Portable Vulnerability Assessment System for Wireless as Data Transition Anomaly in IoT

A Project Report

Submitted by:

ABHISHEK SHARMA(2019643445)

UDIT PRABHAKAR (2018007643)

ASTHA AGARWAL(2018014082)

SHUBHAM KUMAR JHA (2018011469)

Submitted to

Mr. Avinash Kumar

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At

SHARDA UNIVERSITY

Knowledge Park III, Greater Noida, Uttar Pradesh 201310

DECLARATION

We hereby declare that the project "entitled **"Portable Vulnerability Assessment System for Wireless as Data Transition Anomaly in IoT"** submitted for the course of **Major Project-II (Project)** is our original work. We have referenced and properly cited the original sources. We declare that we have adhered to all principles of academic integrity and honesty and have not falsified or fabricated any source/idea/fact/data in the project submission. We also accept the fact that any violation of the above principles and guidelines can call for disciplinary action by the University and can evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken wherever required.

Signature of the Student(s)

Place: Sharda University, Greater Noida

Abhishek Sharma

Date: 9th May 2022

Udit Prabhakar

Shubham Kumar Jha

Astha Agarwal

CERTIFICATE

It is to certify that the work involved for completion of the above-listed project in the project report titled "**Portable Vulnerability Assessment System for Wireless as Data Transition Anomaly in IoT**" by "**Abhishek Sharma, Udit Prabhakar, Shubham Kumar Jha, Astha Agarwal**" has been fairly carried out under my able guidance and supervision and that this work is not submitted or published elsewhere.

Signature of the Guide

Place: Sharda University, Greater Noida

Date: 9th May 2022

ACKNOWLEDGEMENTS

We extend our heartfelt gratitude to Sharda University's authority, and our professor **“Mr. Avinash Kumar** for his guidance in completing our project successfully. Additionally, He’s put in his valuable efforts and knowledge and cooperated with us. We would like to acknowledge all the internet sources which helped in getting useful information to proceed with the project, at the right place. They were crucial in helping us learn the tools and approaches we needed to finish the application. A special thank you to the team, who contributed their talents, knowledge, dedication, and cooperativeness. We would also like to thank our parents for providing us with the necessary environment and criteria to make our work a success.

ABSTRACT

It is simple to take advantage of computer technologies such as WiFi, IoT, and Bluetooth. As a result, as a data transition anomaly in IoT, we want to create a portable vulnerability assessment system for wireless.It uses the Raspberry Pi 4, Bash Scripting, and Comprehensive Linux Os for automating existing manual technologies like laptops and Desktops. Users are achieving the requirements by enhancing day-to-day networks audit and vulnerability scanning easier.

It might result in a smoother user interface and a faster procedure with the aid of excellent configuration on a little device. It can help persons who work in cyber security. Rather of lugging a machine, it may be utilised to focus on their core tasks such as shell scripting, tool use, and so on. When compared to the manual command method through terminal, it will increase the time necessary to audit a network.Businesses may use it to detect weaknesses and vulnerabilities in their wireless networks.

The objective of this project is network discovery, WPA/WPA2 security code cracking, wi - fi intrusions like deauthentication / disassociation attack, mdk4 attack vectors, Deauthentication aireplay threats, as well as other obsolete and yet successful attacks like - Beacon packet flood attacks, Authentication Denial of Service attacks. Researchers may develop a Hardware-based Technology Cycle-based Hardware Testing like Information Transitions Abnormality on IoT to examine network and weaknesses like Poor Passwords, Less Writing Encryption like WPS, and WEP. To conduct out whatever assaults or eavesdrop on connected Pc or Mobile devices, researchers have to build tiny, lightweight, and transportable Computers with these autonomous features.

One of the key features researchers can add to start making the device quite developed and fascinating to use is the integration of devices to Mobile devices or Personal computers windows os via software like juice ssh and vnc technology to interconnect over the devices with the android mobile application for something like the ui of the deployed os on devices.

LIST of FIGURES

Table of Contents

1. INTRODUCTION

1.1. Problem Definition

The project's major goal is to audit the network using a Threat Intrusion Detection System using Wi-Fi as a Data Transition Anomaly in IoT, Capture Handshake, Perform wireless attacks such as deauthentication and mdk4 attacks, as well as certain ancient but successful attacks such as broadcasting beacon frames flooding attacks, spoofed de-authentication frames attacks, and Temporal key integrity protocol assaults attacks. The project is totally built with great care not to be exploited by anyone via attacks. The purpose of the project is to build a Hardware-based Cyber security Threat Intrusion Detection System with a Data Transition Anomaly in IoT to analyze the network and its weaknesses. The Purpose of the project is to build small, compact, and portable hardware to reduce the manual command entry in the terminal for performing any attack or audit via a Connected Mobile phone. Other software, such as VNC player, may be used to sync the graphical interface of a hardware-installed operating system with an Android application. You can connect the hardware with any android based operating system, any tablet, any laptop with SSH and Juice application which runs Terminal in android.

1.1.1 What is Wifi?

Wireless Fidelity is a wireless communication feature that enables computers (laptops and desktops), mobile devices (smart phones and accessories), as well as other devices to access the internet (printers and video cameras). Enables various devices, as well as others, to connect and form a network.

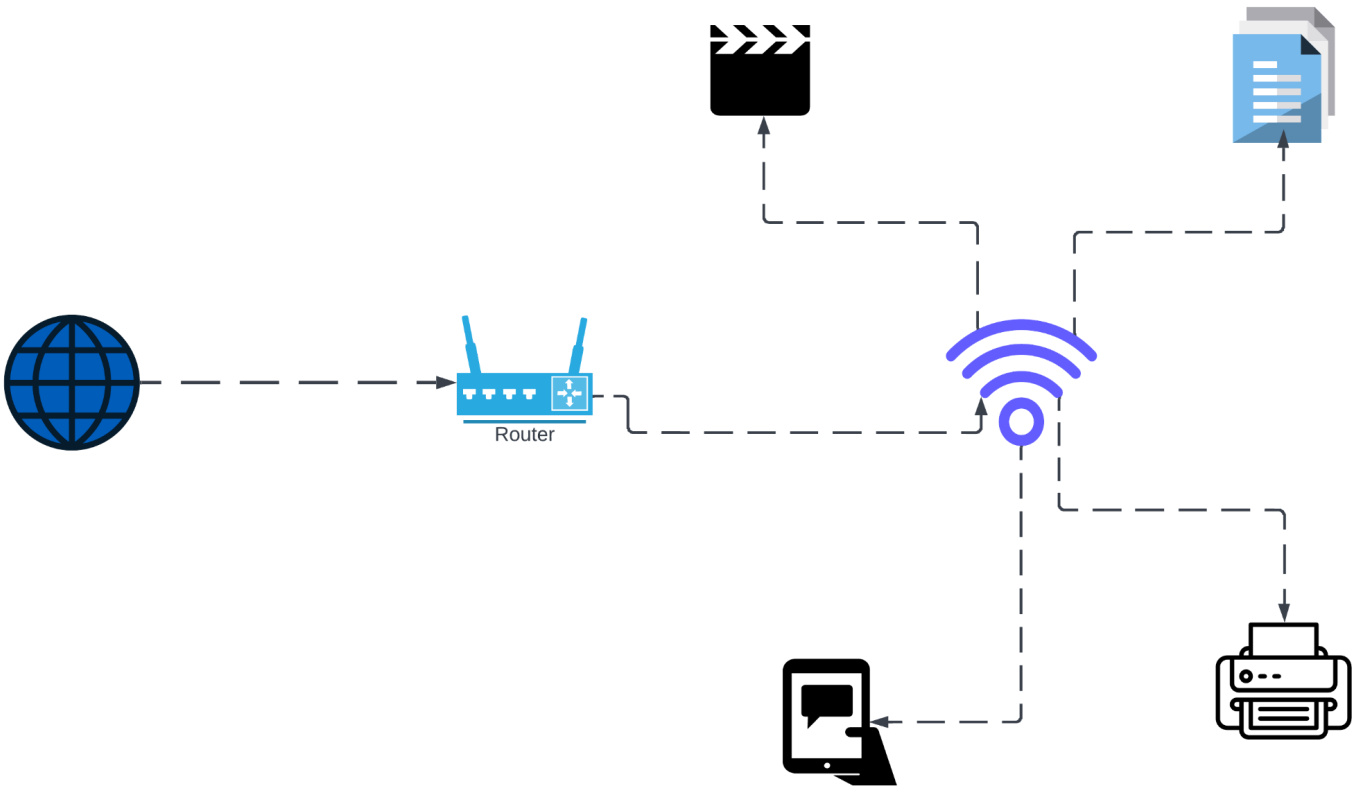


Fig.1 Diagram of Wi-fi

To connect to the internet, a wifi connection is used. Once you link to Wireless-Fidelity, you are equipped with wireless network, which allows all Wireless-Fidelity-enabled devices to access the Web.

What exactly is Wireless Fidelity Security?

Wireless-Fidelity security is indeed the technique of preventing unwanted people from entering a wireless connection. Furthermore, wireless security, often referred as Wi-Fi security, attempts to ensure that the data will be only available to authorized users.

Wireless protocols are intended to safeguard wireless networks used in homes and other types of buildings from hackers and unwanted users. As previously stated, there are four wireless safety systems, each with its own distinct power and capabilities. Wireless technologies encrypt private data while it is transferred over the air.

What are the types of Wireless-Fidelity Security?

The four types of Wireless-Fidelity security are :

- WEP
- WPA
- WPA 2
- WPA 3

What is Wired Equivalent Privacy?

The acronym "WEP" stands for Wired Equivalent Privacy, and it is also abbreviated as WEP. It is a security method designed to offer wireless networks with data privacy (or confidence). WEP (or Wired Equivalent Privacy) was included in the 802.11 specifications. One of the most significant aspects of Wired Equivalent Privacy is its 10 or 26 hexadecimal key, or 40 or 104 bits. Historically, these 40 or 104 bit devices were quite popular among users and were regarded as one of the greatest solutions for rodent control. However, Wired Equivalent Privacy (or WEP) was initially intended to offer a measure of protection for wireless networks, or WLANs.Although, the level of security provided by Wired Equivalent Privacy (or WEP) is similar to the level of security expected from a local wireless network. As its name implies, it transmits data through radio waves somewhere that fall within its range. So the main goal of Wireless Privacy is to add a layer of protection to wireless networks by providing strong data encryption. This way, the data will not be visible to any unwanted or unauthorized users, other than the intended recipient.

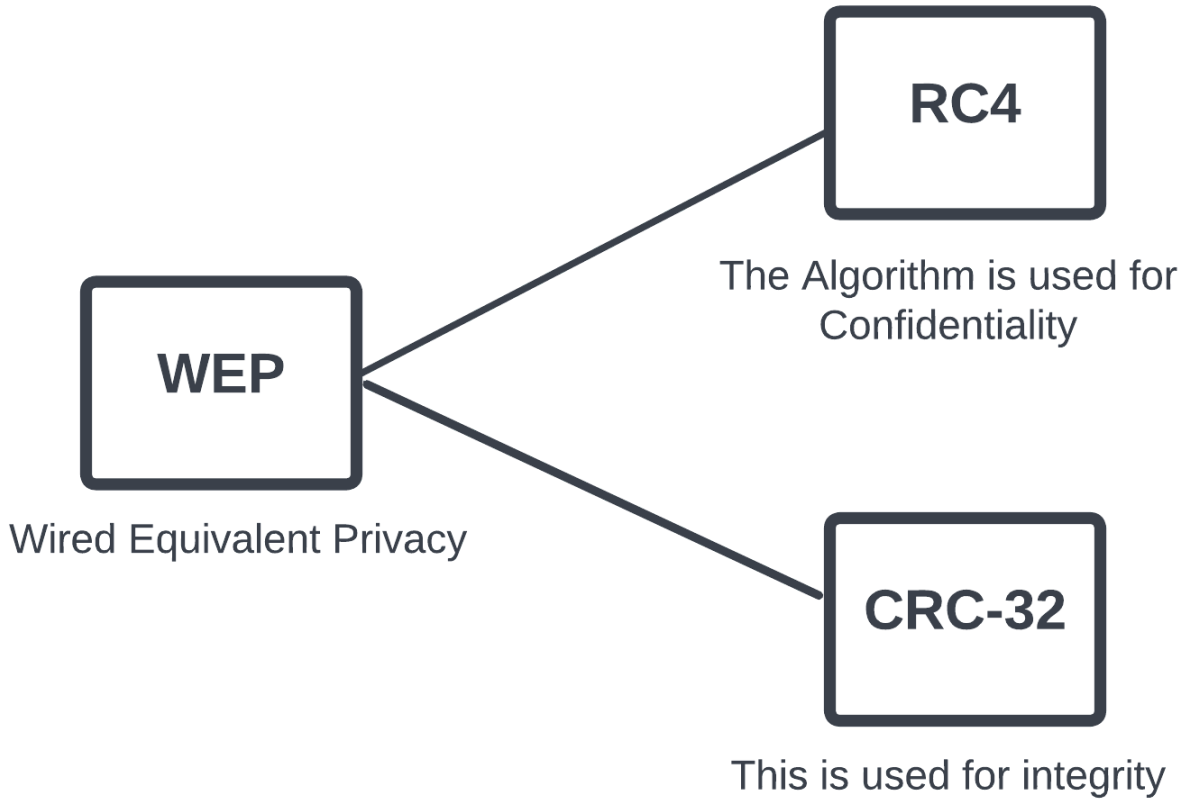


Fig.2 Encryption of WEP

What are the WEP Keys?

The main purpose of WEP is to protect and maintain the integrity of the data. For this it use two shared keys:

1. Unicast Session Key - It is a form of encryption key that is widely used to safeguard unicast communication between a wireless AP and a client (or user). It is called unicast because it can only deliver information or data between two points: (One sender and one recipient).

2. Multicast Key Which is also known as global key - The multicast key is also considered the world key. As its name suggests, it is used to protect multiple streaming traffic between one wireless AP and all of its other wireless clients. The term multicast is used because it can be used to transfer data between one sender and multiple recipients or between multiple senders and one recipient.

What is Wireless-Fidelity Protected Access?

Wireless-Fidelity Protected Access (WPA) is a well-developed Wi-Fi security system designed to address flaws in wireless privacy standards. Enhances WEP authentication and encryption capabilities. WPA2, on the other hand, is a more sophisticated version of WPA; since 2006, any equipment with a Wi-Fi certification has had to utilize it.

