A PROJECT REPORT
ON

" GOVERNMENT POLYTECHNIC PEN PORTAL"

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQURIMENTS
FOR
THE AWARD OF
DIPLOMA IN
COMPUTER TECHNOLOGY

SUBMITTED TO
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI
SUBMITTED BY

Name of Students (Full name)	Enrolment No:
1. Snehal Rajan Gaikwad	2001290184

GUIDED BY:
Mrs. A. S. MORE
GOVERNMENT POLYTECHNIC, PEN
2022-2023

GOVERNMENT POLYTECHNIC PEN

CERTIFICATE

This is to Certify that the project report entitled "Wi-Fi Drone Jammer" was successfully completed by Student of sixth-semester Diploma in Computer Technology.

1. Snehal Rajan Gaikwad **2001290184**

in partial fulfilment of the requirements for the award of the Diploma in Computer Technology and submitted to the Department of Computer Technology of Government Polytechnic Pen work carried out during a period for the academic year 2022-23 as per the curriculum.

Mrs. A. S. MORE
Guide

Smt. S. P. Ambavane
HOD

External Examiner

Dr. S. S. Bhamare
Principal

ACKNOWLEDGEMENT

We have taken a lot of effort into this project (Wi-Fi Drone Jammer). However, it would not have been possible without the kind support and help of many individuals and our project guide. We would like to extend our sincere thanks to all of them.

We are highly indebted to **Mrs. A. S. MORE** for her guidance and constant supervision and for providing necessary information regarding the project and the support of the project.

We would like to express our gratitude to **Smt. S. P. AMBAVANE** (HOD of the Computer Technology Department) for her kind co-operation and encouragement which helped us in this project.

We would like to express our special gratitude and thanks to all the teaching and nonteaching staff members of the computer department for giving us such attention and precious time.

Our thanks and appreciations also go to people who have helped in developing the report and people who have willingly helped us out with their abilities and technical skills.

Project Team:

1. Tanmay Kishor Gangurde
2. Snehal Rajan Gaikwad
3. Pranav Arun Jadhav
4. Samruddhi Dilip Pawar

CONTENT

List of Diagrams:

List of Requirement Tables:

List of Snapshots:

ABSTRACT

Unmanned Aerial Vehicles, often called drones or abbreviated as UAVs, have been popularised and used by civilians for recreational use since the early 2000s. A majority of the entry-level commercial drones on the market are based on a Wi-Fi connection with a controller, usually a smart phone. This makes them vulnerable to various Wi-Fi attacks, which are evaluated and tested in this thesis, specifically on the Amitasha Foldable Drone. Several threats were identified through threat modelling, in which a set of them was selected for penetration testing.

The utilization of Internet-of-Things (IoT) innovation is developing exponentially as more shoppers and organizations recognize the benefits offered by the savvy and shrewd gadgets. The major purpose of this paper arose due to the reason that since drone innovation is a quickly rising segment inside the IoT and the danger of hacking couldn't just purpose an information break, it could likewise represent a noteworthy hazard to the open well-being. On account of their flexible applications and access to ongoing data, commercial drones are used across a wide variety of smart city applications. However, with many IoT devices, security is frequently an untimely idea, leaving numerous drones helpless against programmers.

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW:

Unmanned aerial vehicles (UAVs), when an apparatus utilized distinctly by the military, is currently ending up progressively well-known with the business and non-business showcase. Unmanned aerial (UAVs) vehicles, or drones, are an unmanned aerial vehicle that has no pilot ready, and are explored by either a remote control, or by ready PCs. Drones are normally partitioned into three unique sorts of classes: (a) recreational, (b) business and (c) military drones. The expansion of recreational drone usage has prompted discourses in regards to the security of the unregulated drone usage, and how to maintain a strategic distance from specialist abusing airspace rules. At a similar time as buyers utilized drones as specialists, organizations have progressively investigated utilizing rambles for business use.

1.2 AIM and OBJECTIVE:

- Research and development of a jamming technology that can effectively disrupt Wi-Fi signals used to control drones.
- Designing and building a portable, easy-to-use device that can be deployed quickly and effectively.
- Testing and refining the Wi-Fi drone jammer to ensure that it can disable Wi-Fi signals in a range of environments and conditions.
- Ensuring that the device complies with legal and ethical considerations, such as not interfering with emergency communications or causing harm to individuals or property.

1.3 Problem statement:

Increasing use of drones for malicious purposes such as espionage, smuggling, or terrorism. Drones can be difficult to detect and track, and their small size and manoeuvrability make them a potential threat to critical infrastructure, national security, and public safety.

While various counter-drone technologies exist, the use of Wi-Fi signals to control drones has become increasingly prevalent, and current solutions may not be effective against this type of technology. Therefore, there is a need for a specialized device that can disrupt Wi-Fi signals used to control drones, especially in sensitive areas where drone activity poses a threat.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION:

In 2016 they uncovered that they were trying a conveyance administration where clients could get little bundles up to five pounds in weight with-in 30 minutes or less, using rambles. The expanded use of drones implies that they will end up being a progressively regular objective for malevolent aggressors. In 2017, McAfee Labs referenced "Drone Hacking" as one of the greatest forthcoming dangers in their 2017 Threats Predictions Report. In situations where drones are delivering products, the automations need to not just have dependable well-being techniques for its activities; it additionally needs solid framework security estimations. The use of unmanned aerial vehicles (UAVs), commonly referred to as drones, has grown exponentially in recent years. While drones have numerous applications in areas such as photography, agriculture, and delivery services, they also pose significant security risks. Drones can be used for malicious purposes such as espionage, smuggling, or terrorism, and their small size and manoeuvrability make them difficult to detect and track.

