Y-ROV NETWORK ANALYZER

A PROJECT REPORT

Submitted by

OLEEVIYA BABU P (MES16CS092)
REZWIN RAFEEK V (MES16CS095)
SANGEETHA SHEKARAN (MES16CS099)
SANIN PK (MES16CS100)

to

the APJ Abdul Kalam Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology

in

Computer Science and Engineering

(ISO 9001:2008 Certified)

Department of Computer Science and Engineering
(Accredited by NBA)
MES College of Engineering Kuttippuram
Thrikkanapuram P.O., Malappuram Dt., Kerala, India 679573

NOV 2019

DECLARATION

We, hereby declare that the interim project report ”YRov Network Analyzer”, submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done under the supervision of Mr Shajeesh KU, Assistant Professor, Computer Science and Engineering. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place: Kuttippuram
Date:

Oleeviya Babu P

Rezwin Rafeek

Sangeetha Shekaran

Sanin PK

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MES COLLEGE OF ENGINEERING, KUTTIPPURAM

(ISO 9001:2008 Certified)

CERTIFICATE

This is to certify that the report entitled **"Y-ROV Network Analyser"** submitted by **OLEEVIYA BABU P, REZWIN RAFEEK V, SANGEETHA SHEKARAN, SANIN PK**, to the APJ Abdul Kalam University in partial requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering is a bonafide record of the project work carried out under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor:
Mr. Shajeesh KU
Assistant Professor
Dept. of Computer Science and Engineering .
MES College of Engineering

HEAD OF THE DEPARTMENT :
Dr. Sasidharan Sreedharan
Dept. of Computer Science Engg.
MES College of Engineering

PROJECT Coordinators :

Mr.Sherikh KK
Assistant Professor
Dept. of Computer Science and Engineering .
MES College of Engineering

Mr Viju P Poonthottam
Assistant Professor
Dept.of Computer Science and Engg.
MES College of Engineering

Mrs. Indu P

Assistant Professor

Dept.of Computer Science and Engg.

MES College of Engineering

ACKNOWLEDGEMENT

First of all we wish to thank God Almighty for blessing that made this work a success. We're grateful to *Dr. A. S. Varadarajan, Principal, MES College of Engineering, Kuttippuram,* for providing the right ambiance to do this project. We would like to extend my sincere gratitude to *Dr. Sasidharan Sreedharan, Head of the Department, CSE, MES College of Engineering, Kuttippuram.*

We're deeply indebted to the project coordinators *Mr Sherikh K K, Assistant Professor, Department of Computer Science and Engineering and Mr Viju P Poonthottam, Assistant Professor, Department of Computer Science and Engineering* for his continued support.

It is with great pleasure that we express deep sense of gratitude to our project guide *Mr Shajeesh KU, Assisstant Professor, Department of Computer Science Engineering,* for his guidance, supervision, encouragement and valuable advice in each and every phases.

We would like to thank all other faculty members and fellow students of MES College of Engineering, Kuttippuram for their warm friendship, support and help.

Oleeviya Babu P

Rezwin Rafeek V

Sangeetha Shekaran

Sanin PK

ABSTRACT

A rover that is capable of maneuvering in dangerous territory such as enemy bases or any other hazardous environment. It has the ability to conduct reconnaissance and surveillance operations and it can also initiate denial of service attacks on nearby Wireless access points if necessary. It can also provide other network details like security type, broadcasting channels, info regarding the devices connected to that Access point etc. IoT is gaining importance in our lives and in the military too. The application of IoT paradigm in the military facilitates the commanders to make real-time decisions. However, cybersecurity threats to weapon systems intensify along with the growing of IoT's benefits. Coping with these cybersecurity threats nowadays, but not traditional security solutions. Since only developed countries are capable of developing systems on their own, they need to adopt "security by design" but normally they show a lack of concern leaving these systems vulnerable to attack. However, precautions to stop these kind of attacks are generally not taken as even the protocol used in wireless transmissions are inherently flawed and can be exploited even from outside the network thereby allowing to take control of theses devices causing grave risk to personnel. Here we proposed a new machine that can evaluate networks that could be used to integrate IoT devices and components and a method to address cybersecurity related issues.

CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AP	Access Point
IoT	Internet of Things
DoS	Denial of Services

CHAPTER 1
INTRODUCTION

Y-rov is a military rover that is capable of performing surveillance over a certain area and is also able to initiate Denial of Service(DoS) attacks against selected wireless access points. It can also analyze a wireless access point and provide us with details like type of encryption used by the network, MAC address of the router and all the stations associated with it. It can be controlled remotely over the internet by use of remote desktop protocol. The Internet of Things (IoT) is used in military by integrating systems of sensors, actuators, and control systems into existing military infrastructures, the military can become more efficient and effective.It is used in:-

Logistics :- The connected sensors and digital analytics that IoT technology offers can be used to track supplies and equipment from their source to where they are needed on the battlefield.

Smart Bases :- Automated security screening, for example, increases safety while decreasing manpower, and a network of security cameras connected to their environment via sensors and to a central network via the Internet will also minimize security risks.

