

SIGNAL JAMMER

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering Degree in
Electronics and Communication Engineering

by

NALIN RAJ (39130310)

MARKANDEY (39130285)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL- 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

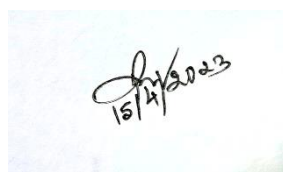
BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **NALIN RAJ** (39130310) and **MARKANDEY** (39130285) who carried out the project entitled "**SIGNAL JAMMER**" under my supervision from November 2022 to April 2023.



Internal Guide

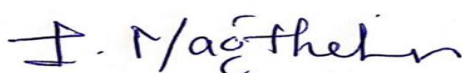
Dr. S. BARANI, M.E., Ph.D.,



Head of the Department

Dr. T. RAVI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 27.04.23



Internal Examiner



External Examiner

DECLARATION

We **NALIN RAJ** (39130310) and **MARKANDEY** (39130285) hereby declare that the Project Report entitled “**SIGNAL JAMMER**” done by us under the guidance of **Dr. S. BARANI**, M.E., Ph.D. at Sathyabama Institute of Science and Technology, Chennai-600119 is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

1.



2.



DATE: 27.04.23

PLACE: Chennai

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of Management of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N. M. NANDHITA, M.E., Ph.D.**, Dean, School of Electrical and Electronics Engineering and **Dr. T. RAVI, M.E., Ph.D.**, Head of the Department, Dept. of Electrical and Electronics Engineering for providing us necessary support and details at the right time during the progressive reviews.

We would also like to express our sincere and deep sense of gratitude to our Project guide **Dr. S. BARANI, M.E., Ph.D.**, for her valuable guidance and suggestions during the progressive reviews for our project.

We wish to communicate our gratitude to all teaching and non-teaching staff individuals from the Department of Electronics and Communication Engineering who were useful from multiple points of view for the fulfillment of the task.

ABSTRACT

In recent times, the utilization of electronic devices has significantly increased in communication and technology, but there has also been a rise in their misuse, particularly in restricted areas like examination halls and confidential rooms. One of the electronic devices commonly misused is mobile phones, which has become a prevalent issue in different sectors of society. The detector is a useful tool for situations where mobile devices are prohibited or unwanted, such as in exam halls or in quiet areas. It is also a helpful tool for parents to monitor their children's mobile usage.

The proposed system can detect incoming and outgoing calls, messages, and video transmissions even if the mobile phone is in soundless mode and can disrupt wireless signals in a specific area, rendering WiFi connections unusable. This technology has a range of potential applications, including preventing unauthorized access to wireless networks, ensuring privacy in public spaces, and blocking distracting WiFi signals in classrooms or other shared spaces. Overall, the mobile signal jammer is a useful tool for detecting incoming calls and messages on a mobile device while respecting privacy and without compromising the content of the communication.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE
	ABSTRACT	v
	LIST OF FIGURES	vii
	LIST OF TABULATION	viii
1.	INTRODUCTION	1
	1.1 Overview	1
	1.2 History	4
	1.3 What is signal jammer?	5
2.	LITERATURE SURVEY	7
3.	OBJECTIVES & PROTOCOLS	12
	3.1 Objectives	12
	3.2 Jamming techniques	12
4.	PROPOSED METHODOLOGY	16
	4.1 Existing system	16
	4.2 Proposed system	17
5.	REQUIREMENT SPECIFICATION	18
	5.1 Hardware requirements	18
	5.1.1 Esp8266 nodemcu	18
	5.1.2 Ca3130 ez	24
	5.1.3 Bc548	32
	5.1.4 Led	38
	5.2 Software requirements	42
	5.2.1 Arduino ide	42
6.	RESULTS & DISCUSSIONS	46
7.	STANDARDS & CONSTRAINTS	51
8.	CONCLUSION	54
	PAPER PUBLICATION	55
	REFERENCES	56