2.2 EXISTING SYSTEM:

Signal Attenuation: One approach is to use signal attenuation, which involves introducing noise into the Wi-Fi signal, thus reducing its strength and preventing the drone from receiving the commands from the operator. This can be achieved through the use of broadband or narrowband jammers, which create interference in a wide or narrow frequency range, respectively.

Frequency Hopping: Another technique involves frequency hopping, which involves rapidly switching between different frequencies to prevent the drone from establishing a stable connection. This technique can be implemented through spread spectrum technology or frequency agile transmitters.

Directional Antennas: A third approach is to use directional antennas, which focus the jamming signal in a specific direction to target a specific drone. This technique can also be used to minimize interference with legitimate Wi-Fi networks in the surrounding area.

2.3 PROPOSED SYSTEM:

One approach could be to use a directional antenna array that can target specific drones while minimizing interference with other wireless devices. The jamming signal could be generated using a frequency agile transmitter that can rapidly switch between different frequencies, making it difficult for the drone to establish a stable connection. Additionally, the device could incorporate artificial intelligence (AI) and machine learning algorithms to analyze the drone's behavior and adjust the jamming signal accordingly.

To ensure the device does not interfere with legitimate Wi-Fi networks or emergency communications, it could be designed to operate on specific frequencies and power levels, as well as incorporating geofencing technology to limit its use to specific areas. The device could also include a detection system that can identify nearby drones and alert the user to their presence.

CHAPTER 3

SCOPE OF THE PROJECT

3.1 Scope of project:

The project can also involve researching and analysing the different technologies used in Wi-Fi drone jammers, including signal attenuation, frequency hopping, and directional antennas, as well as exploring their advantages and limitations. The project can also examine the legal and ethical considerations associated with the use of Wi-Fi drone jammers, including regulatory guidelines, privacy concerns, and the impact of jamming on other wireless devices.

To ensure the project's success, it would be necessary to work with experts in the field of wireless communications and drone technology. The project team would also need to conduct extensive testing and evaluation of the device to ensure its safety and effectiveness in a variety of real-world scenarios.

Overall, the scope of a Wi-Fi drone jammer project is broad, encompassing both technical and ethical considerations. The project's success would depend on the team's ability to design and build a jamming system that is effective, reliable, and compliant with legal and ethical guidelines, while also minimizing the potential risks to other wireless devices and individuals.

CHAPTER 4

METHODOLOGY

4.1 Study of system:

A Wi-Fi deauthentication attack is a type of cyber-attack that targets wireless networks, specifically those using the IEEE 802.11 standard, commonly known as Wi-Fi. The attack involves sending deauthentication packets to a Wi-Fi access point or client, which disrupts the connection between the two, effectively cutting off their communication.

Deauthentication packets are a type of management frame used in Wi-Fi networks to notify clients and access points that a user has disconnected from the network. However, in a deauthentication attack, an attacker sends a high volume of these packets to the access point or client, causing them to become overwhelmed and unable to communicate with each other.

4.2 Technology used:

1. **Wireless Network Adapter:**
   A wireless network adapter is a hardware device that enables a computer to connect to wireless networks. To perform a deauthentication attack on a drone using Kali Linux, a wireless network adapter that supports monitor mode and packet injection is required. Monitor mode enables the adapter to capture all wireless network traffic, while packet injection allows the adapter to send custom packets, including deauthentication packets.

2. **Aircrack-ng Suite:**
   The Aircrack-ng suite is a set of tools for wireless network monitoring, analysis, and penetration testing. It includes tools for packet capture, network analysis, password cracking, and more. The Aircrack-ng suite is commonly used for wireless network security testing and is pre-installed in Kali Linux.

3. **Airmon-ng:**
   Airmon-ng is a command-line tool that is part of the Aircrack-ng suite. It is used to enable monitor mode on a wireless network adapter. Monitor mode enables the adapter to capture all wireless network traffic, including the deauthentication packets used in a deauthentication attack.

4. **Airodump-ng:**
   Airodump-ng is another command-line tool that is part of the Aircrack-ng suite. It is used to capture wireless network traffic and display information about the networks and devices that are active in the area. Airodump-ng can be used to identify the wireless network of the target drone, which is necessary to perform the deauthentication attack.

5. **Aireplay-ng:**
   Aireplay-ng is a command-line tool that is part of the Aircrack-ng suite. It is used to generate and send custom packets, including deauthentication packets. Aireplay-ng can be used to start the deauthentication attack on the target drone, by sending a high volume of deauthentication packets to its wireless network, causing it to disconnect from the network.

6. **Kali Linux:**

   Kali Linux is a Debian-based Linux distribution designed for digital forensics, penetration testing, and security auditing. It was developed and is maintained by Offensive Security, a cybersecurity training company.Kali Linux includes a wide range of security tools, such as network scanners, vulnerability analysis tools, password cracking tools, and wireless networking tools. The tools are organized into various categories based on their function and can be accessed from a command-line interface or a graphical user interface.

7. **Virtual Machine:**

   A virtual machine (VM) is a software emulation of a computer system that enables a physical computer to run multiple operating systems or applications simultaneously, each in its own isolated environment.A virtual machine is created by allocating a portion of the physical computer's hardware resources, including CPU, memory, storage, and networking, to the virtual machine. The virtual machine runs its own operating system, independent of the physical computer's operating system, and behaves as if it were a separate physical machine.