Data Warfare :- By collecting data from a wide range of military platforms – including aircraft, weapon systems, ground vehicles, and troops themselves – the military can increase the effectiveness of their intelligence, surveillance, and reconnaissance systems. But IoT is heavily dependent on wireless networks and most routers nowadays use the wpa2 protocol for security. WPA2 has certain design issues that can be exploited and hence it provides a huge upper hand to any army which can remotely

attack these networks and it is also quite import to analyze one's own network to safeguard from such attacks ,this is were Y-ROV is useful.

CHAPTER 2
LITERATURE SURVEY

The existing way of penetrating enemy bases is to deploy police/military personal in these dangerous environments and thereby putting their lives at risk and performing network analysis in these stressful environment is next to impossible and performing DoS attacks will give-away their location hence leaving them vulnerable to counter attacks. They also suffer from various other drawbacks that are humane in nature that is slow response time, lower visibility in dark areas, inability to move with stealth and the cost of losing lives is one which we cannot inflict as in today's world these dangerous jobs can be easily handled by machines that can be made much more capable with adequate effort and even if a loss does occur it will be a financial one than a loss of a human life and the same skilled officers can operate these rovers remotely thereby they can use their skills to much better effect as they are no longer exposed to the same amount of stress to which they might have been exposed to had they been in the field themselves, from the above mentioned facts it is quite clear that the proposed system is much better than the existing system.

2.1 fundamentals of existing method

Military strategy is the planning and execution of the contest between groups of armed adversaries.Strategy, which is a subdiscipline of warfare and of foreign policy, is a principal tool to secure national interests. t is larger in perspective than military tactics, which involves the disposition and maneuver of units on a particular sea or battlefield, but less broad than grand strategy otherwise called national strategy, which is the overarching strategy of the largest of organizations such as the nation

state, confederation, or international alliance and involves using diplomatic, informational, military and economic resources.But all the strategies takes away the life of our protectors or the existing way of penetrating enemy bases is to deploy military /police personal in dangerous.

2.2 Principles of existing method

Many military strategists have attempted to encapsulate a successful strategy in a set of principles.

2.2.1 Objective

Direct every military operation towards a clearly defined, decisive, and attainable objective.

2.2.2 Offensive

Seize, retain, and exploit the initiative.

2.2.3 Economy of Force

Allocate minimum essential combat power to secondary efforts.

2.2.4 Security

Never permit the enemy to acquire an unexpected advantage. and also know about the security of the life of the military force/police.

2.2.5 Surprise

Strike the enemy at a time, at a place, or in a manner for which he is unprepared.

But all the above principles can't protect the life of the military/police.There is a chance to lost the valuable life of our army/police.All the above principles need to be preserved along with that the, life of everyone need to be protected .For that ,the existing way of penetrating into the enemy bases along with the above mentioned principles need to be showcased.

2.3 robots instead of soldiers: PackBot

Military robots have always been pretty dumb. The PackBot the US Army uses for inspections and bomb disposal, for example, has practically no on board intelligence and is piloted by remote control. What the Army has long wanted instead are intelligent robot teammates that can follow orders without constant supervision.

Figure 2.1: packBot

That is now a step closer. The Army's research lab has developed software that lets robots understand verbal instructions, carry out a task, and report back. The potential rewards are tremendous. A robot that can understand commands and has a degree of machine intelligence would one day be able to go ahead of troops and check for IEDs or ambushes. It could also reduce the number of human soldiers needed on the ground.

"Even self-driving cars don't have a high enough level of understanding to be able to follow instructions from another person and carry out a complex mission," says

Nicholas Roy of MIT, who was part of the team behind the project. “But our robot can do exactly that.”

CHAPTER 3
SYSTEM ANALYSIS

3.1 Existing System

The Existing System relies on human officers to do the job of penetrating into enemy bases and carrying out operations from the enemy bases with their own devices leaving them vulnerable to enemy attacks.

The U.S. is already using unmanned aerial vehicles to conduct surveillance and drop missiles on suspected terrorists overseas in places like Pakistan and Yemen.

That's not to mention how drones have also been deployed stateside to check up on the folks at home. The efficacy and morality of these and other operations are controversial, but supporters say drones are less costly, minimize collateral damage and don't require putting American troops at risk. That's partly because humans can operate these machines – often in far flung, dangerous places – from the safety and comfort of a domestic operations center. [source: Byman]

While drones do their work from high above, other robots are operating on the ground in battlefields worldwide. American forces relied on bomb-squad robots to inspect and defuse possible explosive devices during military operations in Iraq and Afghanistan. The remote-controlled machines moved via tank tread and featured infrared vision, multiple cameras, floodlights and mechanical arms in order to spot bombs and dispose of them, all while human operators stayed a safe distance away [source: Shachtman]

3.1.1 Special Weapons Observation Remote Reconnaissance Direct Action System(SWORDS)

In 2005, Special Weapons Observation Remote Reconnaissance Direct Action System(SWORDS) machines became the first armed ground robots to see action on the ground when U.S. military forces put them to work in Iraq. Equipped with light machine guns, the robots were also mobile, but skittish military officials opted to keep them in fixed locations where they were used to defend perimeters rather than actively chase after bad guys [source: Magnuson].