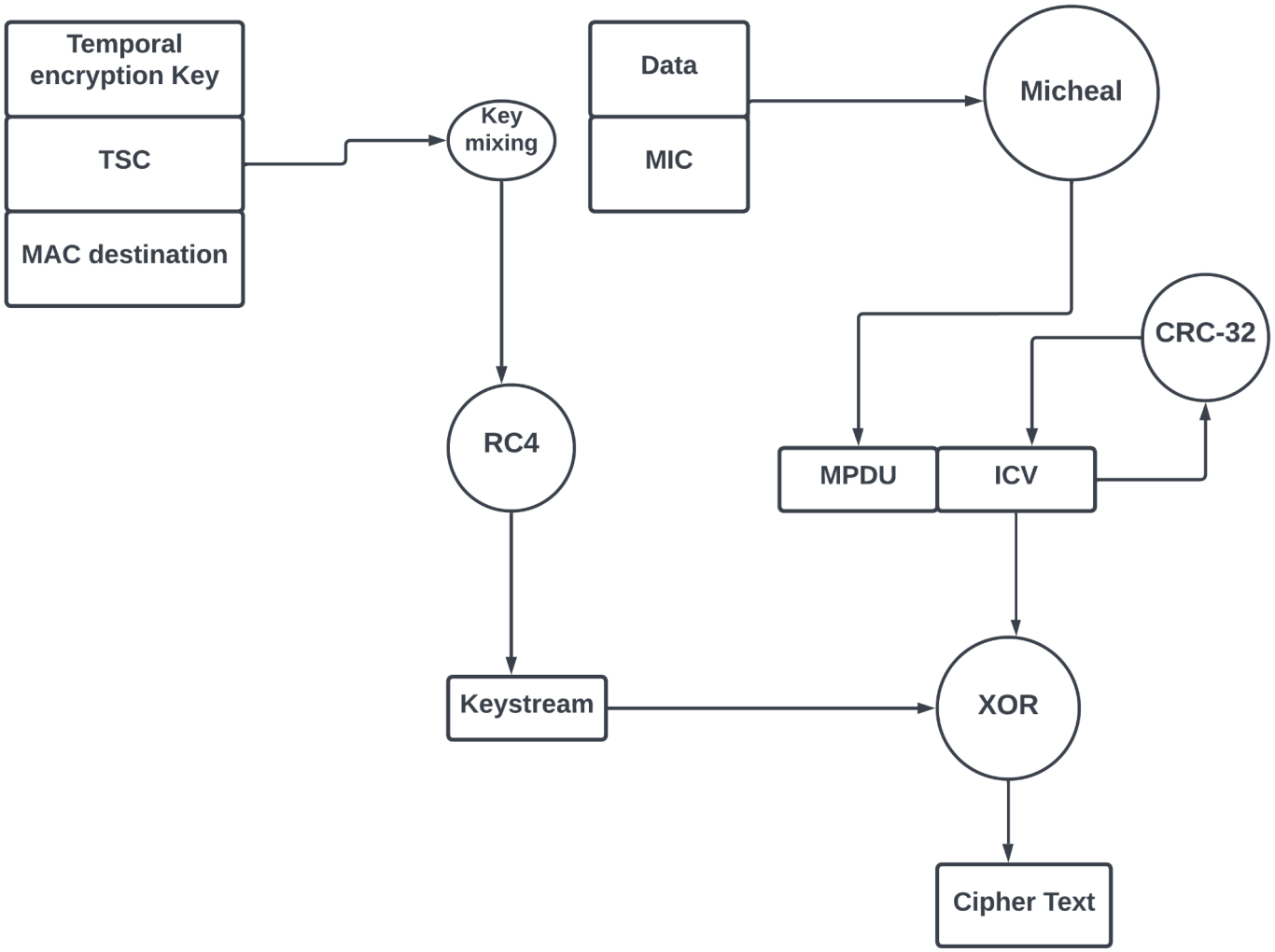


Fig.3 WPA working diagram

What are the features of Wireless-Fidelity Protected Access?

Wi - fi protected Connection provided better security than WEP by adopting one amongst two most popular innovations: temporary key authentication system and enhanced protection levels. WPA also includes crafted authentication, while WEP does not.

What is Wireless Protected Access-Pre-Shared Key?

It is a variation intended for residential networks. It is a simple yet effective WPA approach. A dry key or entrance key is set, like with WEP, However, WPA-PSK utilises TKIP. WPA-PSK changes credentials at periodic intervals to make it makes it harder for attackers to find and exploit flaws

What is WPA - 2?

WPA-2 which comes after Wireless Protected Access, has more sophisticated features and encryption capabilities. WPA 2, for example, employs the CCMP rather than TKIP. This substitution function is well with its ability to encrypt data. Like a result, Wireless Protected Access -2 is widely considered to be the best wireless secure protocol.

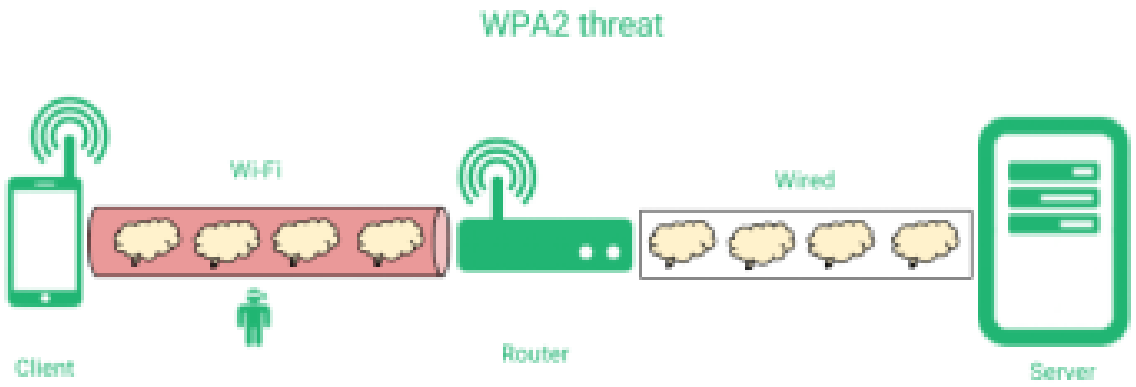


Fig.4 WPA2 Working diagram

Since 2006, all Wi-Fi Alliance certified products have been required to use WPA2. As a result, for more than 15 years, fully approved routers and devices have supported WPA2. As a result, WPA2 is becoming obsolete, which is why an updated version of the standard, known as WPA3, was adopted in January 2019.

Wireless Protected Access 3 incorporates greater security enhancements than Wireless Protected Access 2 and is now required to get an official Wi-Fi Alliance accreditation. WPA2 remains, nevertheless, a key kind of Wi-Fi network security for the time.

What is Wireless-Fidelity Protected Access 3(WPA3)

On June 25, 2018, the Wireless-Fidelity Alliance released and accepted a new standard for Wi-Fi Protected Access 3 (WPA3). WPA3 is not meant to replace the current WPA2 standard, but rather to increase security

and integrate new features. WPA2 may be developed and implemented on devices in the future. For a long time, WPA3 and WPA2 will be accessible in tandem. The first WPA3 certified devices might be available in late 2018.

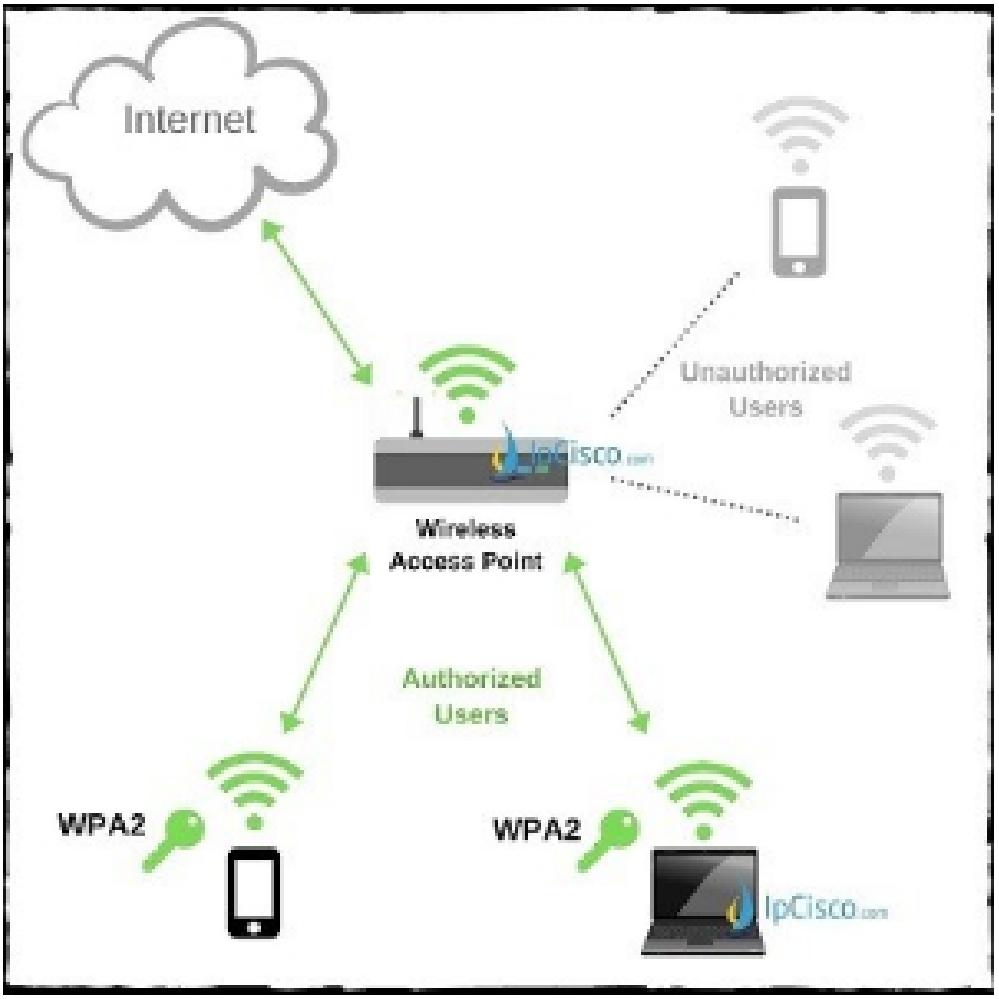


Fig.5 WPA3 working diagram

Wi-Fi Protected Access 3 brings significant improvements to the authentication and encryption environment. It also aims to simplify WLAN device configurations and increase security in high-density areas. Thanks to the 192-bit encryption used, Wireless-Fidelity Protected Access 3 is suitable for wireless networks with high security requirements, such as those used by government officials, industrial companies, the military, or governments.

What are the most serious dangers to Wireless Fidelity Security?

Data security is becoming a big public issue as the Internet becomes increasingly accessible through mobile devices and gadgets, as it should. Individuals and corporations might lose thousands of dollars as a result of data breaches and security breaches. It is critical to be informed of the most frequent dangers in order to implement proper security measures.

INTERMEDIATE ATTACK

A man-in-the-middle cyberattack is a particularly dangerous sort of attack in which a cyber hacker obtains access to the secured networks by mimicking a harmful point of access and gathering information.

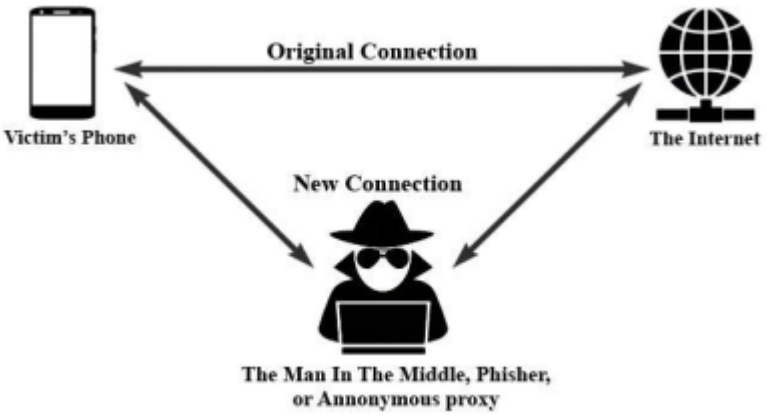


Fig.6 MITM working diagram

To get people to link to them and submit their passwords, the attacker creates computer systems that form a trusted network, such as Wi-Fi. MITM attacks may happen everywhere since devices are connected to a network by a strong signal and will join to whatever SSID name they remember.

RELEASE PERSONS & EXPLANATION

Cracking the code and password is a time-honored method that employs a "brute force assault." This attack depends on trial - and - error in the hope that you will ultimately guess accurately. Hackers, on the other side, can deploy a variety of tools to accelerate the process.

How can I protect my house wi-fi?

It is critical that you first select the most appropriate form of network security for your wireless home network. WPA2-PSK is suggested for residential wifi, whereas WPA2-Enterprise is only necessary for enterprises or colleges with large network traffic.

Consider the following while setting up home Wi-Fi:

1. Modifications to a default passcode and the Service set identifier
2. Create your passphrase at least 10 characters strong and also include mixed alphanumeric and numerical characters.
3. Set the router's firewall to on..
4. Set MAC address filtering to on.
5. Remote management should be turned off.

1.2 Project Overview/Specifications

It is a combination of Hardware and Software that will help increase the range of Wi-Fi IoT devices to detect incomprehensibly.

1.3. Hardware Specifications

- Raspberry Pi 4-4GB Ram
- ESP 8266 Wifi Module
- Tp-Link 722n wifi Adapter (for monitor mode and packet injection)
- Metal Sheet and long screw tight rod (for Wi-Fi big gun)
- Adapter Cable
- Power Bank (for Raspberry pi 4)
- NodeMCU esp8266
- RTL SDR dongle x 2

What exactly is the Raspberry Pi?

The Raspberry Pi is just a tiny computer which fits in the palm of the hand and communicates to a computer display or tv via a normal mouse and keyboard. It's a small device that can read a computer and teach individuals of different ages, R as well as Python are two such examples of computer languages. This could perform all of the operations of a desktop pc, like web surfing & high-definition video playback. and also creating spreadsheet, office software, and playing video games.

Furthermore, the Raspberry Pi can interact with outside environment which has been used in a range of digital maker applications, such music machines and parental locators, and also weather forecasting and sending birds to ir cameras in bird cages.

How does the Raspberry Pi work?

The Raspberry Pi is just a tiny computer that measures approximately 3.4 inches by 2.1 inches (8.6 inches by 5.3 inches) and provides a huge punch. This is owing to the widespread availability of low-cost, low-power CPUs for mobile devices, which necessitate compressing a reasonable level of processing and multimedia capabilities into a compact shell that can keep cool and not absorb a lot of energy.

Like a consequence, the organization selected a Cpu . The CPU has 256 Mb of memory, operates at 700 MHz, and is therefore compatible with high-definition graphics. Regardless of the fact that other ARM processors were available, the team picked the Broadcom CPU cos of Eben Upton's relationship with the company. Broadcom's willingness to fill a lot of small orders enables the firm to achieve the best price on this chip as compared to almost any rival CPU.

Because the device, like some other historical personal computers, lack peripherals and internal memory, the users must paste inputs, outputs, and storage. At the very least, you'll need to have a tv or monitors to receive outputs, a keyboard (and maybe a mouse) to takes inputs, a SD card to connect in the OS plus store the data, energy, and other required connection. You can increase the memory with just an external hard drive, and you'll still need an SD card because of OS will boot from SD by default.

It's not like all Debian operating systems are fully compatible to backwards compatible devices. Linux were adopted in part for its small memory requirements, that enable this to operate a perfectly functioning os on certain basic hardware with really no permanent storage. Since many of its distributions are including extra computer languages, Linux is typically free and effective as a CS study aid.

As additional content producers joins the bandwagon, the open - sourced environment of Debian will help extend the program. The Raspberry Pi Organisation's first aim is to create a source and a learning program around this one, however the team wanted to broaden its reach, concentrating on computers design & enabling the open-minded, dedicated program industry to develop software.

The Raspberry Pi's style and simplicity reminds me of old computers that gave birth to a generation of programmers and system aficionados. This gadget, unlike other PCs, can be used to censor web content. Finding stuff to do with the smartphone will be easier than ever before thanks to the internet. On the Raspberry Pi website, there is a user forum, as well as tutorials and other resources. To connect to the network, you'll need either a Model B Ethernet cable or a USB WiFi device.