8. **Virtual Box:**

   Oracle VM VirtualBox, commonly known as VirtualBox, is a free and open-source virtualization software package developed by Oracle Corporation. It allows users to run multiple operating systems (called "guest" operating systems) on a single physical computer (called the "host" operating system) simultaneously.VirtualBox supports a wide range of operating systems, including Windows, Linux, macOS, and Solaris. It can also run many other operating systems, such as OS/2, MS-DOS, and others. Users can create and configure virtual machines using a user-friendly graphical interface, or they can use command-line tools for advanced configurations.

4.3 REQUIREMENTS

SOFTWARE REQUIREMENTS:

Sr No.	Name of Software	Specification
1	Kali Linux ISO file	Version: 5.27 of KDE Plasma
2	Aircrack-ng Suite	Airmon-ng, Airodump-ng and Aireplay-ng
3	Virtual Box	Version: 6.1

HARDWARE REQUIREMENTS:

Sr No.	Name of Software	Specification
1	Computer System	Processor: Intel i-5 10300h Ram: 8gb Storage: 516gb SSD
2	Wifi Adapter	TL-WN722N
3	Drone	HQ Wifi, camera, remote control.

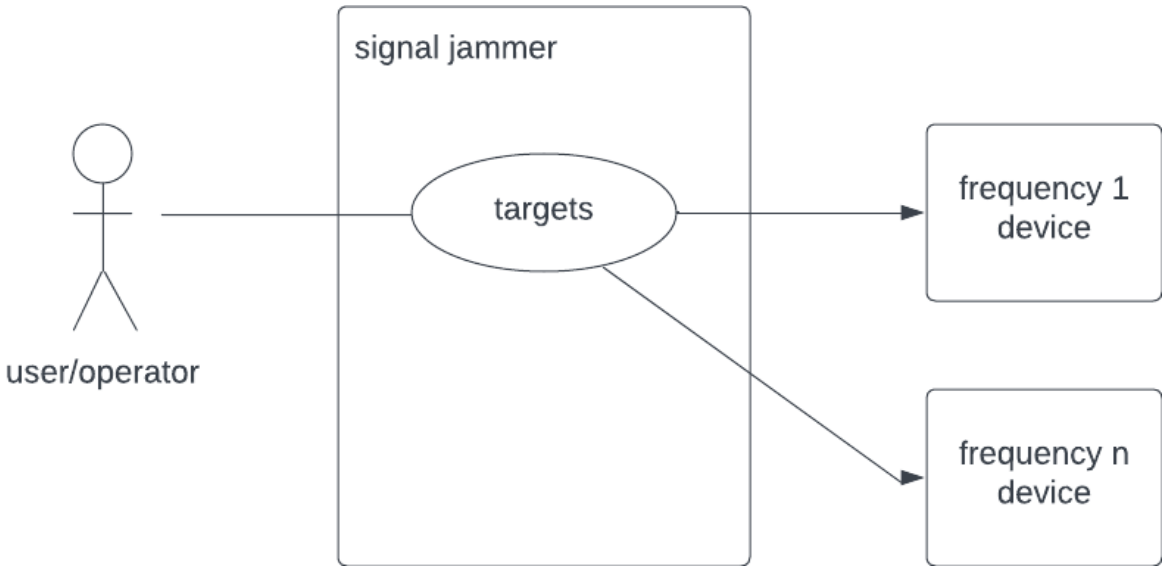
FINANCIAL REQUIREMENTS

SrNo.	**Name of Item**	**Specifications**
1.	Drone	Rs 4000/-
2.	Wifi Adapter	Rs 699/-
	Total =	Rs 4699/-