Military officials have yet to OK the use of armed bots that can shoot autonomously, maintaining that the decision to use deadly force should ultimately be made by a human [source: Magnuson]. But armed robots are being developed to do more than just play defense.

Figure 3.1: Maj. Michael Pottratz (L), explosive ordnance disposal deputy director of technology for the U.S. Armament Research, Development and Engineering Center, explains the functions of the SWORDS robot at a technology conference in 2008.

3.2 Proposed System

A rover that can be remotely controlled over the internet.It Sends live video feed back to the user and can perform Denial of Service attacks on Wireless AP's. It can also provide details of each Wireless AP's like it's security details,bssid,essid. It provide details of the client devices connected to that device.

CHAPTER 4

System Requirements

4.1 Hardware Requirements

RaspberryPi 3B+
Panda Wireless PAU09 N600 Dual Band
4g dongle
32 GB class 10 SD Card
Powersupply (10000 mAH Powerbank)
Pi Camera Module – 5MP

4.1.1 Raspberry Pi 3B+

The Raspberry Pi 3 Model B+ is the latest product in the Raspberry Pi 3 range launched on 14 March 2018 with great enhancements.

It is a credit card sized computer boasting an updated 64-bit quad core processor running at 1.4GHz with built-in metal heatsink,a three-times faster gigabit Ethernet (throughput limited to ca. 300 Mbit/s by the internal USB 2.0 connection) and 2.4 / 5 GHz dual-band 802.11ac Wi-Fi, and PoE capability via a separate PoE HAT.

Power over Ethernet or PoE describes any of several standard or ad hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices

such as wireless access points, IP cameras, and VoIP phones.

The dual-band wireless LAN comes with modular compliance certification, allowing the board to be designed into end products with significantly reduced wireless LAN compliance testing, improving both cost and time to market.

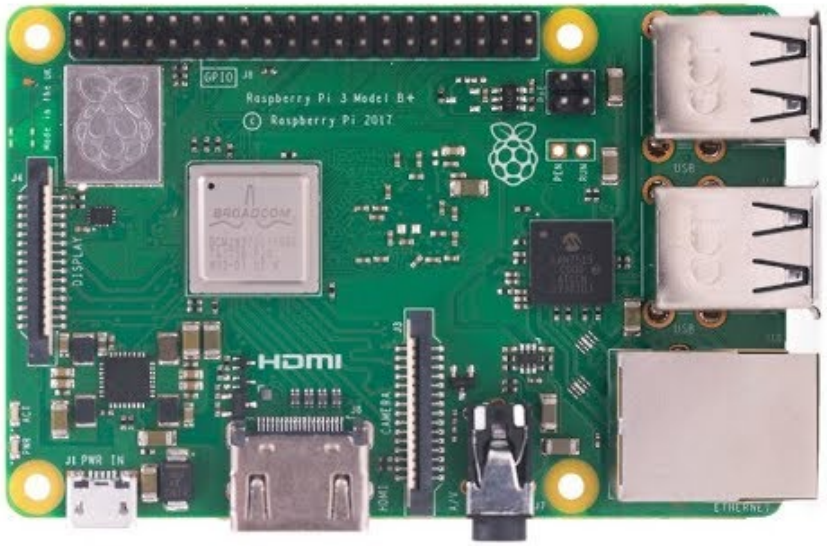

Figure 4.1: Raspberry Pi 3 model B+

4.1.2 Panda Wireless PAU09 N600Dual Band

The Panda PAU09 is a dual band (2.4GHZ and 5GHZ) wireless USB adapter with wide compatibility, from Windows 10 to Kali Linux. It also has two large 5dBi Rubber duck antennas to improve the distance a WiFi signal can travel and suitable for picking up weaker signals.

Panda PAU09 upgrades the WiFi interface on a computer to the latest 802.11n standard. It has Max data rate up to 300 Mpbs with any 802.11ac/n 2.4GHz and 5GHz networks. It has low power consumption to extend the battery life of your laptop or portable devices. It Supports state of the art standards-based security features

like 64b/128bit WEP, WPA and WPA2 to prevent unauthorized users to access your wireless network. It is compatible with most any version of Windows including XP/Vista/7/8/8.1/10/2012r2 32-bit and 64-bit. It is also compatible with Linux including Kali and going into monitor mode which is necessary to do Wireless Penetration Testing.

Figure 4.2: Panda Wireless PAU09 N600 Dual Band

4.1.3 4g dongle

A 4g dongle is a small device, which resembles a USB stick or “key”. It give you access to the mobile 4g network enabling you to connect to the Internet from your device from wherever you are. This is of course providing you have access to the network and, as with your mobile phone, have paid for access to the network. Like a USB key, the dongle fits into the USB port of a device such as a laptop, So the

plug-and-play capability that makes them popular.