Raspberry Pi components

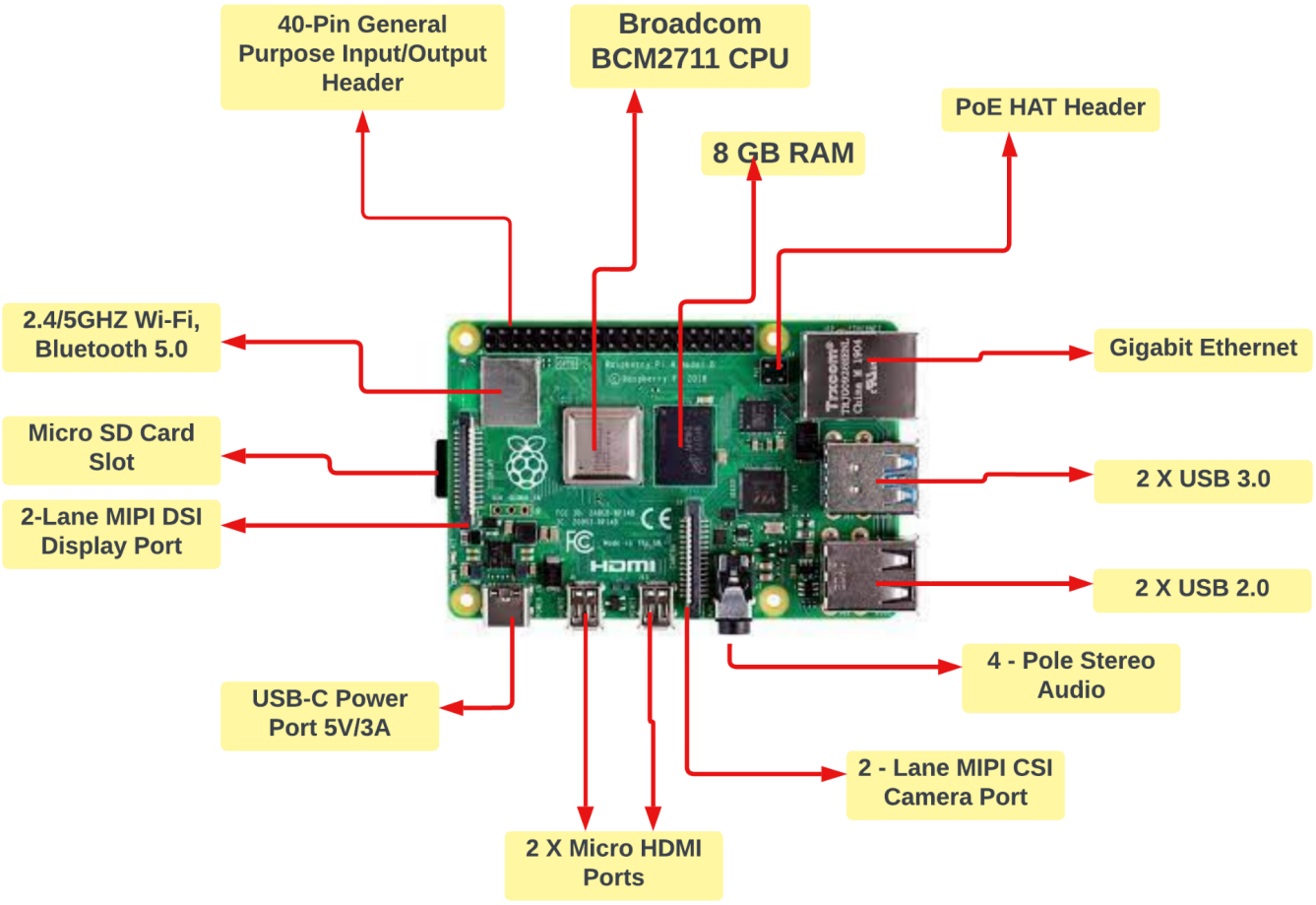


Fig.7 Raspberry Components

- **The Micro-USB Power Supply:** A little 5V USB cable is usually used to power this gadget. The amount of current required by the Pi, on the other hand, varies according on what it can do..

  Pi's use is determined by what you do with it. Video playback & online surfing are more powerful than idle startup. It also relies on the resources you have connected; certain keyboards and mouse consume more energy than others.

- **Secure Digital Card Socket:** Since the Raspberry Pi does not have internal storage or storage systems, a Micro Sd Card is just a removable device that stores that's also necessary for use in Raspberry Pi programs. SDHC and SDXC cards both are compatible by the Raspberry Pi. class ten card is the best suited card for such uninterrupted performance among all kinds of applications.

- **Universal Serial Bus Ports, LAN Ports:** Universal Serial Bus port: The Raspberry Pi model determines the number and kind of USB ports. Model B of Raspberry Pi has two Standard usb jacks, whereas the 2B and 3B + has four. The Raspberry Pi 4 features two Standard usb connectors and usb 3.0 port.

According to the Pi 4, USB ports are attached to the hybrid Ethernet card, and that is a USB device that is connected to the BCM2835's single transportable USB port. The USB hub chipset of the Pi 4 is linked to the SoC through the PCIe bus. The SoC of the Model A and 0 series is linked directly via an only one USB 2.0 port.

LAN Port: Raspberry Pi includes an Ethernet port that allows you to connect to the Internet and upgrade software or install the most recent packages from online storage. The Raspberry Pi (All Models) features an RJ45 Ethernet Jack that can connect to CAT5 / 6 cables. This cable connects The cord links the Raspberry Pi to the router, ADSL modems, and any other gadget which allows users to share the Internet service.

- **HDMI Ports:** An HDMI cable links the Raspberry Pi to an High Definition Telivision via the Hdmi cable. The Raspberry Pi could support a 1920x1200 pixel. Full Hd MPEG-4 can be transmitted also with help of Displayport.

- **Radio Corporation of America Cable(Video Out):** Besides from HDMIcable connection, that allows for increased communication, the Raspberry Pi may be linked to a normal screen via an RCAoutput cable. The RCA cable is much less expensive than just a Hdmi, but for convenient sound, a 3.5mm sound cord is needed..

A 4mm pole 3.5mm stereo port with a hybrid video feed is included in the Raspberry Pi 4 and Pi 2. It allows the actual Model B's composite video connector to be eliminated.

A 4-pole connection for video and audio communication are included completely redesigned jacket. Identical connectors could be seen on a range of mobile phones, like ipod, Music players, and phones. This is now available on the Pi 2, and Pi 4 Chipsets.

- **Led light indicator:** The Raspberry Pi includes 5 main LEDs for the following activities:

I. RULE: (Green_LED): The ACT LED's primary role is to display the state of the card. It usually shines in the middle of the end user's SD card activity.

II. PWR: (Red): The fundamental function of a PWR-powered device. When the Raspberry Pi is turned on, this withdrawal is OPENED indefinitely and it will keep going till the Raspberry Pi is did turn_off.

III. FDX: (Orange_LED): An FDX led's original objective is full duplex. Whenever the Ethernet port is in full duplex operation, the LED will flash.

IV. LNK - (Orange_LED): LNK was in charge of the work, which was overseen by Link. This LED illuminates whenever an Ethernet connection has been established and packets transmission starts.

V. 100: (Orange): The 100 Led's function is to represent a connecting speed of 100 Mbps.When an Ethernet link is made, the LED only glows if the connection has a speed of 100 Mbps and shuts off if the connectivity has a speed of 10 Mbps.

- **GPIO:**The GPIO connector on the Raspberry Pi is being used to attach a variety of external devices. The Raspberry Pi has 40 GPIO pins on board, with 26 of them being used for digital input or output. Importantly, nine of the fourteen extra GPIO pins are specialized input/output pins which enable UART, I2C, & SPI Bus, yet there are plenty of spare GPIO connection pins.

- **Camera Serial Interface Camera Port:** A Serial Interface Type 2 Mobile Industry Processor Interface (MIPI) is included into the Raspberry Pi (CSI-2). The Broadcom BCM 2835 CPU may be attached to a small camera through the CSI-2 interface. The goal of this interface is to configure camera modules on mobile industrial processors. MIPI CSI-2 version 1.01 supports up to four data bits but each modem does have a 1 gigabyte every second bandwidth. To facilitate data flow, the D-PHY standard specifies a virtual layer interface between the camera and the CPU.

The following Raspberry Pi models are available:

- Raspberry Pi 1 Model A+
- Raspberry Pi 1 Model B+
- Raspberry Pi 3 Model B
- Raspberry Pi 3 Model B+
- Raspberry Pi 3 Model A+
- Raspberry Pi 4 Model B
- Raspberry Pi Pico
- RP2040
- Raspberry Pi Zero 2 W

What exactly is the Esp8266 Wi-Fi Module?

The Esp8266 Wi - fi Module is a self SOC with only an inbuilt TCP/IP protocol which enables any CPU to access to your Wifi connection. It can execute its very own application or outsource all Wi-Fi network communications to some other application processor. Every ESP8266 module comes pre-programmed with just an AT command patch, users can connect it to your Arduino system have the same WiFi-ability as just a WiFi Protective layer. An ESP8266 module is a low-cost module which has a large and growing customer base.

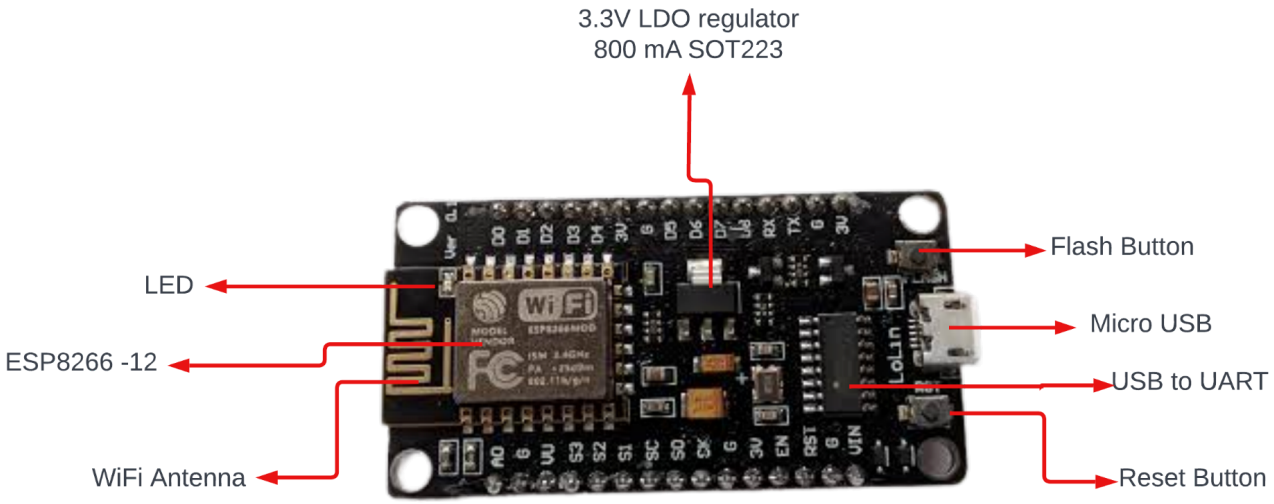


Fig. 8 ESP8266 components

Technical requirements?

- Processor: L106 32-bit RISC CPU core running at 80 MHz based on the Tensilica Xtensa Diamond Standard 106Micro[5].
- Memory consumption:
  - Instruction RAM of 32 KiB
  - RAM with 32 KiB instruction cache and 80 KiB user data
  - ETS system-data RAM 16 KiB RAM
- Up to 16 MiB of external QSPI flash memory is supported (512 KiB to 4 MiB typically included)
- IEEE 802.11 b/g/n Wi-Fi standard
  - TR switch, balun, LNA, power amplifier, and matching network are all integrated.
  - Authentication using WEP, WPA/WPA2, or open networks
- 16 GPIO pins is required
- I²C (software implementation)[6]
- I²S interfaces with DMA (sharing pins with GPIO)
- UART on dedicated pins, plus a transmit-only UART can be enabled on GPIO2
- 10-bit ADC (successive approximation ADC)

What is Tp-Link 722n Wi-Fi Adapter?

The TL-WN722N Standards For Wireless USB Adapter attaches a desktops or laptop computer to a wireless connection via providing high-speed Internet connectivity. They are IEEE 802.11n compliant and can provide wi - fi rates up to 150Mbps, which would be perfect for playing online games or streaming video.Furthermore, wi - fi security encrypting may be simply set up by pressing the QSS (Quick Setup Security) button, protecting the networks from the outside attacks.

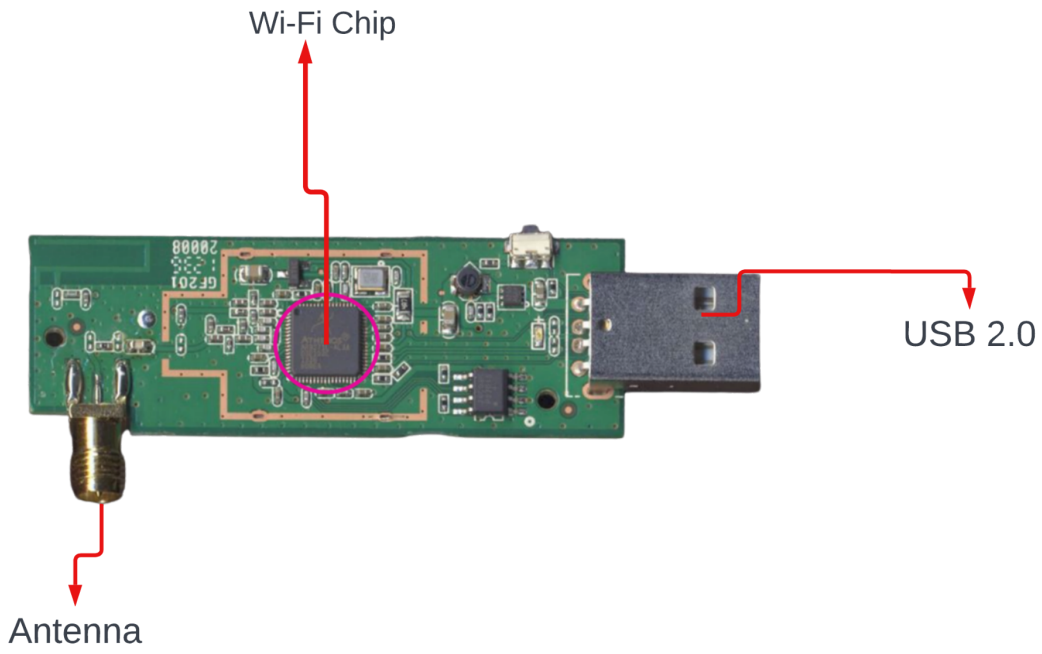


Fig.9 Wi-fi adapter components

This TL-WN722N, that is based on IEEE 802.11 wireless technologies, has improved its ability to mitigate loss of data over vast distances as well as around barriers in a small office, a luxury apartment, or maybe even a steel-and-concrete tower. As compared to previous 54M devices, this TL-WN722N provides performance improvements, enabling users to have a much more comfortable browsing session, incorporating document transfer and video streaming.

What is RTL2832U - Software defined Radio?

SDR refers to a radio communication system in which formerly hardware-implemented elements (e.g., mixers, filters, amplifiers, modulators/demodulators, detectors, and so on) are being used. Currently, these are executed as programs on a desktop pc or the other home computer . When receivers were firstly developed, each product's electronics had a particular function; one component might receive a signal, the other would tune it, and yet another would transform the signal to sound waves so people could hear it. It's now possible thanks to high performance computing.