CHAPTER 5

DETAILS OF DESIGN, WORKING AND PROCESSES

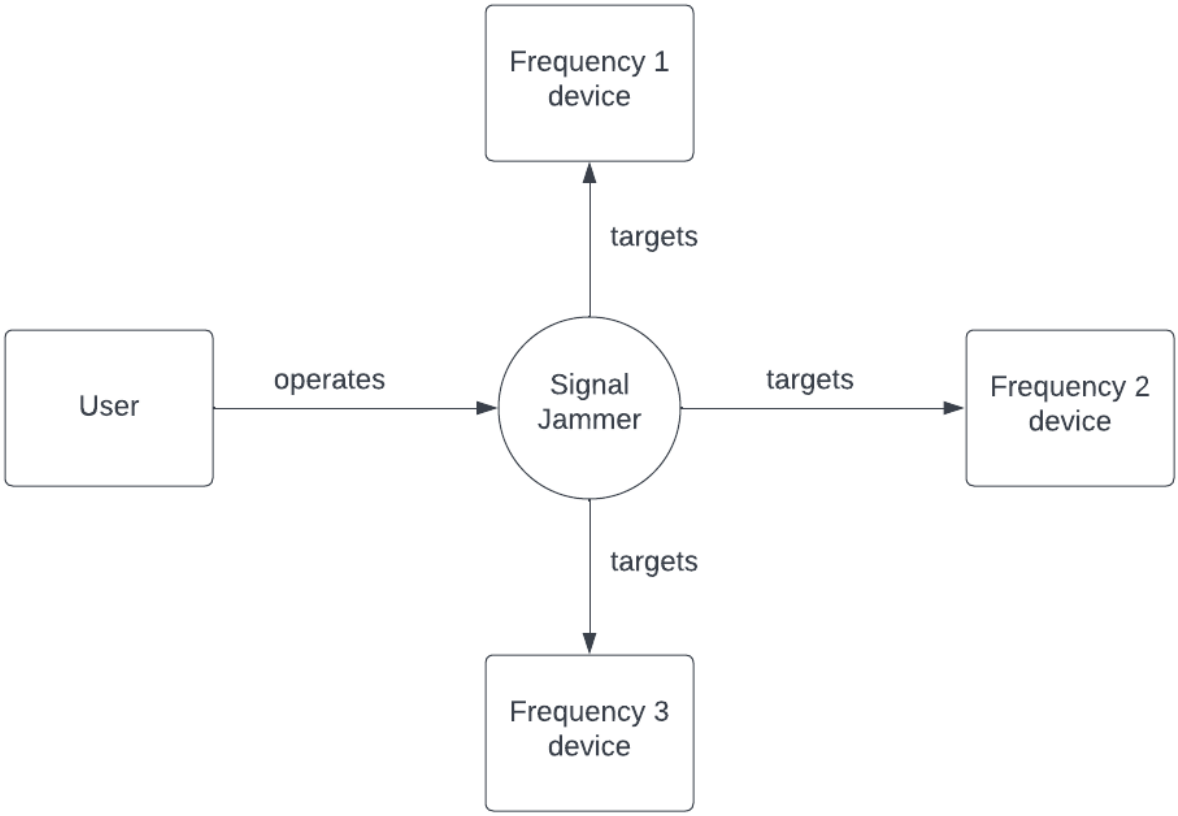
5.1 USE-CASE DIAGRAM



5.2 DFD DIAGRAM

DFD Level 0:

DFD Level 1:



5.3 ARCHITECTURE DIAGRAM

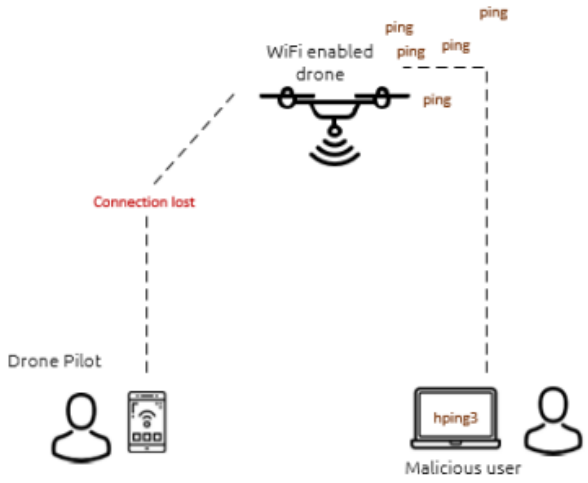


Fig. 6. Denial of Service attack where connection is lost due to ping flood.

5.4 SEQUENCE DIAGRAM

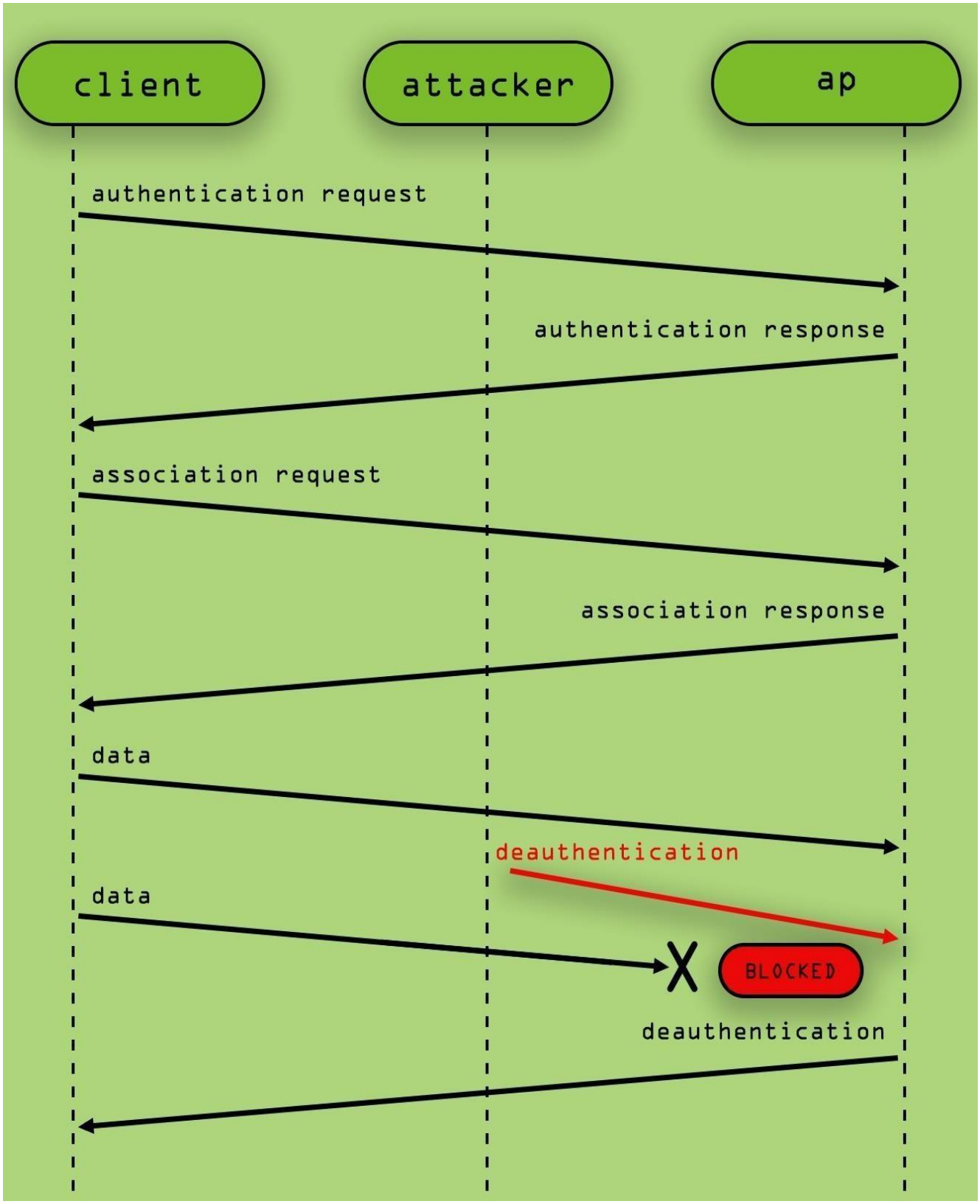
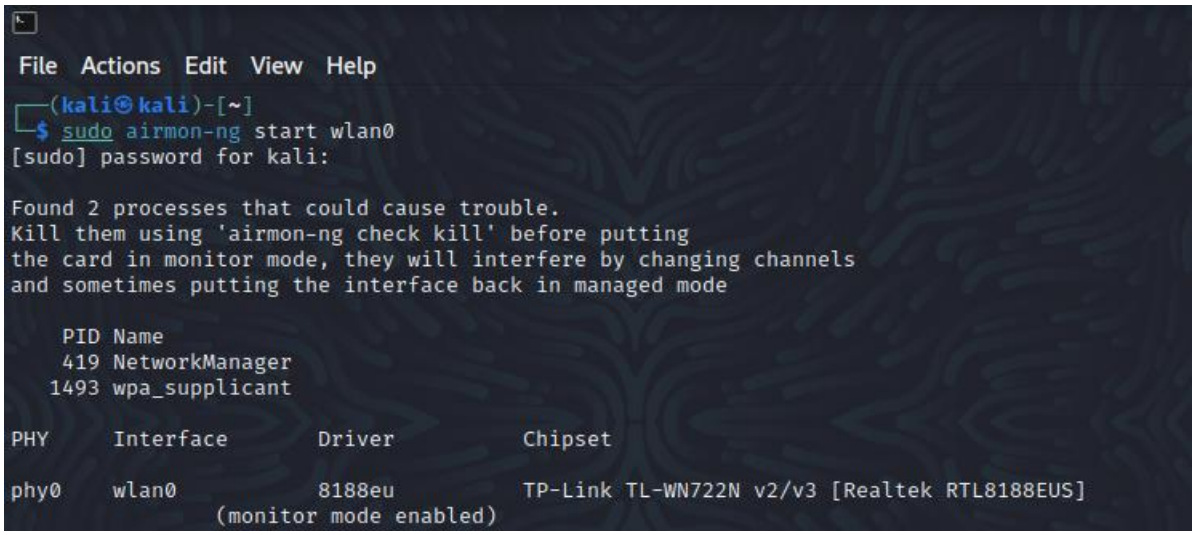