4.1.4 32GB class 10 SD Card

SD cards have five different classes; Class 2, Class 4, Class 6, Class 8 and Class 10. The difference is mainly the speed of each one's minimum serial data writing speed. A Class 10 memory card supports sustained writing at 10Mb/s or better.It is the fastest, suitable for "full HD video recording" and "HD still consecutive recording". In Digital Single Lens Reflex (DSLR) , higher quality like class 10 is used.

4.1.5 Pi Camera Module – 5MP

The Pi camera module is a portable light weight camera that supports Raspberry Pi. It communicates with Pi using the MIPI camera serial interface protocol. It is normally used in image processing, machine learning or in surveillance projects. The 5MP camera module is perfect for small Raspberry Pi projects which have very little space allowance just boot up the latest version of Raspbian. It is connected to the Raspberry Pi via the camera port and it is used to provide visual feedback. It is fully Compatible with the Model A, Model B and Model B+ Raspberry Pi.

Figure 4.3: Raspberry Pi 5MP Camera Module

4.2 Software Requirements

Python3
Guizero
Aircrack-ng
BS4
Selenium
VNC Viewer
Chrome Remote Desktop
Raspian OS

4.2.1 Python

Python is a widely used general-purpose, interactive, object-oriented, and high-level programming language. It was initially designed by Guido van Rossum in 1991 and developed by Python Software Foundation. It was mainly developed for emphasis on code readability, and its syntax allows programmers to express concepts in fewer lines of code. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming. It is often described as a ”batteries included” language due to its comprehensive standard library.

4.2.2 Guizero

Guizero is a python modules that make the process of creating simple GUIs quick, accessible and understandable for new learners. Guizero is installed using command prompt and pip for Windows, macOS, Raspberry Pi and Linux. pip or pip3 is a

command line tool for installing Python 3 modules.

To install Guizero, **pip3 install guizero** command is used.

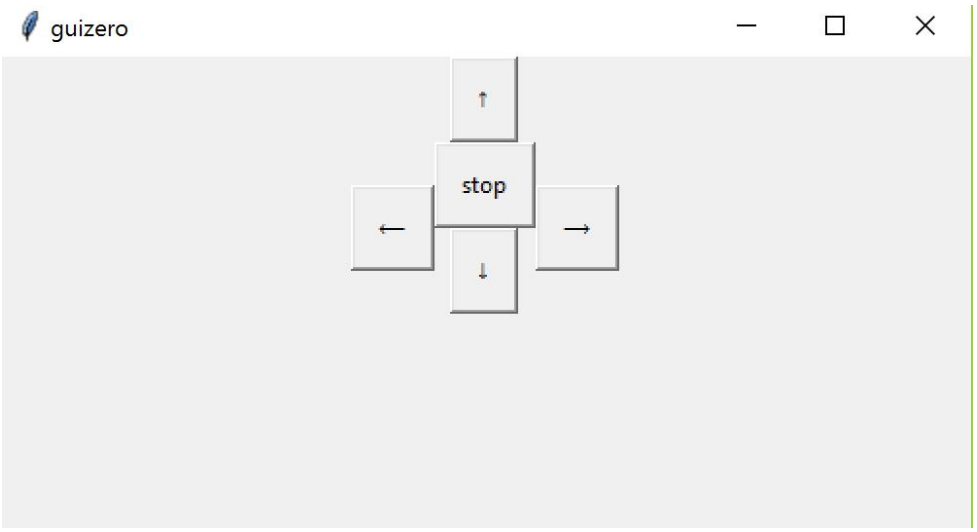

Figure 4.4: Push Buttons created using Guizero module

4.2.3 Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.

It focuses on different areas of WiFi security:

Monitoring: Packet capture and export of data to text files for further processing by third party tools

Attacking: Replay attacks, deauthentication, fake access points and others via packet injection

Testing: Checking WiFi cards and driver capabilities (capture and injection)

Cracking: WEP and WPA PSK (WPA 1 and 2)