The RealTek RTL2832U-Software Driven Radio is a low-cost USB device which can be used as a computer-based radio receiver to record live radio transmissions. Depending on the RTL-SDR, it can detect frequencies ranging from 500 kHz to 1.75 GHz. The large bulk of RTL-SDR technology is also community-developed, open-source, and therefore, in the overwhelming majority of cases, free.

It commonly intercept frequencies ranging from 500kHz to 1.7GHz.

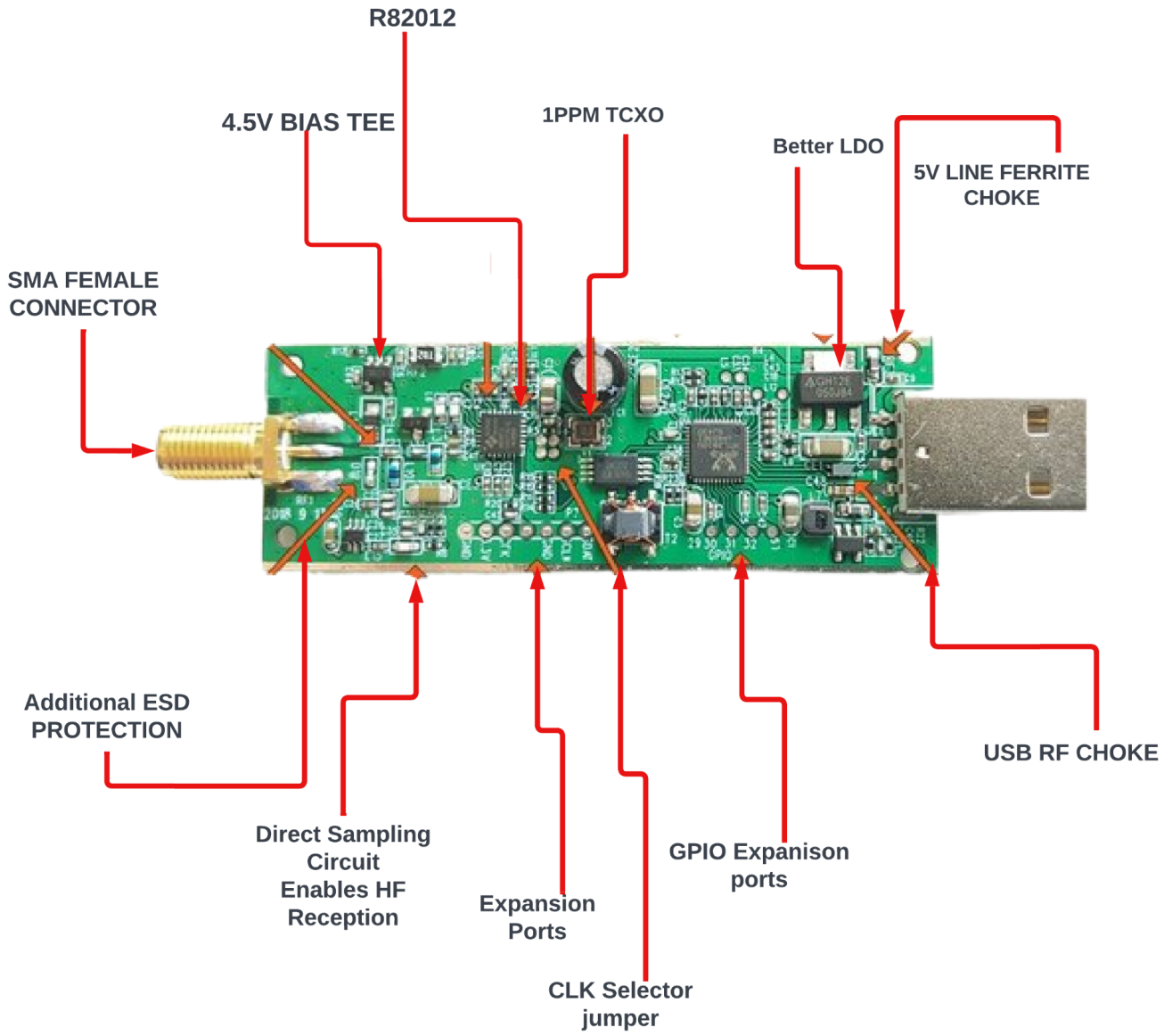


Fig.10 RTL SDR components

RTL-SDR arose from DVB-T-TV tuners built using the RTL2832U chipset.As according Antti Palosaari, the raw I/Q data in the RTL2832U could be accessed and modified to utilise proprietary software driver built by Steve Markgraf. It's comparable to finding that your old Zune MP3 player can quickly run Excel and Microsoft Word.

It has grown in popularity since its discovery, providing users with access to a wide range of radio frequencies. So, for a little investment, you may get radio signals that would have cost thousands of dollars just a few years ago. A word of caution: we live in a mass-production culture, which comes fraudsters with it. Keep a look out for 'knock-off' RTL-SDRs; they're out there and numerous, but they can appear identical to the actual units, down to the writing on the casings. I'm not saying that knockoffs won't function; nevertheless, buyer beware, and you get what you pay for.

1.4. Software Specifications

- Kali Linux Raspberry pi 4 (64-bit) (img.xz)
- Shell Script (for automation of Vulnerability assessment)
- Juice SSH/VNC Viewer (Android/ Windows application to act as touch display of Raspberry pi

What exactly is Linux?

Kali Linux is an open-source Linux system based on Debian that is designed for sophisticated vulnerability assessment and security audits. Kali Linux provides hundreds of tool for information security services such as penetration testing, security research, computer forensics, and reverse engineering. Kali Linux is a multi-platform solution for data security experts and enthusiasts that is both user-friendly and free.

Kali Linux was released on March 13, 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, fully adhering to Debian development guidelines.

How does Linux function on the Raspberry Pi?

Kali Linux is a Debian-based os designed primarily for pen testing. All of the tools required for penetration testing are pre-installed in Kali Linux. Even if something isn't installed by default, it will be in Kali Linux's official package repository. As a consequence, you can install anything from Kali Linux's official package repository with ease. Kali Linux is a great tool for penetration testers.

The following items are necessary to build a functioning kali linux operating system on a raspberry pi:

1. The Raspberry Pi 4 is a single-board computer.
2. A USB type - c power adapter for the Raspberry Pi 4
3. A microsd card with a size of 32GB or greater
4. A card reader used to install Kali Linux on a microSD card.
5. A computer or laptop to be used for flashing the microSD card.
6. A mouse and a keyboard
7. A cable that connects a Micro-HDMI to an HDMI port.

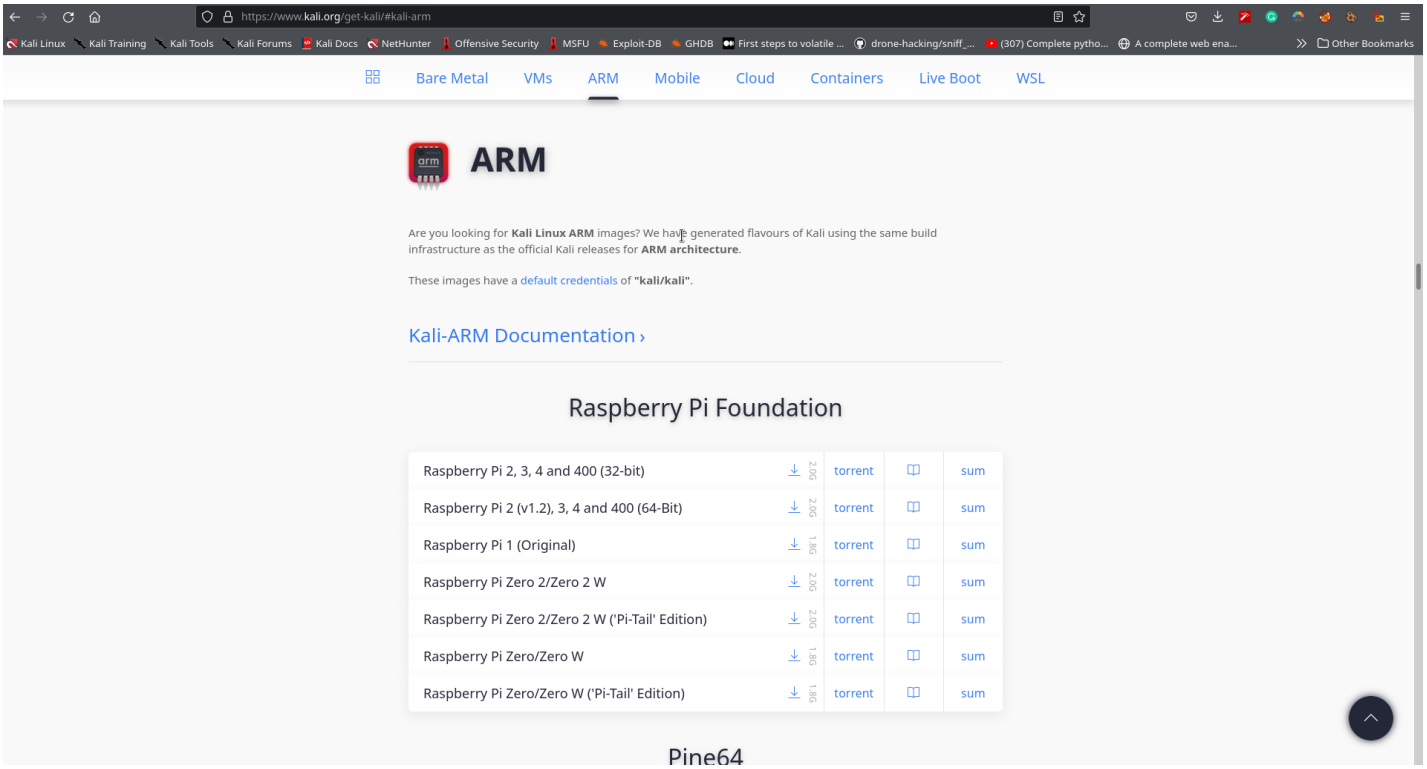
The following is the procedure for installing Kali Linux on a Raspberry Pi 4:

The first step is to get the Linux software for Raspberry Pi from website.

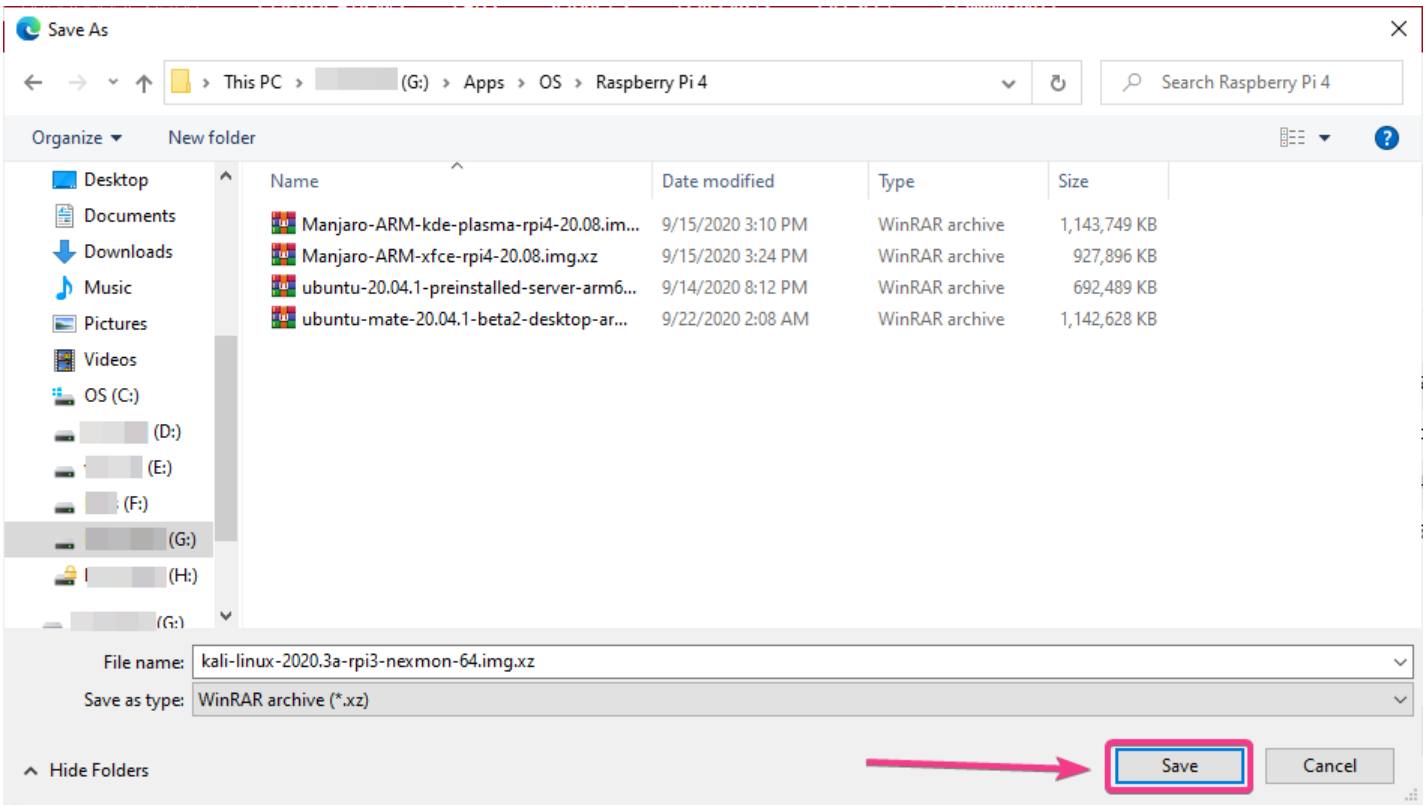
Navigate to the official Kali Linux ARM image download page in your browser. Once the page is open, navigate to the RASPBERRYPI FOUNDATION area and click on one of the KALI LINUX PI IMAGES, as seen in the screenshot below.

If you have a Raspberry Pi 4 with 2GB of RAM, then download the KALI LINUX RASPBERRY PI 2,3, and 4 images.

Alternatively, if you own a 4GB or 8GB Pi board, you may download the KALI LINUX RASPBERRY PI 2(v1.2), 3, and 4 (64 bit) image.



The browser will urge you to save the Kali Linux Raspberry Pi image when you click the download link. Choose the place where you wish it to be saved. then click the save button



Your browser will now begin downloading the Raspberry Pi's ARM image, which may take some time.