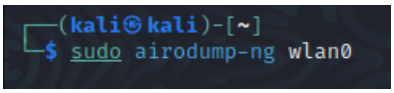
FIG: Active Process of Denial of Service attack to create loss of connection.

5.5 SCREENSHOTS

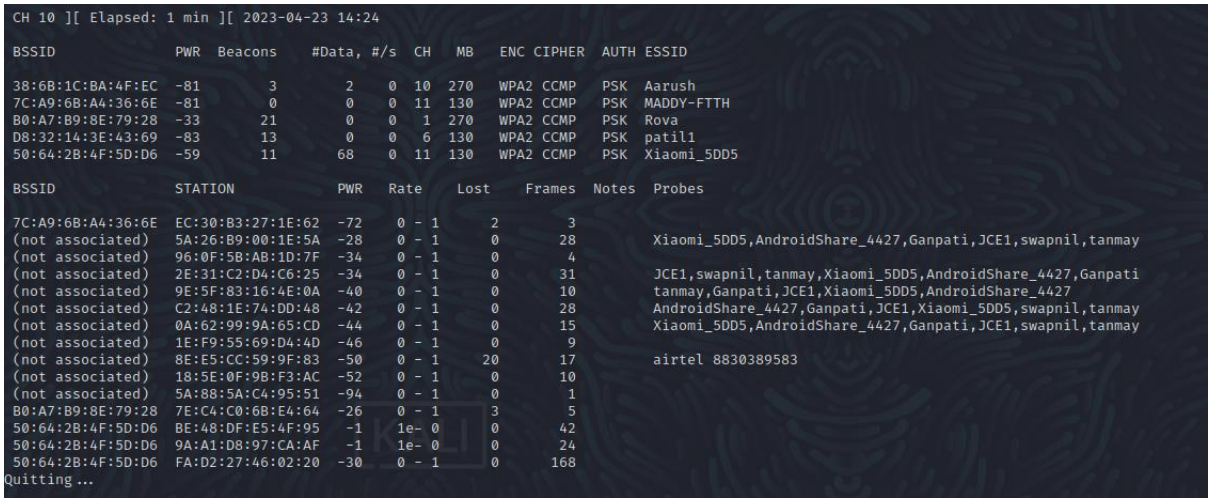
- **ACTIVATE WIFI ADAPTER TO MONITOR MODE:**