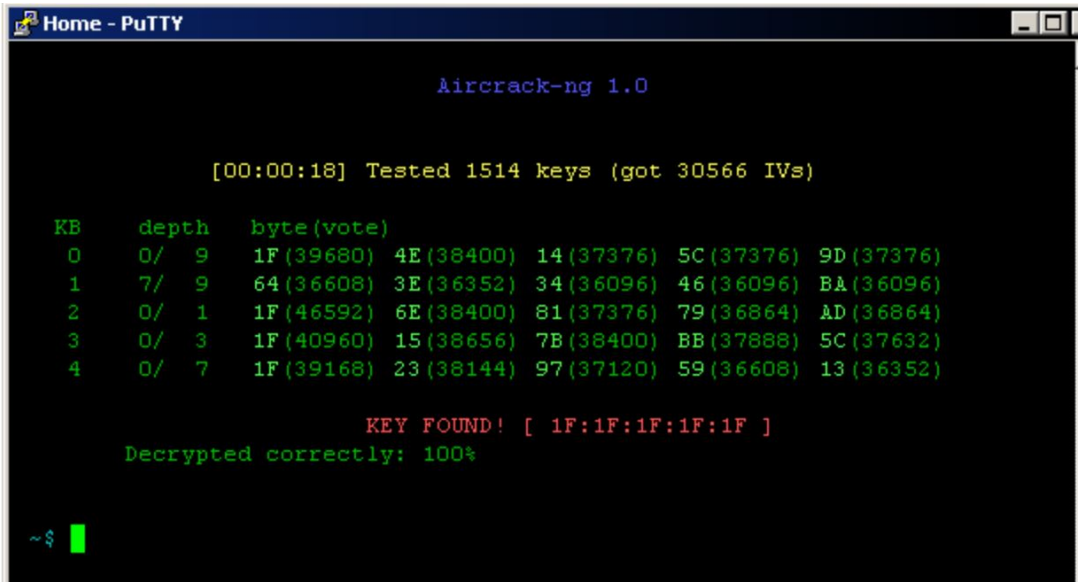

Figure 4.5: Aircrack-ng

4.2.4 BS4

Beautiful Soup is a Python library that parses HTML or XML documents into a tree structure that makes it easy to find and extract data. It works with parser to provide idiomatic ways of navigating, searching, and modifying the parse tree. It is often used for scraping data from websites. Beautiful Soup features a simple, Pythonic interface and automatic encoding conversion to make it easy to work with website data. Beautiful Soup 4 is published through PyPi, so it can't install it with the system packager, install it with **easy_install** using **easy_install beautifulsoup4** command or **pip** using **pip install beautifulsoup4** command.

Web Scraping:

Web Scraping (also termed Screen Scraping, Web Data Extraction, Web Harvesting etc.) is a technique employed to extract large amounts of data from websites using a software that simulates human web surfing, whereby the data is extracted and saved to a local file in your computer or to a database in table (spreadsheet) format.

4.2.5 Selenium

Selenium is a free (open-source) automated testing framework used to validate web applications across different browsers and platforms. The Selenium Test Scripts can be written as HTML tables or coded in a number of popular programming languages such as Java, c, Python and can be run directly in most modern web browsers. Testing done using the Selenium tool is referred to as Selenium Testing.

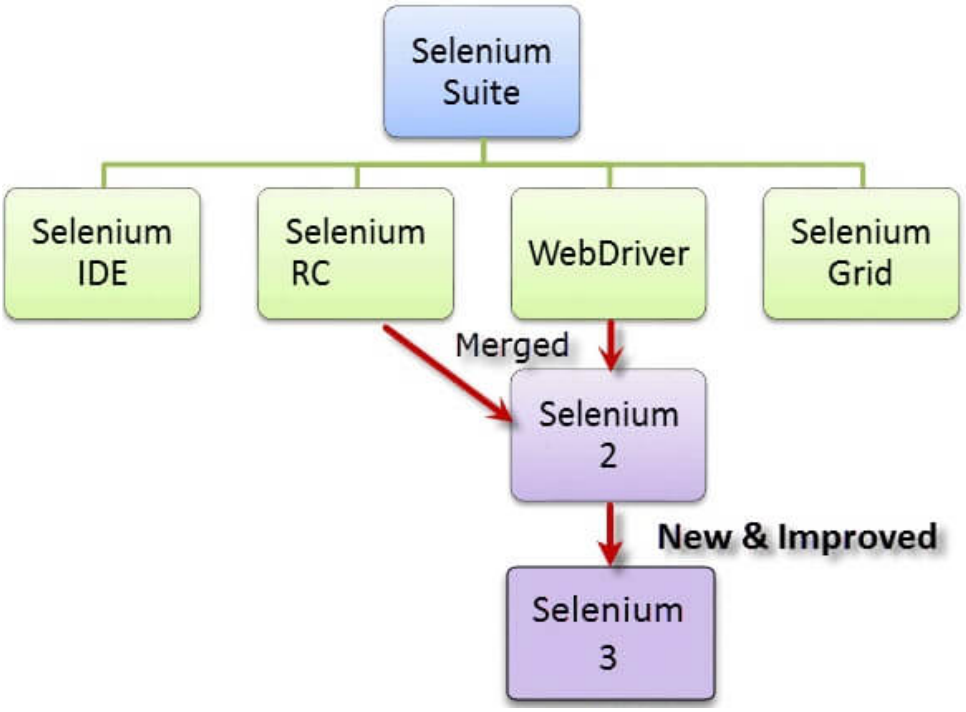

Figure 4.6: Components of Selenium Suite

Selenium suite consist of four tools:

1. Selenium Integrated Development Environment (IDE)

Shinya Kasatani of Japan created Selenium IDE, a Firefox extension that can automate the browser through a record-and-playback feature. It is the simplest framework in the Selenium suite and is the easiest one to learn. It is a Firefox plugin that can be installed than other plugin. However, because of its simplicity, Selenium IDE should

only be used as a prototyping tool.