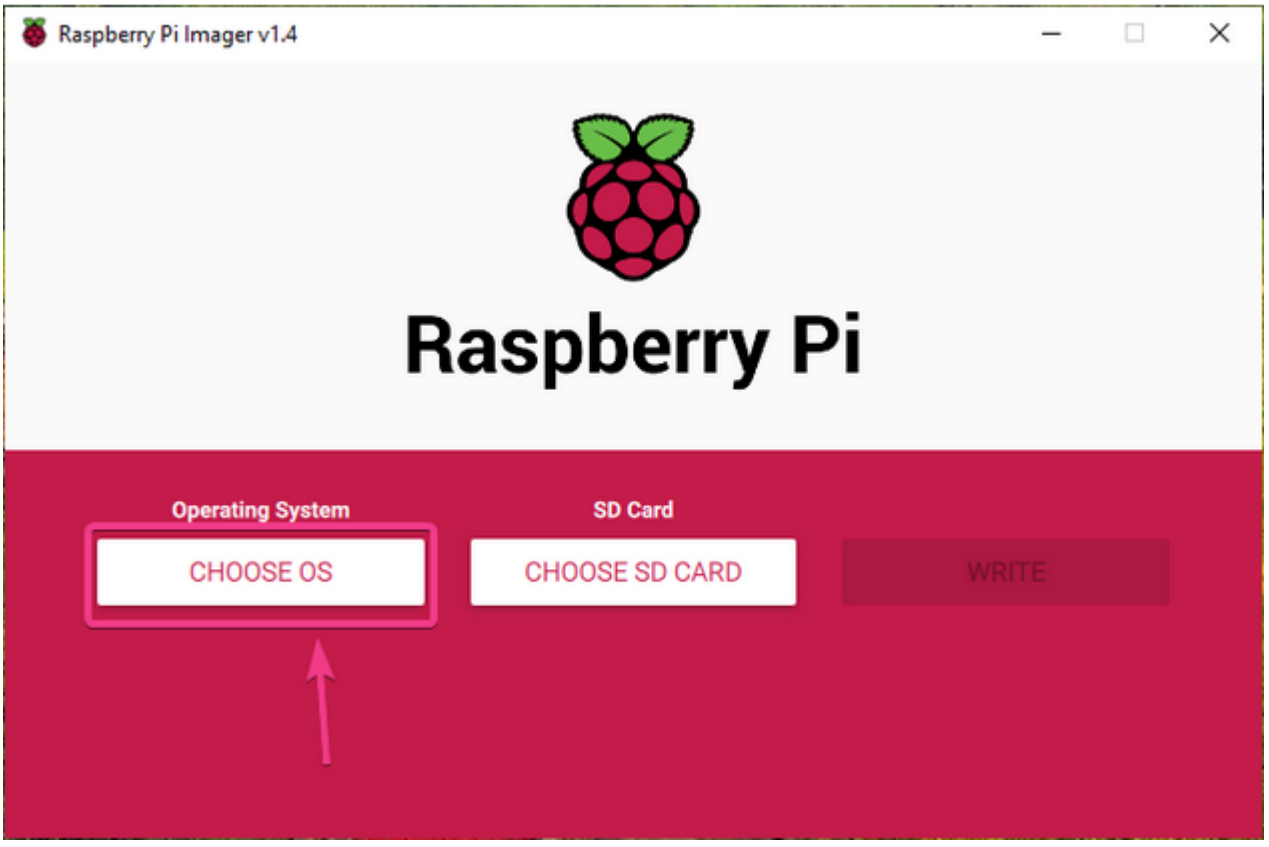
From here, the method for flashing kali linux for raspberry pi on the SD CARD, which will serve as a storage device for the raspberry pi device, will begin.

Save the Kali Linux Raspberry pi ARM Image to a microSD card after you've downloaded it. Use tools such as Balena Etcher or Raspberry Pi Imager to flash it to a microSD card.

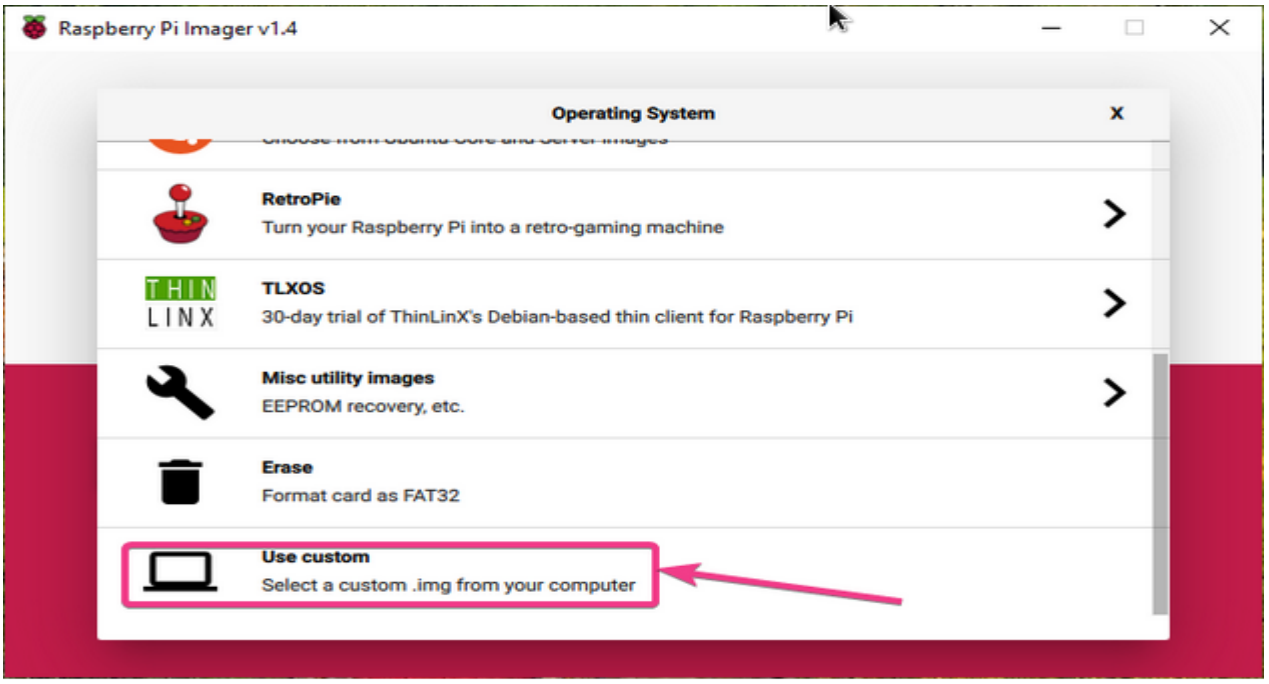
The Raspberry Pi imager programme is used to write the Kali Linux image to the microSD card. Raspberry Pi Imager is available for download from the Raspberry Pi Foundation's official website. It works with Windows 10, Ubuntu, and Mac.

Insert the microSD card into your system after installing Raspberry Pi imager on your PC, and then start Raspberry Pi imager.

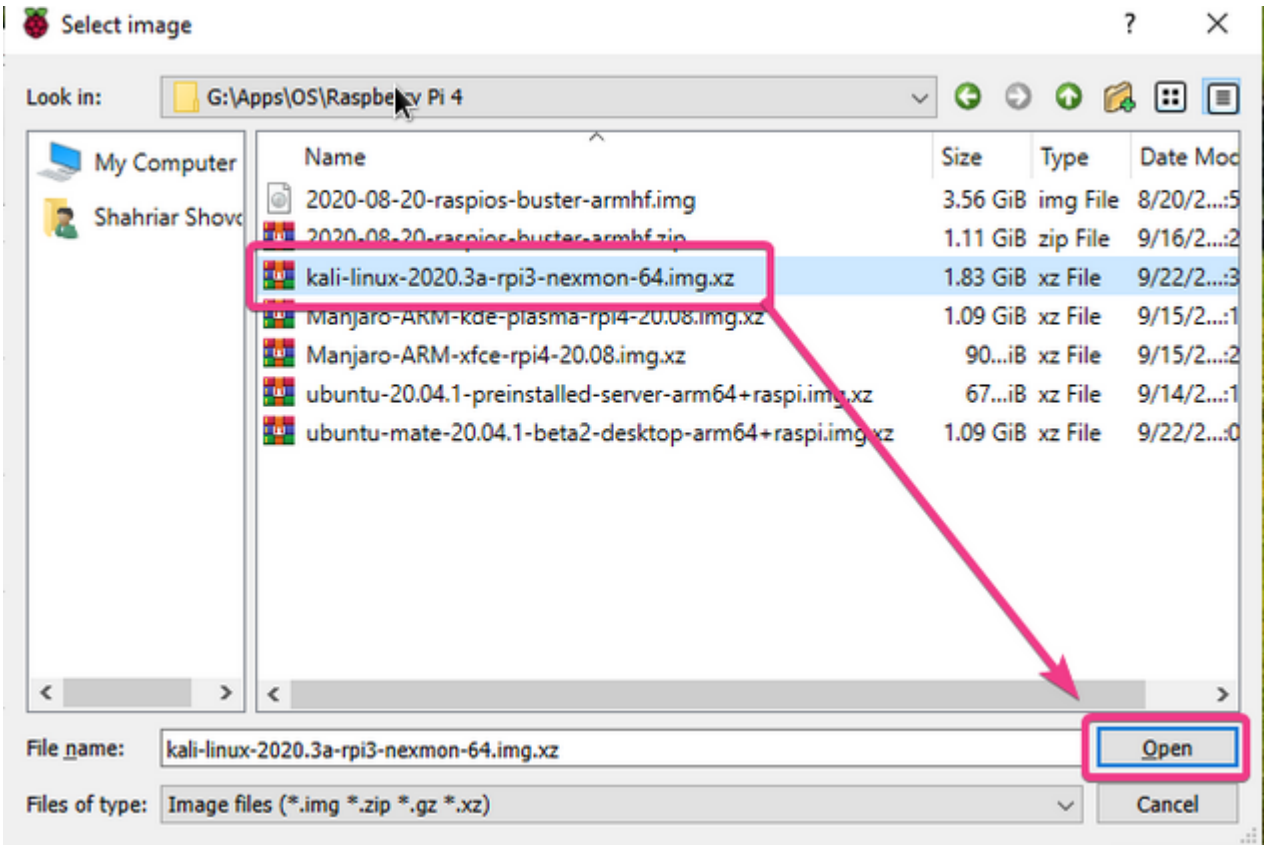
Now, select an OS Image by clicking on the CHOOSE OS button.



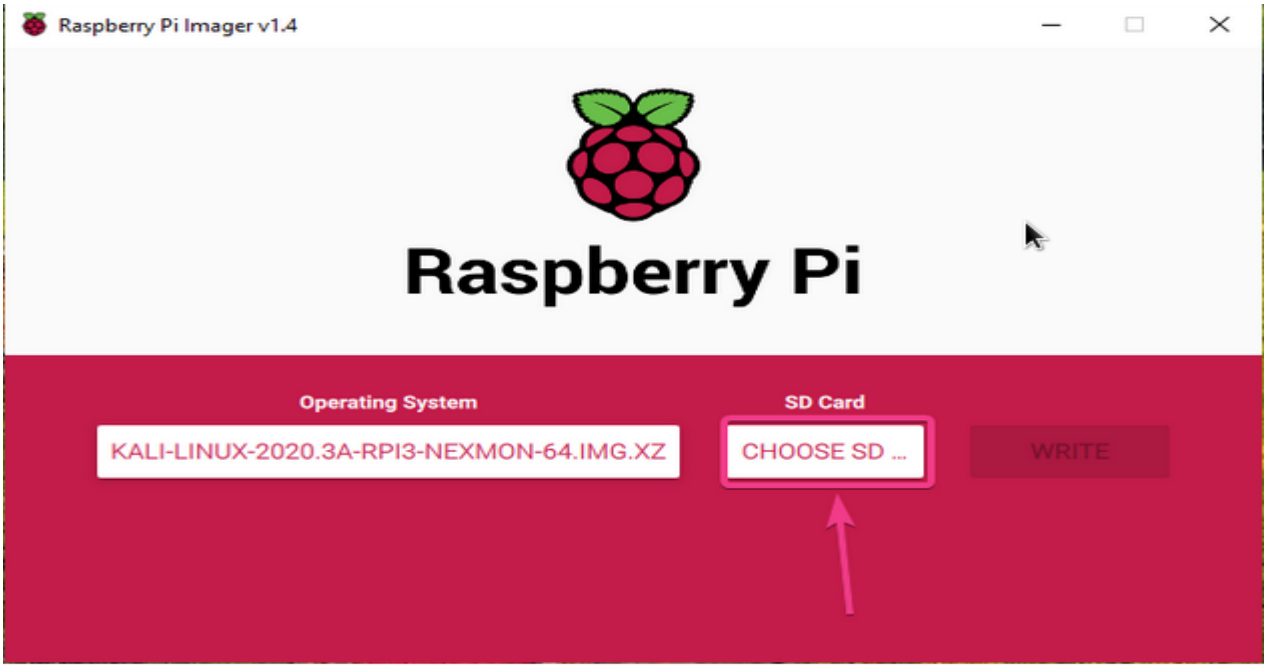
After you've chosen an operating system, choose USE Custom from the drop-down option.



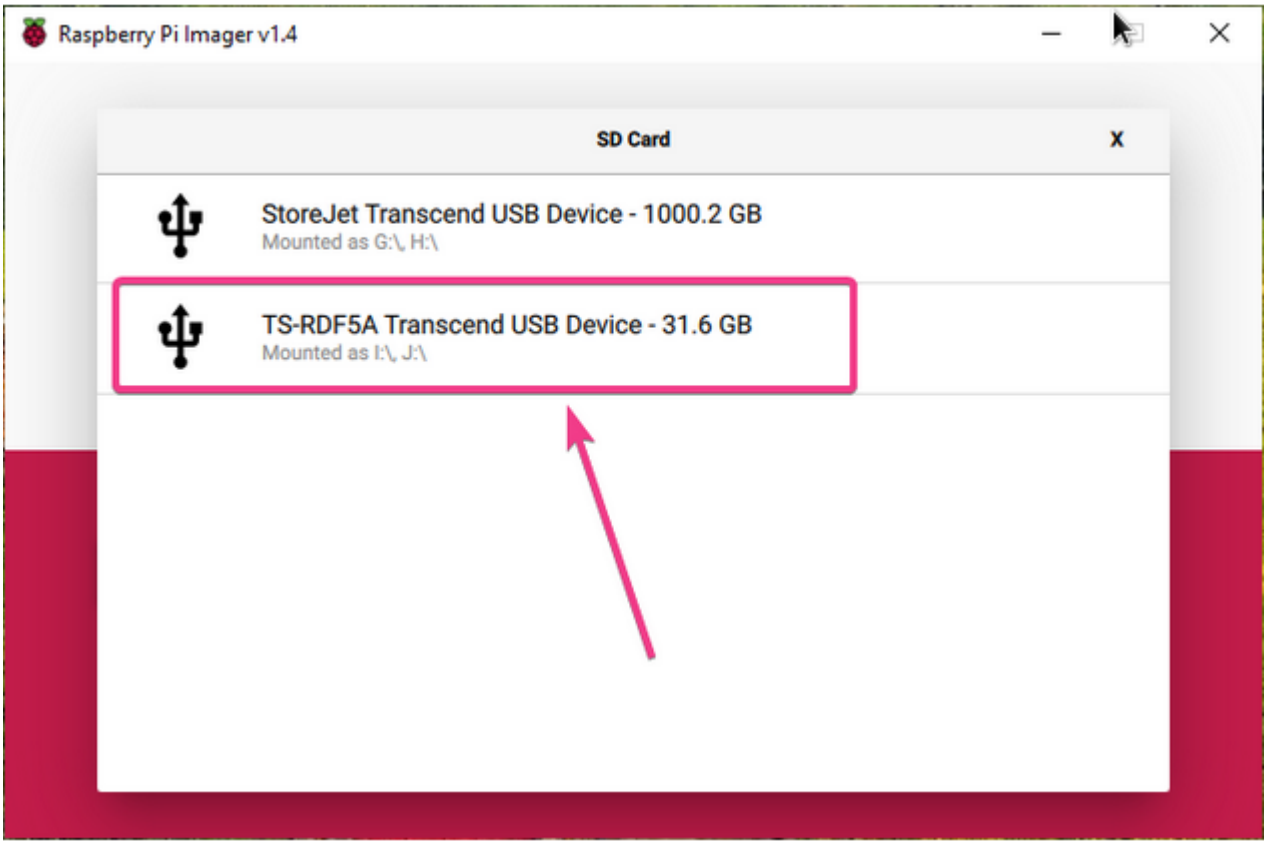
Now, open the raspberry pi image that you downloaded earlier.