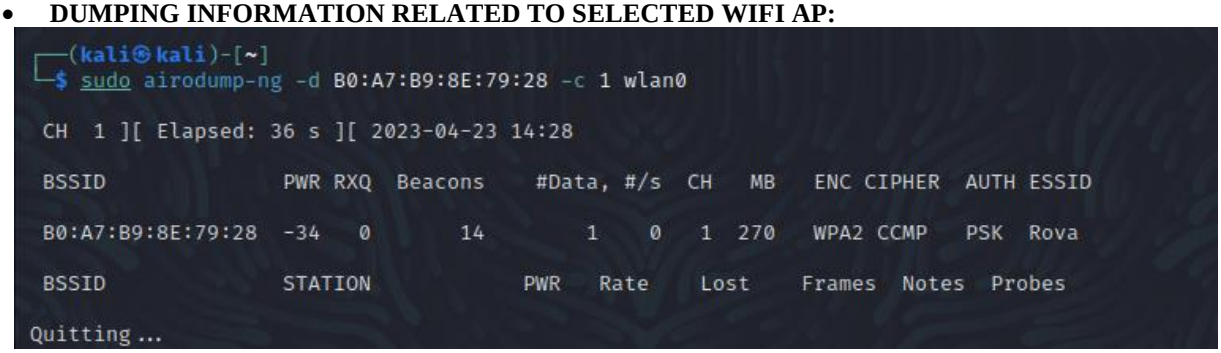
- **ACTIVATE SCANNING OF WIFI SIGNALS USING ADAPTER:**



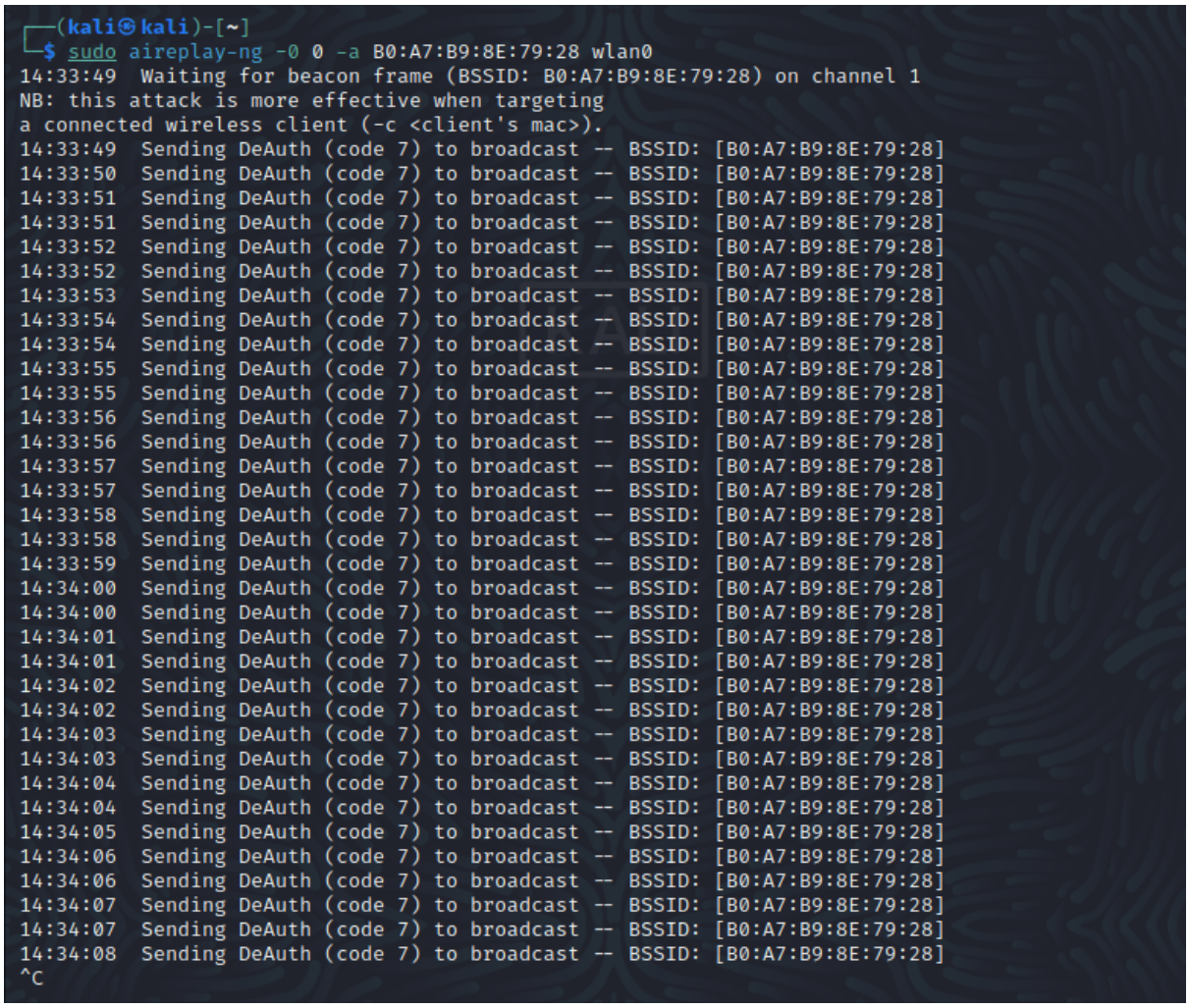
- **RESULTANT OF WIFI SCANNING:**



- **DUMPING INFORMATION RELATED TO SELECTED WIFI AP:**



- **LAUNCHING DEAUTHENTICATION ATTACK ON THE SELECTED MAC ADDRESS OF AP:**



5.6 WORKINGS

STEP 1:
To enable monitor mode on the interface, run "**airmon-ng start wlan0**".

STEP 2:
To find AP near us, run the "sudo airodump-ng wlan0" command.

STEP 3:
Select the Mac ID or BSSID of the AP you want to deaunthenticate. For this, use the command- "sudo airodump-ng -d B0:A7:B9:8E:79:28 -c 1 wlan0", This will give me the clients of our target AP.
We can see above the clients and their MAC addresses.