2. Selenium RC

Selenium RC was the flagship testing framework of the whole Selenium project for a long time. This is the first automated web testing tool that allowed users to use a programming language they prefer. It has faster execution as compared to IDE.

3. WebDriver

The WebDriver proves itself to be better than both Selenium IDE and Selenium RC in many aspects. It implements a more modern and stable approach in automating the browser's actions. WebDriver, unlike Selenium RC, does not rely on JavaScript for Automation. It controls the browser by directly communicating with it. It has faster execution time than IDE and RC.

4. Selenium Grid

Selenium Grid is a tool used together with Selenium RC to run parallel tests across different machines and different browsers all at the same time. Parallel execution means running multiple tests at once.

Selenium RC and WebDriver are merged into a single framework to form Selenium 2 and Selenium 1 refers to Selenium RC.

4.2.6 VNC Viewer

VNC Viewer is a VNC Viewer (client). It can connect to any computer running a protocol-compliant VNC Server, displaying the remote desktop. VNC stands for vir-

tual network computing. This is a desktop sharing system that allows you to remotely control another computer. VNC works on a client/server model: A VNC viewer (or client) is installed on the local computer and connects to the server component, which must be installed on the remote computer. The server transmits a duplicate of the remote computer's display screen to the viewer. It also interprets commands coming from the viewer and carries them out on the remote computer. A virtual network computing system is platform dependant. This means that the client working on one type of operating system can't connect to the VNC server that operates on a different type of operating system.

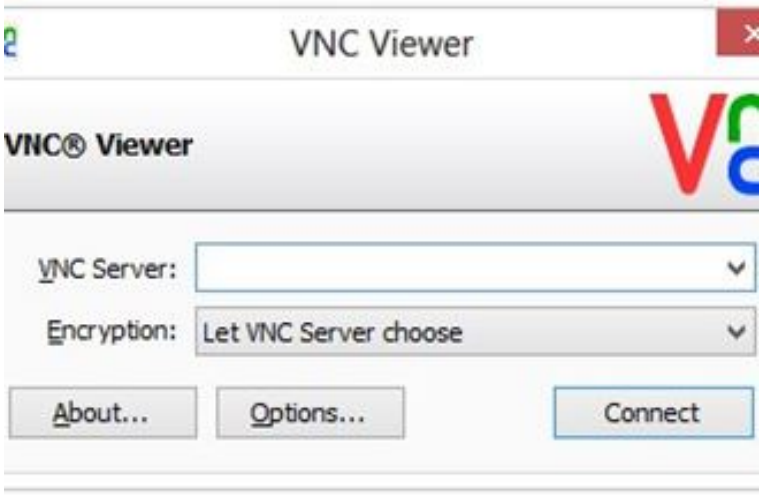

Figure 4.7: VNC Viewer

4.2.7 Chrome Remote Desktop

Chrome Remote Desktop is a remote desktop tool by Google that allows a user to remotely control another computer through a proprietary protocol called "Chromoting". It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. This feature therefore consists of a server component, for the host computer, and a

client component on the computer accessing the remote computer. ou can set up remote access to your Mac, Windows, or Linux computer.

Access a Computer remotely by:

STEP 1: Open Chrome in computer by:

STEP 2: In the address bar at the top, type remotedesktop.google.com/access, and press Enter.

STEP 3: Click Access to select which computer you want.

STEP 4: Enter the PIN required to access another computer.

STEP 5: Select the arrow to connect.