After selecting OS, to choose SD CARD to which OS will be installed just click on CHOOSE SD CARD.

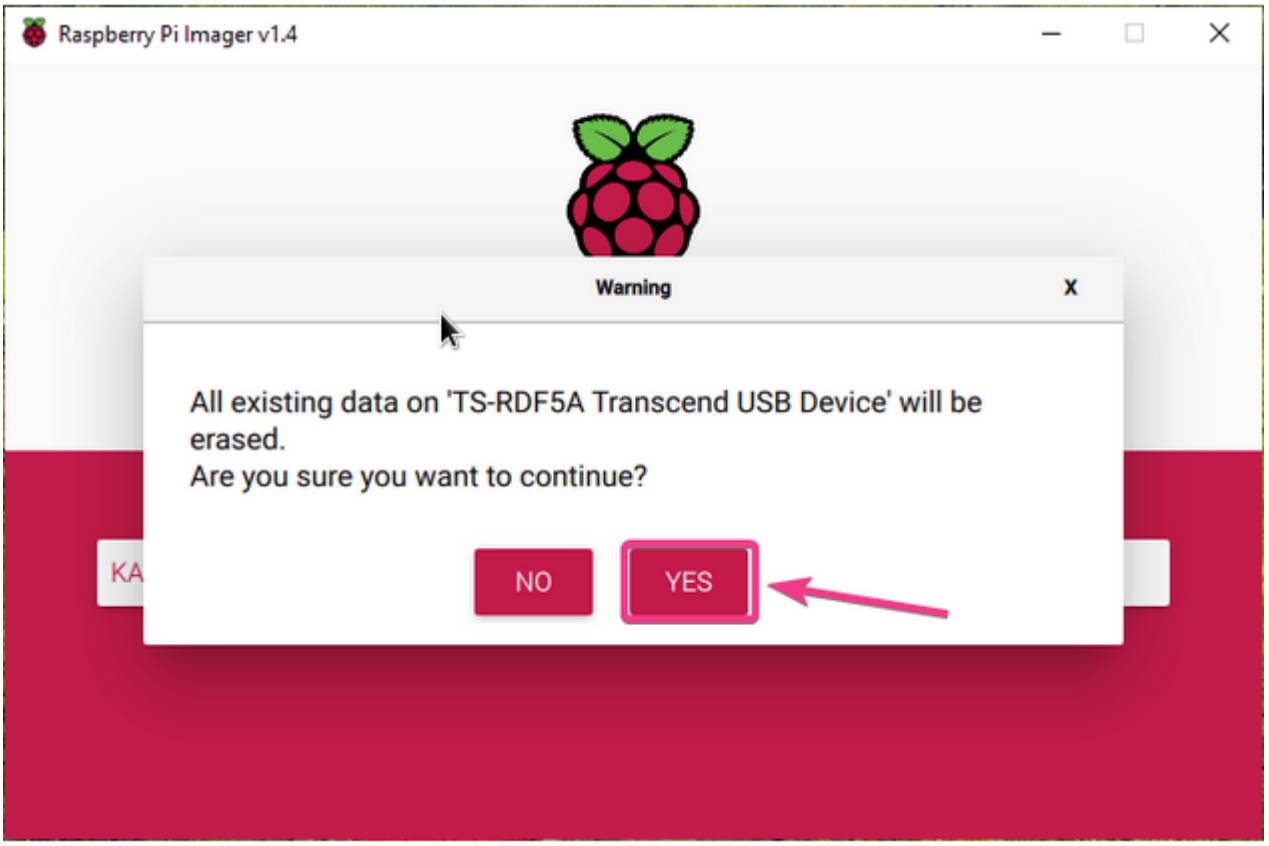


Now Select the microSD CARD from the list.



To continue flashing the Microsd card Click on Write Option.

To flash a microsd card with a new OS, make sure that no important data on you microsd card are present because it must be erased before flashing it, now click on YES.

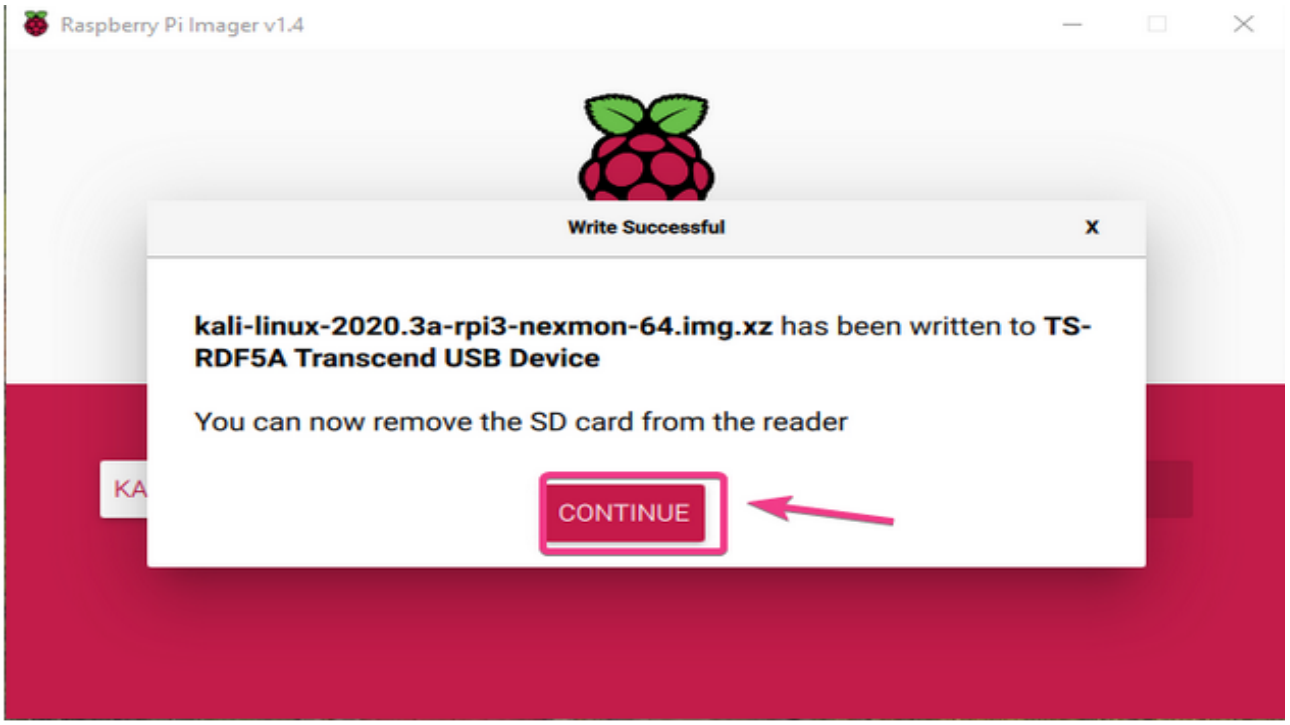


After this the raspberry pi image will start flashing the microsd card with kali linux.

To complete writing the image, it may take some time to process it.

After writing the image on the microsd card. The writer application will analyse the microsd card for any damaged sectors or write errors, which might take some time.

At this point, the ARM image should be flashed to the SD Card. Exit the raspberry pi imager programme and unplug the microSD card from the system by pressing the CONTINUE button.



After going through the difficulty of installing Kali Linux, it's now time to run a linux system on the Raspberry Pi 4:

Connect the SD card to your Raspberry Pi 4 once you've removed it from the computer. Connect the tiny HDMI to HDMI cable, keyboard, mouse, RJ45 network cable, and Type-c power cord to the raspberry pi 4 to power it.

2. LITERATURE SURVEY

S.No	Paper Title	Technology Used	Merits	Future Scope
1.	EvilScout: Evil Twin Attack Detection and Mitigation in SDN Enabled WiFi	Wi-fi Adapter with monitor mode & Packet injection, shell script	Evil-twin is a fake WiFi access point that's sounds to be legitimate but designed for wireless communication This can be used to steal the credentials and attracting people	In future, mitigation of APSB attacks is detecting the presence of bad twins on isolated channel from (LAP). In addition, how to detect additional attacks on WiFi using SD control of network monitoring
2.	Small-scale Wireless Fidelity Technologies for IoT: Attacks and Defenses	Wireless Fidelity, , Zigbee protocol, Bluetooth connectivity, RFID mechanism	Security mechanism of the IoT infrastructure depends largely on the security of its wireless However, is said to be most widespread, the most important, and the most vulnerable part of IoT.	The research contributed the following : Introduce the general attack on Wi-Fi infrastructure, RFID, ZigBee, and Bluetooth IoT. Check out Wireless Fidelity attacks, Bluetooth connectivity, ZigBee protocol, and RFID technology.

			their fragmentation and security for infrastructure.	
3.	Concurrent utilization of security devices of residential Wireless Local Area Network access points	Tenda WiFi wireless access point, Kali Linux version 2017.1	It is noted that the predefined security measures are in jeopardy. The researchers used several WLAN security measures that focused on one WLAN security parameter at a time.	The access point set up in a secure MAC filter mode. Thereafter an additional hidden SSID securitywas added to the AP. Three security modes were then lowered to provide three-tier security. This WPA2 PSK cascade model with SSID encryption and filtering of MAC is also ecploited
4.	Adaptive Indoor Passive Intrusion Detection in wireless fidelity	Wireless fidelity, channel state information (CSI), without device detection, and predefined testing	APID, a flexible input detection system, which allows for flexible, free in-device intrusion detection using CSI wireless fidelity signals	an access flexible personal input based on existing WiFi devices. Basic strategies based on the amplitude of the CSI amplitude analysis of a different feature

5 .	Wireless Fidelity Security Certification through Device Information	Wireless fidelity security authentication technique for grasping device details	The experiment make sure that authentication technique can stops illegitimate users from connecting to wireless hotspot, thus creating a strong Wireless Fidelity communicatio n	Analyzes and researches the current Wireless fidelity hotspots configuration information,
6.	4-Way Handshake Strategy and Secure Authentication for secured single Communication in public Wireless Fidelity networks	Wireless Fidelity, Wireless Fidelity Protected Access 2 - Pre - Shared Key Authentication, and elliptic curve cryptography are all examples of 4-way handshake security.	an elliptic curve of the concept of public key encryption	When compared to existing networks, the solution can improve the security of Wireless Fidelity protected Access 2 - Pre-Shared Key -based Wi-Fi social networks. Existing Wireless Fidelity tactics are the most deadly since the aforementioned ancient assaults.

7.	WIDS: Wi-Fi Enhanced Access Access System (IEEE 802.11) Protocol	irregularity conduct Analysis, Internet of Things Security, Wi-Fi Security, Machine learning.	Wireless Access Program (WIDS) Program; how to analyze confusing behavior to analyze attacks on Wireless Fidelity networks with huge precision and low negative alarms.	
8.	Finding Critical Security Issues of the IoT World:	Social IoT, heterogeneous technologies, DDos attack, physical wireless security.	Essential Defense Controls is a set of recommended online defense actions that provide specific and effective ways to stop today's ubiquitous and dangerous attacks.	The IoT paradigm will include most of smart devices processed, sensors- ing and trapping skills that can be connected to the internet.

9.	Security Testbed for Internet-of-Things Devices.	Testbed framework,MITM Attacks (Man in the Middle attack), XSS Attacks (cross site scripting) ,Security testing manager module.	The automatic security testbed is one of the main tracks of the Internet Research Equipment and Safety Lab. The goal of the automatic security testbed is to test the security and privacy of a unique IoT device on the market.	The proposed security testbed faces a major challenge in the IoT research field, namely the evaluation of security and performance analysis, as IoT systems are considered to be the most complex situations due to the scope of operation and the variety of tasks involved in this process.
10.	Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks.	Generic IoT network, hierarchical Internet of Things network, authentication, key administration, security, Automated Validation of Internet Security Protocols and Application simulation.	Smart Internet of Things devices can be accessed remotely managed using network infrastructure that allows direct integration of computer systems with the physical world.	

2.1. Existing

- Wi-Fi adapters have antennas that can range up to only 50 meters to 60 meters, while this invention of the Wi-Fi gun will increase the range of adapter to 4 kms to 5kms with strong and powerful signals that help to transmit data fastly.
- The existing system is also lacking anomaly detection with a short range of antennas, all those systems are not capable of finding anomalies in IoT devices.
- This system is complete with a small computing power device called raspberry, So we can integrate any type of computing power into it.

2.2. Proposed System

- A process of Auditing the Network, Capture Handshake, finding anomalies in IoT devices, and capturing wireless signals within the range of 4 to 5Km. A compact machine consists of capturing signal mechanisms with the computing power from any static location having a range of 4 to 5 km.

- A process in claim 1 also adds the vulnerability assessment in wireless devices. Computing power allows the automation of finding vulnerabilities, drone jamming, and response to incidents.

- A process for treating wireless devices, the process being substantial as described herein with reference to and as illustrated in the accompanying drawings.

- Machine for treating wireless devices, This machine comprises a Wi-fi gun, Raspberry Pi 4 Model B with 2GB of RAM, and NodeMCU Esp8266 for increasing the range of Wi-Fi signal up to 5 Km with automation scripting for jamming drone or anomaly detection in IoT.

- Existing Wi-Fi adapters have antennas that can range up to only 50 meters to 60 meters, while this invention of the Wi-Fi gun will increase the range of adapter to 4kms to 5kms with strong and powerful signals that help to transmit data fastly.

3. SYSTEM DESIGN AND ANALYSIS

3.1. System Design

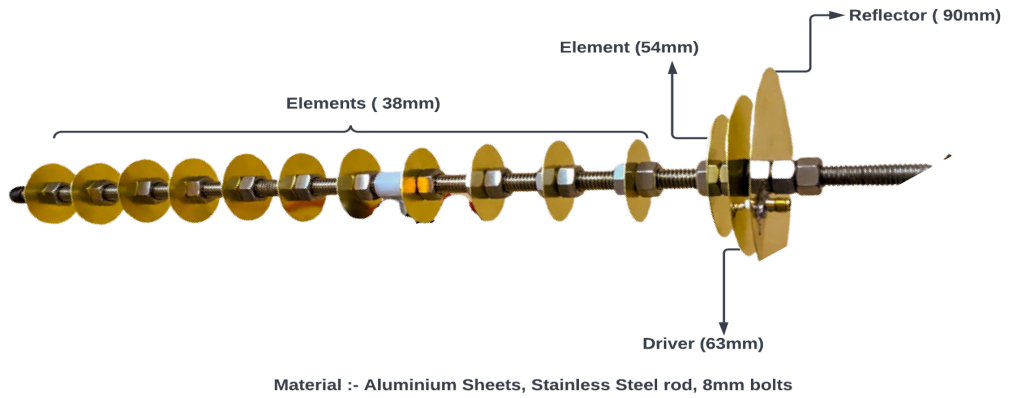


Figure 11. Design of Wi-Fi Gun

Requirement Specification

- Raspberry Pi 4 - 4GB Ram
- ESP 8266 Wifi Module
- Tp-Link 722n wifi Adapter (for monitor mode and packet injection)
- Metal Sheet and long screw tight rod (for Wi-Fi big gun)
- Adapter Cable
- Power Bank (for Raspberry pi 4)
- NodeMCU esp8266
- RTL SDR dongle x 2
- Kali Linux Raspberry pi 4 (64-bit) (img.xz)
- Shell Script (for automation of Vulnerability assessment)
- Juice SSH / VNC Viewer (Android/ Windows application to act as touch display of Raspberry pi 4)

3.2 BACKGROUND STUDY

3.2.1 What is Drone

A drone is an unmanned aircraft i.e. an aircraft which does not require any person to operate. Drones are officially termed as unmanned aerial vehicles (UAVs). In essence, a drone is like a robot as it is remotely controlled or spontaneously using software-based flight systems in its embedded, integrated sensory system and global positioning system (GPS).

