36 21-02-2019 18:50 Pre RAJASTHAN 223.188.8.0 59.144.144.99 839 airtelgprs. 100.76.24 100.76.24 223.224.40.13
KENKO 97 40416-914 8.69E+15 4.05E+14 785222 21-02-2019 18:42 21-02-2019 19:52 Pre NESA 223.188.8.0 172.217.167.2 4190 airtelgprs. 100.76.65. 100.76.65. 223.224.40.13
9.72E+09 40416-914 8.69E+15 4.05E+14 785222 21-02-2019 18:42 21-02-2019 19:52 Pre NESA 223.188.8.0 149.129.129.1 4190 airtelgprs. 100.76.65. 100.76.65. 223.224.40.13
IP CDR
Ready
Type here to search
ENG
13:34
30-09-2019

Conclusion :-

The experimental process concludes that in order to detect the location of a wifi-jammer the entire process started with creation of a small network virtual private network (vpn) which could be either homogenous or heterogeneous followed by enabling the jammer. Now it was detected that entire network was jammed. Any upload or download process couldn't be done since jammer produced strong signals which created disturbance throughout the network. Hence none of the system network could work.

Second process started with Linssid (routine-software) which initialise the process of detecting media control address (mac) of all the systems in the network even the software could detect system having wifi-jammer enabled.

Third and final stage consist of detection of ip corresponding to mac address using ip cdr report. It could be done through commands manually but since we don't know the operator we used ip cdr report.

Reference :-

Practical Cloud Security A Guide for Secure Design and Deployment By :- Chris Doston

Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali By :- OccupyThe Web

Cyber Forensics By :- Dejey, Murugan

Computer Forensics and Cyber Crime: An Introduction, 2e By :- Britz

https://github.com/DanMcInerney/wifijammer

http://ubuntuhandbook.org/index.php/2013/08/linssid-wifi-scanner-for-ubuntu-linux-mint/

http://find-cell.mylinkov.org/

https://github.com/Oros42/IMSI-catcher

https://www.ip-tracker.org/