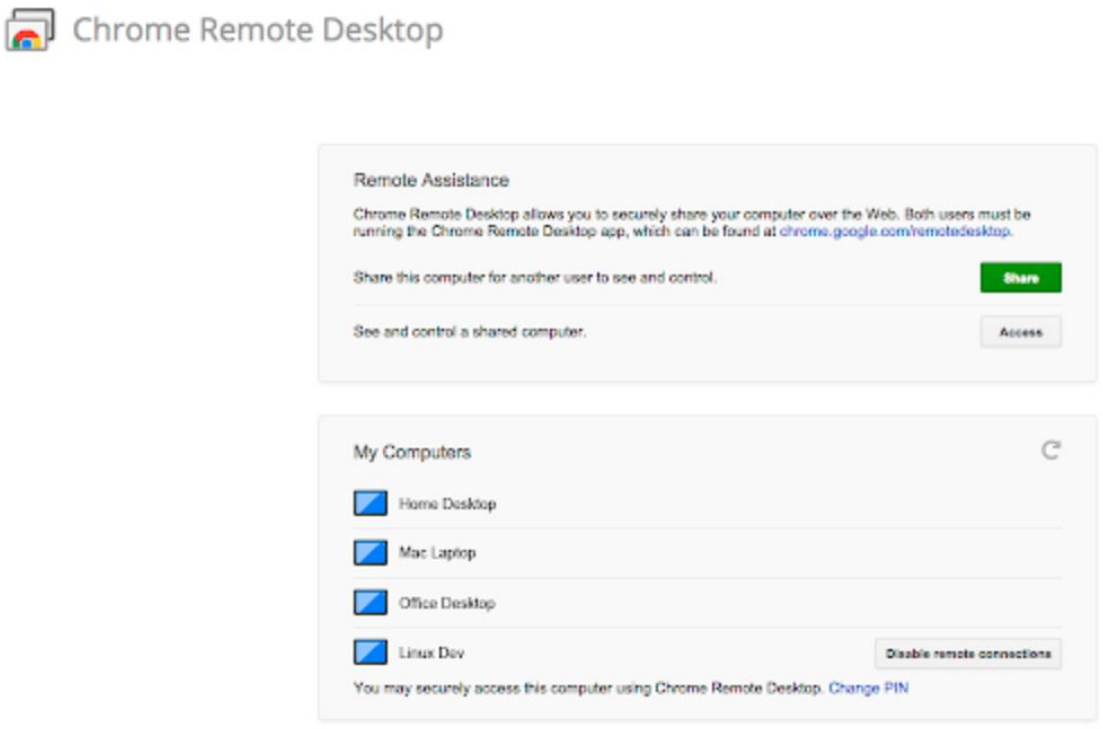

Figure 4.8: Setup Chrome Remote Desktop to Access Any PC Remotely

4.2.8 Raspbian OS

Raspbian is a Debian-based (32 bit) computer operating system for Raspberry Pi. Raspbian comes pre-installed with plenty of software for education, programming and general use. It comes with over 35,000 packages: precompiled software bundled in a nice format for easy installation on your Raspberry Pi. Raspbian uses PIXEL, Pi Improved X-Window Environment, Lightweight as its main desktop environment as of the latest update.

STEPS TO INSTALL RASPBIAN OS IN RASPBERRY PI

Step 1: **Download the Required Software and Files**

It is required to download 2 software and 1 OS i.e. Raspbian for this complete process. The first software is Win32 Disk Imager downloaded using `https://sourceforge.net/projects/win32diskimager/` and second software is SD Card Formatter using `https://www.sdcard.org/downloads/formatter_4/`, then extract all files to the desktop.

Step 2: Get the SD Card and the Card Reader

Get a minimum 8GB class 10 SD card with a card reader. Insert that card into the card reader and plug that to the USB port.

Step 3: Check the Drive in Which the SD Card Is Mounted

Go to my computer or My PC and find the drive name where the SD card is mounted.

step 4: Format the SD card

Open SD Card Formatter and select the drive that noticed in the previous step then Click on format and don't alter any other options. When formatting is completed, click on OK.

Step 5: Write the OS on the SD Card

Browse the .img file of Raspbian OS that was extracted from the downloaded file. Click on open and then click on Write. If any warning pops up then ignore those by clicking OK and Wait for the write to be completed.

step 6: Eject the SD card

Finally,the OS is installed in the Raspberry Pi.

CHAPTER 5
DESIGN

5.1 Basic Layout

The following figure illustrates the various components used and also the connection between those components

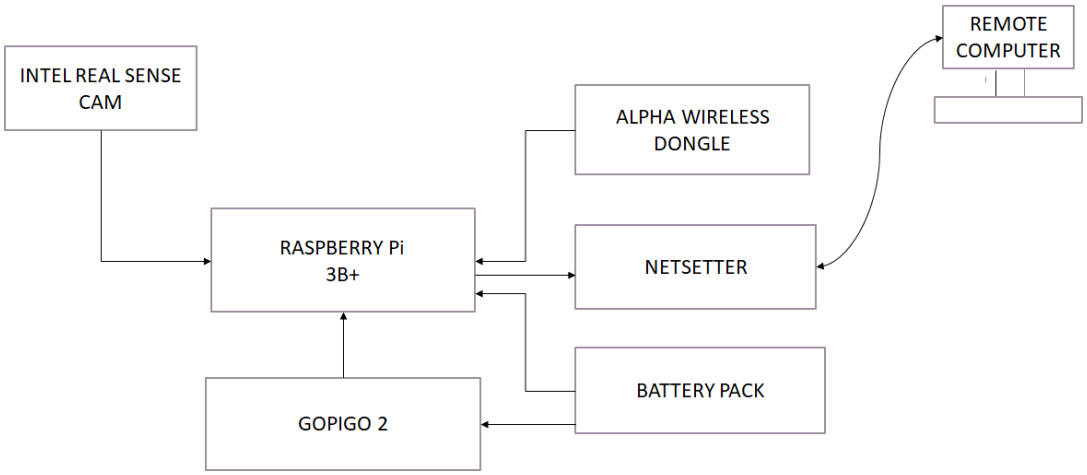

Figure 5.1: Block Diagram:Basic Layout

The basic connection layout is as shown in the figure above , A raspberry pi is mounted on top of a gopigo2, the gopigo2 is responsible for the movement of the rover and the RaspberryPi 3B+ handles all the processing workload. A Picam is connected to the Raspberry Pi via the camera port and it is used to provide visual feedback. A Netsetter(4g Dongle) and an Alpha Wireless Dongle is connected to the usb ports of the RPi . The functionality of the 4g dongle is to provide Internet connectivity to the rover so that it can send the video feed back to the remote computer and also accept control signals, Alpha wireless adapter is responsible for sniffing packets,monitoring,sending deauth packets etc.