Drones were primarily built for military and aerospace industries. But now these are exclusively used for other purposes as well due to their advanced security and efficiency. These drones are actually like robots as they do not require any human to be operated and have different variations of autonomy. A drone's autonomy can range from remote sensing to supervised, that indicates all relies upon that various sensors and LIDAR sensors to compute its movement.

Drones may hover at various altitudes and distance. Hobbyists typically hire ultra-short-range drones, that can travel up to 3 miles. Short-range unmanned aircraft have such a range of approximately 30 miles. Short-range drones, that can hover approximately 80 miles, are most often deployed for data and information gathering. Its mid-range UAV does have a range of 400 miles and can be used for collecting information, academic research, or weather prediction. Most longest-range drone were classified as "durable" and then they can fly over 400 miles and achieve heights above 3,000 feet. Our drones can be remotely controlled can hover at such a range of distances and heights, making it ideal for such worlds largest challenging tasks. It help in the retrieval of disaster victims, the surveillance of terrorist scenarios by law enforcement and military, as well as the improvement of scientific research in some of the worlds largest extreme climates. Uavs have invaded our homes, acting as a source of entertainment for hobbyists and an essential tool for photography.

The working of drone?

1 - UAV

The Drones are frequently referred to as UAVs.. These are operated under the control of a system called Unmanned Aerial System (UAS). They exist in different forms. There are lighter UAVs, such as airships and hot air balloons, and smaller UAVs with "wings".

2 - GCS

The GCS is essentially the system's processing or control unit. It allows UAVs to fly and operate. These stations can be large enough like a multiview table or very small like a handheld controller or in the form of an app. These can be either controlled by the user or through satellites. It is in charge of controlling the flight, monitoring payload sensors, providing status readings, and connecting data connection systems.

3 - Payload

Drones, particularly UAV, come in a variety of dimensions and may carry payload of various size. Drones are commonly utilised for delivery, whether in rescue missions or packing, but they are required to be built in that way to be used for this purpose. Some drones can fly over the sea very easily, while some would only be able to fly only some thousands feet. Some drones can hold the capacity to hold hundred pounds, while others can have the capacity of around 10 100 pounds only. Thus, it becomes a crucial step for the operators to choose the correct type of drone according to the job or purpose the drone is going to be built.

4-Data Links

The data link acts as a transmission hub. This enables the drone to interact with base operators while flying.Data links that typically use radio frequency technology for communication provide the operator with important information as available flying time, proximity to controller, range to destination, flying height, and so on Using the UAV at 2ghz for controlling and 5.0 Gigahertz for cameras allows the controller to travel approximately four kilometers., while 900 MHz fOver 20 miles could be reached through using 1.3 Gigahertz for aircraft controls + 1.3 Gigahertz for visual management. Operators should identify the suitable UAS for such job at hand.

How do drones fly?

VTOL drones

vertical take-off and landing or VTOL drones are generally multi-rotor. These drones can vertically take off, fly, and land and hence the name.

GNSS

Duo GNSS, like GPS and GLONASS, are aircraft which are used in a number of uavs. These can easily operate in both satellite and non satellite modes. They provide improved communication during operation. These can be activated using a GCS remote control which helps the pilot to determine Whether there are still enough GNSS satellites for the uav to travel independently, the aircraft's actual position in respect to the operator, and also the "home area" to which uav must return. Returning to Home could be triggered autonomously whenever the battery is low or contact between both the aircraft and the operator is lost, in additional to just being handled by the operator.

Unmanned aerial vehicles Varieties

Helicopters with an one propeller

Only one rotor aircraft resembles small helicopters. They could be either electrical or fuel powered. The capability of a mono blade, gas-powered uav to stabilise and assist in long haul flights. These drones are mainly build for carrying heavier objects, like the LIDAR system, which is used to survey the ground or the storm and map erosion.

Drones with Several Rotors

Multi-rotor uavs are the smallest & smallest among all kinds of uavs. Since, it is small in size, it has limited range, speed and altitude, but it is an ideal aircraft for hobbyists and aerial photography. These drones can typically fly in the air for around 20-30 minutes with a light payload like a camera.

Uavs with Fixed Wings

Fixed-wing uavs characterized mainly uav, but its wings offer greater pull than rotor, make them completely effective. Such drone typically run on gasoline instead of power, enabling it to stay airborne for further nearly 16 hours. Such uavs are typically much larger &, by design, can fly and land on runway like aircraft. The army needs fixed-wing Drones to perform attacks, researchers are using them to carry large amounts of equipment, or even non-profit organisations use them to deliver food and other goods to difficult places.

3.2.5 Is a licence required to fly a drone?

Until 2016, all business firms employing drone technology, regardless of industry, were needed to hold a licence. New government laws, however, have already been put in place which enable commercial uavs to get a Flying Control Agents remotely by undergoing a pilots proficiency test. The exam includes 60 optional questions covering subjects such as UAS measurement regulations, restrictions and Uavs operations, climate impacts on UAS operations, emergency procedures, airport laws, decision making, care, and much more. A person must be at least 16 years old, able to read, understand, speak, and write English, and physically and psychologically fit to fly a drone to qualify for the exam.

3.2.6 What are communication medium of Drone?

Drones are the common flying device that do not hold pilots with it. These are controlled by a person sitting on the ground who holds some sort of contol device which is contains a transmitter which is responsible for generating signals to communicate with the drones. The transmitter generates the signals, and these signals are transmitted in to the air and are send to the Drone via a communication medium. Once the signals are sent by the transmitter via the communication system, the receivers in the drone receive these signals and function accordingly.

There are various communication media used in drone technology. These are:

(1) Radio Frequencies

This is the most commonly used communication channel in the dron system. Radio frequencies are the invisible waves that are a part of the electromagnetic spectrum. For the system to establish the communication

link, both the transmitter and the receiver are required to be operated in the same frequency. This type of communication medium uses RFID or Radio Frequency Identification which is an identification code which is being assigned to both the transmitter in the controller and the receiver in the drone. RFID enables the system to uniquely establish the connection between the transmitter and the receiver. The drone only responds to those signals which are sent by transmitter with that specific RFID.

(2) Wi-Fi

Since, drones are popularly used for security purposes, the controllers are basically the app and the drones are generally equiped with a camera. To establish the communication and to stream the video, Wi-Fi is the more appropriate one to use as the communication medium. Wi-Fi enables the drone system to stream the video footage from a drone in real-time, thereby establishing the real-time communication between the controller and the drone. Unlike radio frequencies, Wi-Fi operates on very high frequencies and hence are best used for shorter ranges.

(3) Global Position System (GPS)

GPS has further enhanced the Wi-Fi communication system. It does this by improving stability, enabling Return Home, and identifying non-Fly zones. In GPS based communication medium, a GPS is attached to the drone. Drones receive the coordinates from the controller and the GPS of the drone simply follow these coordinates.

(4) Satellite Link

Drones are also very commonly used as military drones. The above mentioned communication medium are only successful in short-range areas and fails for long distance communication. Since, military drones are mostly used in critical situations and for long distance reach, there is a high chance of signal loss during any point of time so, satellites become the trusted medium to communicate with the drone. With satellite based communication system, military can easily control their drones while they are thousands of miles away.

3.2.7 What are security mechanism of drone?

Drones are popularly used for security and surveillance purposes. With simpler, faster and cheaper drone security mechanism, they are an ideal solution for security uses over other security methods.

The security mechanism in the drones is very simple. Drones are equipped with cameras and other sensors which are responsible for gathering the data from the surroundings. There are algorithms written for the drones to autonomously gather the data from the surroundings. The acquired images and data are then processed by the drones. This processing is nothing but the conversion of the collected images and data into the codes so that the drone can understand. This converted data is further compared with the predefined thresholds set up by the user. With the help of these thresholds, the drones are able to detect the anomalies or

the security breaches, if any. If such anomalies are found, then the drone sends a signal to the controller of the system indicating that a breach is found which further triggers an alarm to the user.

Further, to detect the human motion as part of drone security mechanism, there are heat sensors installed in the drones which allow to detect the body temperatures. For detecting human motion, the drone first collects the data as seen by the camera and process this data into the understandable code. It then compares the recorded features with actual human features provided by the user. If the comparison is true i.e., if the human body is found, then the drone starts tracking the motion of the human body. Thus, in this way, the security system of the drones track the human motion.

3.2. FLOWCHARTS

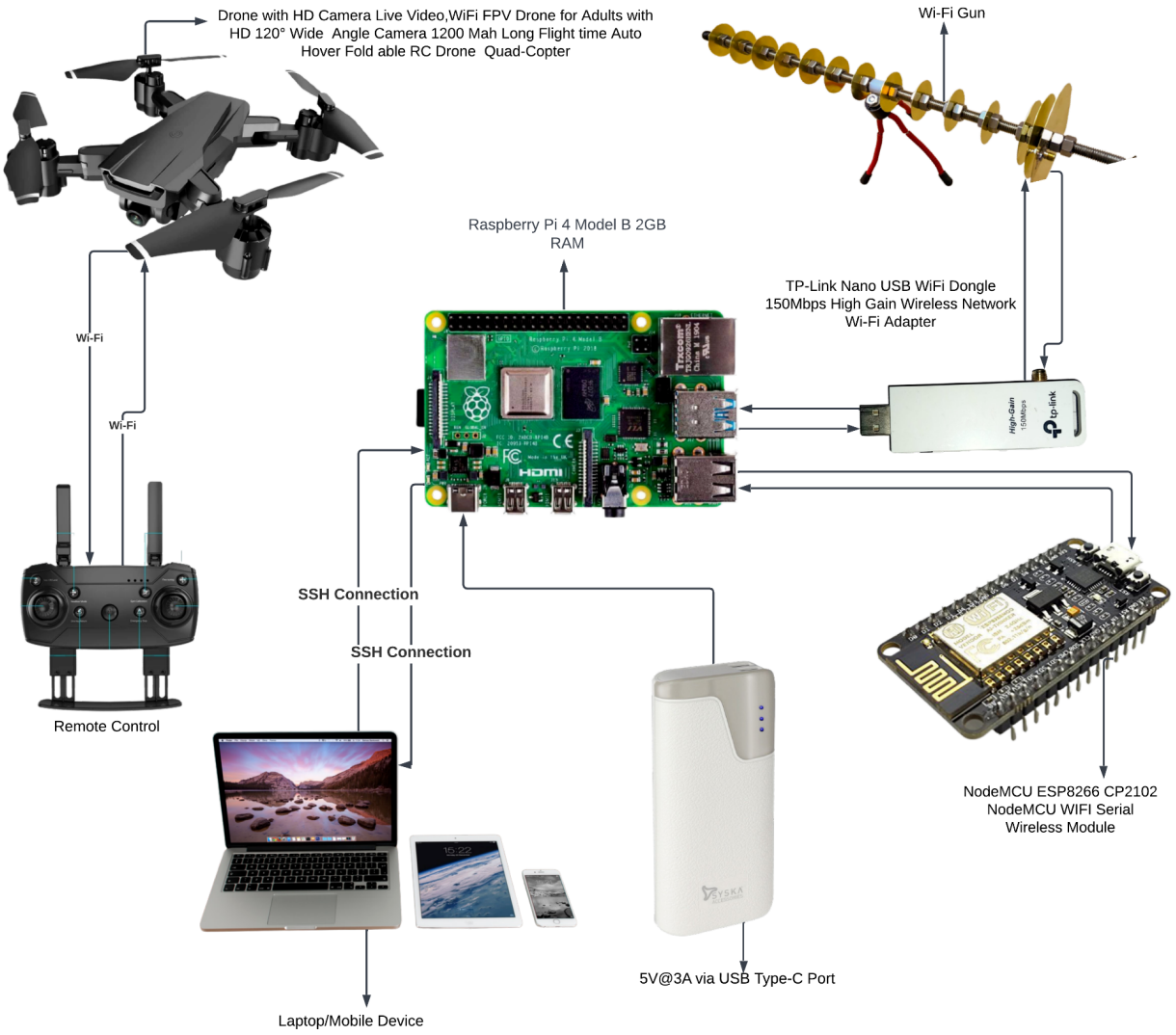


Fig.12 Showing the working of the device

3.3 Algorithms/ Code

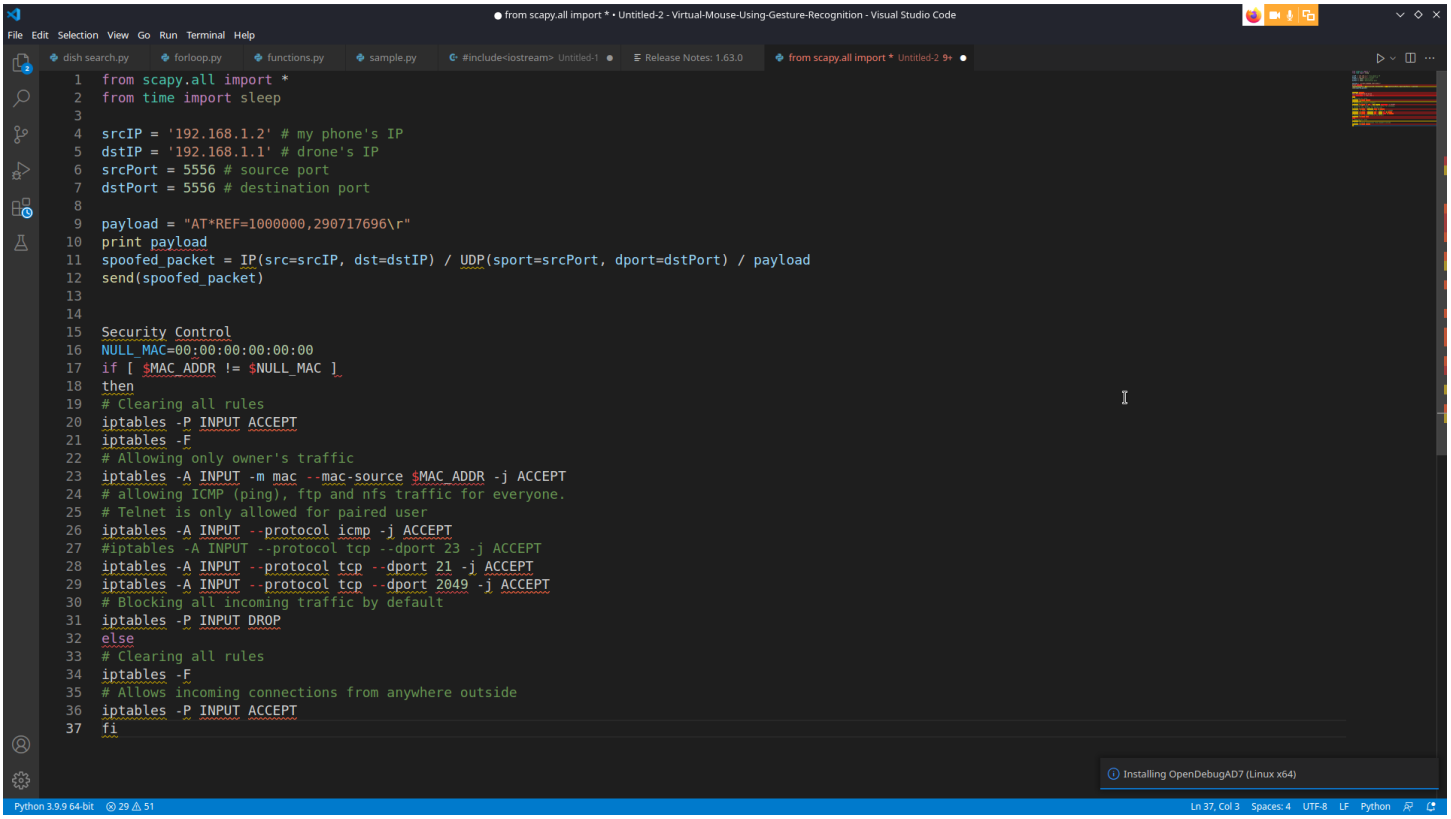


Fig.13, Code for drone hacking

3.4 Testing Process

A Wi-Fi gun is a combination of two types of Wi-Fi hotspots that can transmit or receive signals from one to hundreds of miles from where they are installed. This depends on how you set it up, where you put it, or what items you will use. This device also works very well on both laptops and smartphones. Also, this powerful machine is made of simple and inexpensive materials and is very easy to make. When done right, you can easily find a powerful and efficient Wi-Fi signal anywhere you go without any hassle.