STEP 4:
Now run the following command to deauthenticate the AP and create high amounts of ping.
"sudo aireplay-ng -0 0 -a B0:A7:B9:8E:79:28 wlan0".
Here, -0 0 makes use of deauth attack(type 0) for duration of 0(infinity)
-a is our AP

5.7 TEST CASES

Test Case Id	Test Case Name	Objective	Steps	Expected Outcome	Actual Outcome	Status
TC001	Scan for wireless networks	Verify that airodump-ng can scan and list all the available wireless networks in range	Open the terminal and run the command ‘airodump-ngg wlan0	A table with a list of all the available wireless networks in range with BSSID channel and encryption type	The expected outcome is achieved	Pass
TC002	Caputure packets from a specific network	Verify that airodump-ng can capture packets from specific wirless network.	Open the terminal and run the command ‘airodump-ng--bssid AA:BB:CC:DD:EE:FF-w captured packet wlan0	A message indicating that packets are being captured and saved to the specified file	The expected outcome is acheived	Pass
TC003	Filter packets by specific criteria	Verify that airodump-ng can filter packets by a specific MAC address	Open the terminal and run the command ‘airodump-ng --bssid AA:BB:CC:DD:EE-w filtered packets --filter ‘src 00:11:22:33:44:55 wlan0	A message indicating that packets are being captured and saved to the specified file “filtered packets	The expected outcome is acheived	Pass
TC004	Display captured packets	Verify that airodump-ng can display captured packets	Open the terminal and run the command ‘airodump-ng --bssid AA:BB:CC:DD:EE-r captured-packets.cap	A table with a list of all the packets captured from the specified network including source and destination MAC addresses.	The expected outcome is acheived	Pass
TC005	Display summary statistics	Verify that airodump-ng can display summary statistics for multiple wireless networks	Open the terminal and run the command ‘airodump-ng --write summary_file--output-format csv wlan0	A message indicating that packets are being captured and saved to the specified file summary_file	The expected outcome is acheived	Pass
TC006	Deauthenticate a client	Verify that aireplay-ng can deauthenticate a client	Open the terminal and run the command ‘airplay-ng -0 5-a AA:BB:CC:DD:EE:FF-c 11:22:33:44:55 wlan0	A message indicating tha deauthentication packets	The expected outcome is acheived	Pass

		from a wirless network		are being sent to the client		
TC007	Injection Test	Verify that aireplay-ng can successfully inject packets into a wireless network	Open the terminal and run the command ‘airplay-ng -9 wlan0	A message indicating that the injection test was successful	The expected outcome is acheived	Pass
TC008	ARP request replay	Verify that aireplay-ng can perform an ARP request replay attack	Open the terminal and run the command ‘airplay-ng -3-b AA:BB:CC:DD:EE:FF-h 11:22:33:44:55 wlan0	A message indicating that the ARP request replay attack is in progress	The expected outcome is acheived	Pass
TC009	Fragmentation attack	Verify that aireplay-ng can perform a fragmentation attack on a wirless network	Open the terminal and run the command ‘airplay-ng -5-b AA:BB:CC:DD:EE:FF-h 11:22:33:44:55 wlan0	A message indicating that the fragmentation attack is in progress and that packets are being captured	The expected outcome is acheived	Pass
TC010	Deauthentication Attack Test	To test the ability of aireplay-ng to perform a deauthentication attack.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airodump-ng wlan0mon'. 3. Monitor the output for the target network's BSSID and channel. 4. Enter the command 'aireplay-ng -0 0 -a [target BSSID] -c [client MAC address] wlan0mon'. 5. Wait for the attack to complete.	The test should successfully deauthenticate the target client from the target network.	Actual outcome matches the expected outcome.	Pass
TC011	Enable Monitor Mode Test	To test the ability of airmon-ng to enable monitor mode on a wireless interface.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airmon-ng start wlan0'. 3. Monitor the output for a successful monitor mode activation.	The test should successfully enable monitor mode on the wireless interface.	Actual outcome matches the expected outcome.	Pass
TC012	Check Interface Status Test	To test the ability of airmon-ng to check the status of a wireless interface.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airmon-ng check wlan0mon'. 3. Monitor the output for any errors or warnings.	The test should report the status of the wireless interface as 'OK'.	Actual outcome matches the expected outcome.	Pass

TC013	Kill Processes on Interface Test	To test the ability of airmon-ng to kill processes using a wireless interface.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airmon-ng check kill'. 3. Monitor the output for any errors or warnings.	The test should successfully kill any processes using the wireless interface.	Actual outcome matches the expected outcome.	Pass
TC014	Disable Monitor Mode Test	To test the ability of airmon-ng to disable monitor mode on a wireless interface.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airmon-ng stop wlan0mon'. 3. Monitor the output for a successful monitor mode deactivation.	The test should successfully disable monitor mode on the wireless interface.	Actual outcome matches the expected outcome.	Pass
TC015	Check Wireless Drivers Test	To test the ability of airmon-ng to check the wireless drivers installed on the system.	1. Start Kali Linux and open a terminal. 2. Enter the command 'airmon-ng'. 3. Monitor the output for a list of installed wireless drivers.	The test should list all installed wireless drivers on the system.	Actual outcome matches the expected outcome.	Pass
TC016	Driver Installation Test	To test the ability of Kali Linux to detect and install the driver for the wifi adapter.	1. Plug the wifi adapter into the USB port. 2. Open a terminal and enter the command 'lsusb' to check if the adapter is detected. 3. Check the output of 'dmesg' for any driver-related messages.	The test should show that the wifi adapter is detected and the appropriate driver is installed.	Actual outcome matches the expected outcome.	Pass
TC017	Adapter Configuration Test	To test the ability of Kali Linux to configure the wifi adapter for use.	1. Plug the wifi adapter into the USB port. 2. Open a terminal and enter the command 'ifconfig -a' to check if the adapter is listed. 3. Enter the command 'iwconfig' to configure the adapter.	The test should show that the wifi adapter is configured and ready for use.	Actual outcome matches the expected outcome.	Pass
TC018	Connection Establishment Test	To test the ability of Kali Linux to connect to a wireless network using the wifi adapter.	1. Plug the wifi adapter into the USB port. 2. Open a terminal and enter the command 'iwlist wlan0 scan' to scan for available wireless networks. 3. Enter the command 'iwconfig wlan0 essid "network_name"' to connect to a network.	The test should show that Kali Linux is able to connect to the wireless network using the wifi adapter.	Actual outcome matches the expected outcome.	Pass
TC019	Signal Strength Test	To test the ability of Kali Linux to	1. Plug the wifi adapter into the USB port. 2. Open a terminal and	The test should show that Kali	Actual outcome matches	Pass