5.2 Data Flow

The Remote Computer sends commands to the RPi over the internet. The Rpi then transfers these commands to the required device, it also send the data obtained from the connected devices back to the remote computer.

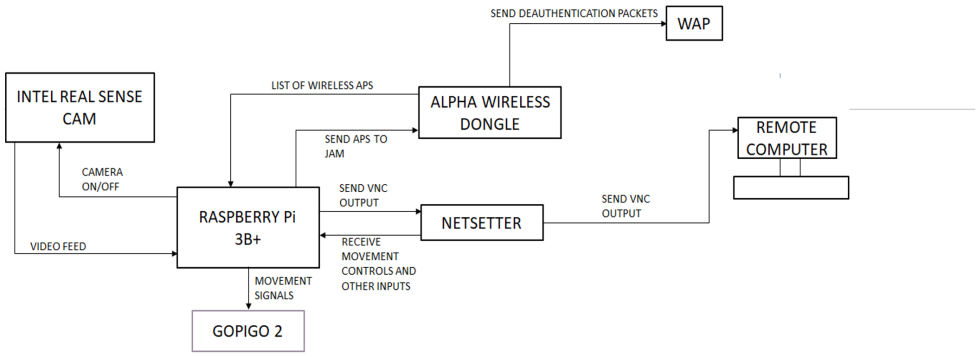

Figure 5.2: Data Flow Diagram

5.2.1 Movement of the Rover

The RPi forwards the control signals it recieved from the Remote Desktop to the Gopigo2, the Gopigo then moves accordingly.

5.2.2 Video Feed

The videofeed from the PiCam is transferred to the Rpi and is displayed on the display of the Rpi and this display is mirrored to the Remote computer via VNC using Chrome Remote Desktop.

5.2.3 Network Analysis

The Rpi requests the Alpha Wireless Dongle to retrieve the list of nearby Wireless AP's. The Alpha Wireless Dongle then sends back the list of wireless AP's nearby along with its BSSID,the type of security in place and also the list of clients associated

with that Wireless AP's and the device name and MAC address of each of these connected devices.

5.2.4 Network Jamming

Rpi provides the Name of the WAP to be jammed (ESSID) it then translates it into BSSID and sends the jamming request to the Alpha Wireless dongle which forges deauthentication packets and sends them to the WAP at a rapid pace disassociating all its clients and thereby denying its service.

CHAPTER 6
METHODOLOGY

6.1 Network Analysis

Start by putting our wireless adapter in monitor mode. This is similar to putting a wired adapter into promiscuous mode. It allows us to see all of the wireless traffic that passes by us in the air. Now that the wireless adapter is in monitor mode, we have the capability to see all the wireless traffic that passes by in the air. The wireless adapter grabs all the traffic it can see and displays critical information about it, including the BSSID (the MAC address of the AP), power, number of beacon frames, number of data frames, channel, speed, encryption (if any), and finally, the ESSID (what most of us refer to as the SSID).

6.2 Denial Of Service Attack

The initial phase of DOS is similar to that of network analysis ie the wirelss adapter is put into in monitor mode which allows us to see all of the wireless traffic that passes by us. It the grabs the traffic it can see and displays critical information about it, including the BSSID (the MAC address of the AP), power, number of beacon frames, number of data frames, channel, speed, encryption (if any), and finally, the ESSID (what most of us refer to as the SSID). Next step is to focus our efforts on one AP, on one channel, and capture critical data from it. We need the BSSID and channel to do this which we obtained in the previous step. We then de-authenticate the clients of that AP by forging deauthentication packets and sending it to them,and their system will automatically re-authenticate, but when this process is repeated with

a high frequency then no communication can occur between the AP and the clients thereby disrupting the service.

CHAPTER 7
CONCLUSION AND FUTURE WORK

IoT will play a major role in the coming years and any IOT based product relies heavily on wireless AP's and the rover is capable of detecting flaws in such AP's and exploiting them if necessary. So such a tool will be vital in the arsenal of any military.Completed Design and Layout. Started work on network analysis.Many different adaptations, tests, and experiments will be done in the next phase. Future work concerns deeper analysis of particular mechanisms, new proposals to try the methods.

REFERENCES

[1] https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-ai rcrack-ng-0148366/

[2] https://www.howtogeek.com/204335/warning-encrypted-wpa2-wi-fi-networks-are-still-vulne rable-to-snooping/

[3] https://www.kali.org/tutorials/secure-kali-pi-2018/

[4] Long Chen, Shervin Erfani, "A note on security management of the Internet of Things", Electrical and Computer Engineering (CCECE) 2017 IEEE 30th Canadian Conference on, pp. 1-4, 2017.

[5] Shervin Erfani, Majid Ahmadi, Long Chen, "The Internet of Things for smart homes: An example", Industrial Automation and Electromechanical Engineering Conference (IEMECON) 2017 8th Annual, pp. 153-157, 2017.