Components to be used

Brass Sheet Metal 0.016 ″ X 6 ″ X 12 ″ Quantity: 1

You Need To Cut The Next Circles From A Piece Of

Steel

90mm Circle Size: 1

68mm Circle Size: 1

54mm Circle Size: 1

38mm Circle Size: 1

37mm Circle Size: 3

Each circle will need to be drilled in the middle of the circles. What Will Fit The Whole Series. "Please note".

You will need A Piece Of Every Thing 6 1/2 inches Or 165mm in Length “I Used 5/16 Inch Or 8mm Dia”. You will need about 12 nuts that will be used throughout the series.

How can I make my own WiFi antenna?

In order to make the Wifi Gun, you will need a long threaded (50 cm long), a straight rod, Bolts, and a Wire connector. You will also need a metric ruler, scissors, and aluminum sheet cutters.

Why do we go for the Wi-Fi gun?

A Wi-Fi gun is an antenna used to access Wi-Fi networks located over long distances. It is a very simple tool that users can install to Get long-distance Wi-Fi easily and with good internet speed. It covers up to 1km of coverage area. It is useful for college Campuses, Trekking Camps, Wildlife Photographers Camps, Bus Stands, and Railway Stations through which we can achieve a range of up to 2 km.

How Efficient is This Technology?

This gun is easy to build, inexpensive, reliable, and easy to repair and maintain. After reviewing many articles, there is one research paper that discussed improving Wi-Fi coverage; However, there is no mention of being actuators to adjust.

Need of the WI-FI Extender.

Ordinary consumer Wi-Fi hotspots are limited and do not provide coverage for the entire city of Wi-Fi networks. The Wi-Fi router covers an area of about 150m. Users cannot access Wi-Fi beyond that range, even if they are away from Wi-Fi and get low internet speed. In a large area of the campus or in any of the stations we can not get Wi-Fi access from one end to the other.

Today it is so important to have long-range Wi-Fi.

3.5. METHODOLOGY

This antenna is a directional wavelength antenna consisting of a metal disc linked in series. The suggested system includes a copper disc plate antenna, as shown in block Fig. This comprises a number of disc plates. This indicates that it is linked to a Wi-Fi module. The Antenna's primary job is to focus on signal strength in order to receive radio waves in communication equipment such as the Internet, ad hoc and mobile networks, wireless cards, and so on. When compared to standard horns, this performs extremely well at receiving signals over a large region of low strength. The shiny part transmits information to contacts while providing a minor diversion. The reception signal of the disc antenna may be modified, allowing it to be utilised in a range of situations.

ANTENNA DESIGN

The antenna is based on the idea of a circular waveguide selection frequency is the most important part of the design. As in Wi-Fi network devices operate at frequencies ranging

from 2412 GHz to 2462 GHz. Appropriately, the TE11 disconnection frequency should be less than 2412 GHz and the TM01 cut-off frequency should be higher than 2462 GHz.

3.6. ANTENNA CIRCUIT DESCRIPTION

A. Copper Plates

The antenna is built on the widely held belief that the circular waveguide is the most significant component of the design. Wi-Fi network devices use frequencies spanning from 2.412 GHz to 2.462 GHz. TE11 disconnection frequency should be less than 2.412 GHz and TM01 cut-off frequency should be more than 2.462 GHz.

B. Wireless Router

The antenna is built around a traditional perspective of the circular waveguide, which is the most significant aspect of the construction. Wi-Fi network equipment, for example, operate in frequencies ranging from 2.412GHz to 2.462GHz. The appropriate TE11 disconnection frequency is less than 2.412 GHz, whereas the TM01 cut-off frequency is more than 2.462 GHz.

C. SubMiniature A connector

SMA connections (SubMiniature version A) are very small semi-precision coaxial RF connectors developed in the 1960s. Coaxial optical connection with screw-type binding mechanism. The connection features a 50-second delay. SMA is intended for usage from DC (0 Hz) to 18 GHz, however it is most typically seen in portable radios, mobile phone sticks, and, more lately, Wi-Fi hotspots. It has a wide range of uses for delivering RF link connections within devices that require coaxial communication. A 50 Ohm impedance connection to an external antenna (GPS, Bluetooth, mobile, Nordic, and XBee) is required for SMA connections. Using SMA connections, it is frequently used to provide RF communication between boards and numerous microwave components like as filters, attenuators, mixers, and oscillators.

3.7. Steps to make Wifi Big Gun:-

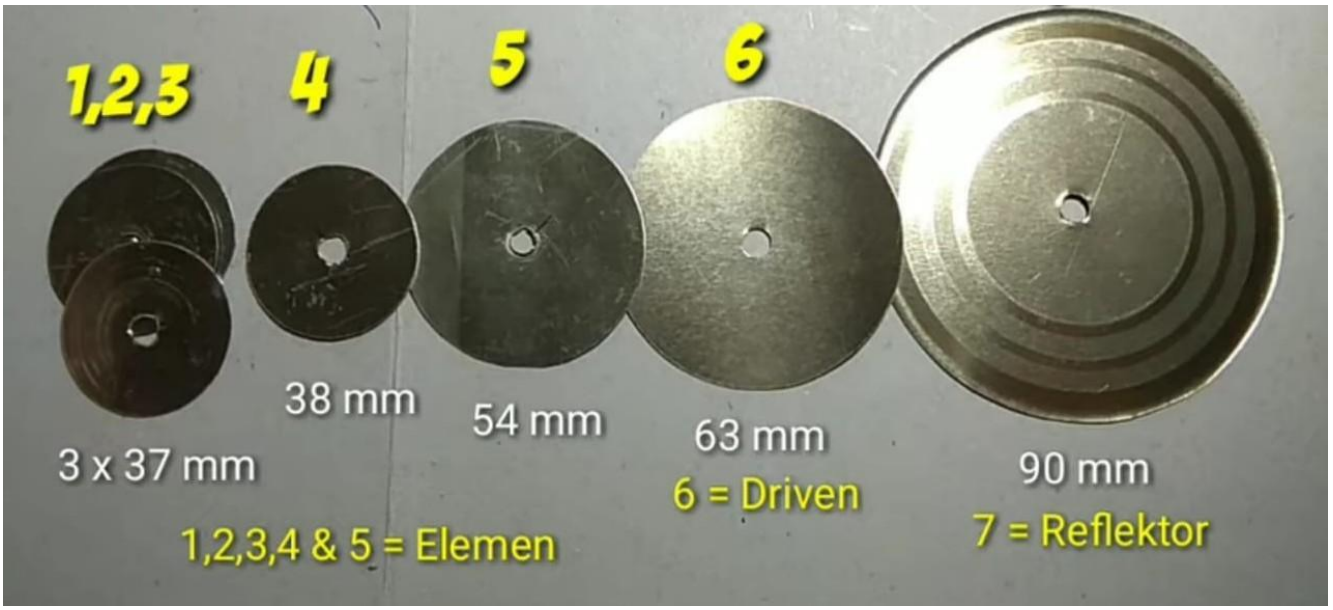


Fig.14. Dimensions to cut the aluminum sheet

Fig.15. Showing no, of pieces of aluminum circles.

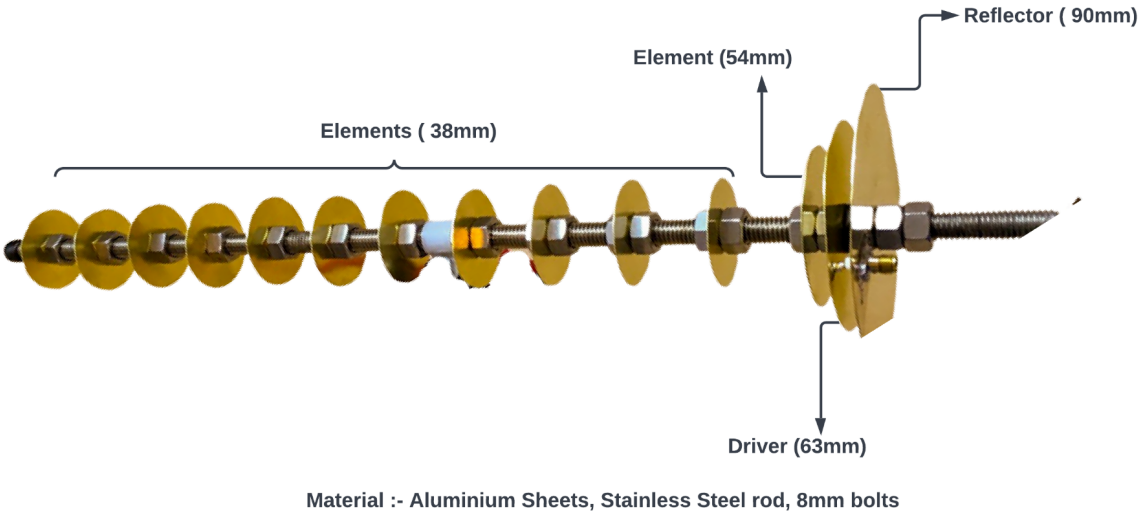


Fig. 16. Completed structure of Wi-Fi Gun.

3.8. FUTURE SCOPE

We can implement this module on the base station extending the range of the Wi-Fi. We can use this module in low network areas. This module can be carried along for adventure activities (trekking, wildlife photography, off-road racing/biking, etc.) where the network percentage is very low. This module can be installed in the Institutes and Corporate offices which cover large campus areas where it becomes difficult to provide a long-range network.

4. RESULTS/OUTPUTS

1) A process of Auditing the Network, Capture Handshake, finding anomalies in IoT devices, and capturing wireless signals within the range of 4 to 5Km. A compact machine consists of capturing signal mechanisms with the computing power from any static location having a range of 4 to 5 km.

2) A process in claim 1 also adds the vulnerability assessment in wireless devices. Computing power allows the automation of finding vulnerabilities, drone jamming, and response to incidents.

3) A process for treating wireless devices, the process being substantial as described herein with reference to and as illustrated in the accompanying drawings.

4) Machine for treating wireless devices, This machine comprises a Wi-fi gun, Raspberry Pi 4 Model B with 2GB of RAM, and NodeMCU Esp8266 for increasing the range of Wi-Fi signal up to 5 Km with automation scripting for jamming drone or anomaly detection in IoT.

5. CONCLUSION

"Wi-Fi Gun" antenna incorporates features like long-distance (500m-1Km) better quality network providers that are lacking in the conventional Wi-Fi routers which are restricted to 150 to 200 m. The design of the Wi-Fi gun has shown satisfactory results and works well by providing a long-distance range network. It works well to provide a long-distance delivery of a Wi-Fi network.

6. IMPROVEMENTS

- In this machine we can also increase the range of the antenna using AC current so that we are able to capture signals from a very long range.
- As we are using this system for anomaly detection, Also need to fine-tune our anomaly detection techniques by integrating machine learning techniques.
- This can also be used as radar for security purposes. Under that condition, we have to fine-tune our process of detection and de-authenticating higher levels of encryption techniques.
- We can also increase the computing power of this device by integrating more than 1 raspberry pie or manually integrating a CPU.

7. REFERENCES

[1] Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and mitigation of evil Twin attack in Sdn Enabled wifi. IEEE Transactions on Network and Service Management, 17(1), 89-102. doi:10.1109/tnsm.2020.297277

[2] Lounis, K., & Zulkernine,M.(2020).IEEE Access, 8,88892-88932. doi:10.1109/access.2020 .2993553

[3] Akram, Z., Saeed, M. A., & Daud, M. (2018). Real-time exploitation of security mechanisms of residential WLAN access points. 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). doi:10.1109/icomet.2018.8346378

[4] Tian, Z., Li, Y., Zhou, M., & Li, Z. (2018). Wifi-based adaptive indoor passive intrusion detection. 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP). doi:10.1109/icdsp.2018.8631613

[5] Wen, Y., & Liu, T. (2018). Wifi security certification through device information. 2018 International Conference on Sensor Networks and Signal Processing (SNSP). doi:10.1109/snsp.2018.00065

[6] Noh, J., Kim, J., & Cho, S. (2018). IEEE Access, 6, 16539-16548. doi:10.1109/access.2018.2809614

[7] Satam, P., & Hariri, S. (2021). WIDS: An ANOMALY-based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18(1), 1077-1091. doi:10.1109/tnsm.2020.3036138

[8] Cook, A. A., Misirli, G., & Fan, Z. (2020). Anomaly detection for IoT time-series data: A survey. IEEE Internet of Things Journal, 7(7), 6481-6494. doi:10.1109/jiot.2019.2958185

[9] Zhu, Q., & Sun, L. (2020). IEEE Access, 8, 31398-31408. doi:10.1109/access.2020.2973214

[10] Sahu, N. K., & Mukherjee, I. (2020). (ICOEI)(48184). doi:10.1109/icoei48184.2020.9142921

[11] Hahnsang Kim, Shin, K. G., & Pillai, P. (2011). IEEE Transactions on Mobile Computing, 10(7), 968-981. doi:10.1109/tmc.2010.245

[12] Hwang, R., Peng, M., Huang, C., Lin, P., & Nguyen, V. (2020). An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access, 8, 30387-30399. doi:10.1109/access.2020.2973023

[13] Lounis, K., & Zulkernine, M. (2020). Attacks and defenses in short-range wireless technologies for IoT. IEEE Access, 8, 88892-88932. doi:10.1109/access.2020.2993553

[14] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743. doi:10.1109/access.2019.2924045

[15] Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal, 5(1),269-282.doi:10.1109/jiot.2017.2780232

[16] Gauniyal, R., & Jain, S. (2019). IoT security in wireless devices. 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA). doi:10.1109/iceca.2019.8822124

[17] Shao, C., Park, H., Roh, H., Lee, W., & Kim, H. (2020). IEEE/ACM Transactions on Networking, 28(4), 1587-1600. doi:10.1109/tnet.2020.2989387

[18] Yoon, S., & Kim, J. (2017). Remote security management server for IoT devices. 2017 International Conference on Information and Communication Technology Convergence (ICTC). doi:10.1109/ictc.2017.8190885