		detect the signal strength of a wireless network using the wifi adapter.	enter the command 'iwconfig wlan0' to check the signal strength. 3. Move to different locations and observe the change in signal strength.	Linux is able to detect the signal strength of the wireless network using the wifi adapter.	the expected outcome.	
TC020	Data Transfer Test	To test the ability of Kali Linux to transfer data over a wireless network using the wifi adapter.	1. Plug the wifi adapter into the USB port. 2. Open a terminal and enter the command 'ping -c 5 google.com' to test the internet connectivity. 3. Enter the command 'wget http://testurl.com/testfile' to download a test file.	The test should show that Kali Linux is able to transfer data over the wireless network using the wifi adapter.	Actual outcome matches the expected outcome.	Pass

CHAPTER 6

RESULTS AND APPLICATIONS

6.1 APPLICATION

There are several potential applications for a WiFi drone jammer, which is a type of jamming technology that targets the Wi-Fi signal used by drones to communicate with their remote controllers. Here are a few examples:

1) **Security:** WiFi drone jammers can be used to prevent unauthorized drones from entering restricted airspace or sensitive areas, such as airports, military bases, or other secure facilities. They can also be used to prevent drones from being used for spying or other malicious activities.

2) **Crowd control:** In crowded events, WiFi drone jammers can be used to prevent drones from flying too close to people, which could cause accidents or injuries**.**

3) **Privacy protection:** WiFi drone jammers can also be used to protect privacy by preventing drones from being used for surveillance or other intrusive activities.

4) **Wildlife conservation:** In some areas, drones can disrupt wildlife, disturb nesting sites, or interfere with animal behavior. WiFi drone jammers can prevent drones from entering sensitive wildlife areas and causing harm.

5) **Anti-terrorism:** WiFi drone jammers can also be used to prevent terrorist attacks. For example, drones can be used to deliver explosives or conduct surveillance, and jammers can prevent these activities.

CHAPTER 7

CONCLUSIONS AND FUTURE SCOPE

7.1 CONCLUSION

When a drone loses its Wi-Fi connection, it depends on the specific drone and the circumstances of the disconnection to determine what happens next. Here are a few possibilities:

1) **Autonomous drones:** Some drones are designed to continue operating autonomously even if they lose their Wi-Fi connection

2) **Manual control loss:** In some cases, losing the Wi-Fi connection means that the drone loses its ability to be manually controlled by the user.

3) **Return to home function:** Many drones have a "return to home" function that activates if the drone loses its Wi-Fi connection.

4) **Crash:** If the drone is flying too far away and too low when it loses its Wi-Fi connection, it may crash or be lost.

7.2 FUTURE SCOPE

As drones become increasingly popular and accessible, the need for effective drone jamming technology is also growing. Here are a few potential future applications for drone jamming technology:

1) **Security:** Drone jamming technology can be used to prevent unauthorized drones from entering restricted airspace, such as military bases, prisons, or other secure facilities. This technology can help to prevent security breaches and protect sensitive areas.

2) **Public safety:** In crowded areas such as sports events, concerts, or protests, drone jamming technology can help prevent drones from flying dangerously close to people, which could cause accidents or injuries.

3) **Anti-terrorism:** Drone jamming technology can also be used to prevent terrorist attacks. For example, drones can be used to deliver explosives or conduct surveillance, and jamming technology can prevent these activities.

4) **Protecting privacy:** Some people may feel uncomfortable with drones flying over their property or recording their activities. Drone jamming technology can prevent drones from flying in areas where they are not wanted or legally permitted.

5) **Wildlife conservation:** In some areas, drones can disrupt wildlife, disturb nesting sites, or interfere with animal behavior. Drone jamming technology can prevent drones from entering sensitive wildlife areas and causing harm**.**

CHAPTER 8

REFERENCES

8.1 REFERENCES

1. Ethical hacking and penetration testing using raspberry-pie, Maryna Yevdokymenko, Elsayyed Mohammed, Paul Onwuakpa Arinze Infocommunication Engineering department Kharkiv National University of radio electronics Kharkiv, Ukraine.

2. Early Detection of cybersecurity threats using collaborative cognition, Sandeep Narayan, Ashwinkumar Ganesan, Karuna Joshi and Tim Finn Department of Computer Science and Elelctronic engineering University of Maryland, Baltimore County, Baltimore, MD 2150, USA.

3. A Cyber-Defensive Industrial control system with redundancy and Intrusion detection. Dayne Robinson and Charles Kim Electrical engineering and Computer Science Howard University Washington DC: USA.