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
1.1	Jammer devices	6
4.1	Existing System	16
4.2	Block Diagram	17
5.1	NodeMCU	18
5.2	Pin Layout	21
5.3	Architecture of Chip	24
5.4	CA3130 MOSFET OP-AMP	24
5.5	CA3130 Pin Layout	26
5.6	Schematic Diagram	28
5.7	Block Diagram of CA3130 Series	30
5.8	BC548 NPN Transistor	32
5.9	BC548 Pinout	33
5.10	Modes of Operation	35
5.11	LED	38
5.12	Cross-sectional View	39
5.13	Arduino IDE	42
6.1	Beacon Attack	48
6.2	Working Model	49

LIST OF TABLES

TABLE NO	TITLE	PAGE
5.1	Pin Layout of CA3130	26
5.2	BC548 Pin Layout	34
5.3	LED Colors	40

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Signal jamming is a form of communication interference in which a device is used to interrupt or obstruct the normal transmission of wireless signals. This technology has been used in a variety of settings, including military operations, law enforcement, and security applications. Mobile devices have become an integral part of our daily lives, and their widespread use has revolutionized the way we communicate and access information. However, there are situations where the use of mobile devices is prohibited or unwanted, such as in exam halls, theaters, libraries, or hospitals. In these environments, mobile devices can be a source of distraction or disruption, compromising privacy and security. To address these challenges, mobile signal detectors have been developed as a tool for detecting mobile signal activity.

A mobile signal detector is a device that can identify the presence of mobile devices by detecting the radio waves emitted by mobile phones when they receive or transmit data. This technology has been in use for several years and has been continuously improved to meet the increasing demand for mobile signal detection.

Mobile signal detectors come in different forms, ranging from handheld devices to stationary systems. Handheld devices are compact and portable, making them suitable for personal use. They are commonly used by individuals, such as parents, teachers, or security personnel, who want to monitor mobile device activity in a specific location. On the other hand, stationary systems are designed for use in larger areas, such as airports, conference halls, or stadiums, and can cover a wide range of frequencies to detect various types of mobile signals.

Mobile signal detectors have several applications, including enhancing security, monitoring mobile device usage, maintaining privacy, preventing

distractions, and complying with regulatory requirements. For instance, in secure facilities, such as prisons or military bases, mobile signal detectors can be used to prevent the use of mobile devices for illegal activities or espionage. In healthcare settings, mobile signal detectors can be used to ensure that no mobile devices are present in sensitive areas, such as operating rooms or intensive care units, where they can interfere with medical equipment.

However, with the widespread use of wireless networks comes the potential for security breaches and unwanted access to private networks. To address these concerns, WiFi jammers have been developed as a tool for disrupting wireless network connectivity.

A WiFi jammer is a device that transmits a signal on the same frequency as a WiFi signal, effectively blocking or disrupting the wireless network connection. The use of WiFi jammers can prevent other users from accessing or using a wireless network, thereby increasing network security and privacy. WiFi jammers come in various sizes and forms, ranging from handheld devices to larger, more powerful systems that can cover a wide range of frequencies.

The use of WiFi jammers, however, is controversial and is prohibited in most countries due to the potential negative impact on public and emergency communication networks. The use of WiFi jammers can interfere with important wireless communication systems, including those used by emergency services, air traffic control, and navigation systems. Furthermore, using a WiFi jammer can result in legal consequences, including fines or imprisonment.

Despite the potential legal and ethical issues associated with the use of WiFi jammers, they have some legitimate uses, such as enhancing security in private networks or blocking unwanted access to wireless networks. They can also be used to prevent distractions caused by wireless devices in environments where focus is critical, such as in classrooms or during business meetings. Mobile jammers were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosives. The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise & reckless

invasion of privacy. That being said, nowadays, mobile phones have become an essential tool in our daily life. Here in India, for example, with a rather High population (around 1.25 billion), a large number of mobile network carriers are available such as Airtel, VI, Jio, etc, which operate at GSM 900 frequency bands. Needless to say, the wide use of mobile phones could create various problems, but the sound of a ringing phone becomes annoying at certain times. This could happen in some in some really important public places thereby putting you in the limelight. Hence one simple way to stop this annoyance at some really important places is to install a device in such places which will inhibit the use of mobiles, i.e., make them obsolete. Such a device is known as cell phone signal jammer, which is basically some kind of electronic countermeasure device. The technology behind cell phone jamming is very simple.

The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. It should be mentioned that cell phone jammers are illegal devices in most countries. However, recently, there has been an increasing demand for portable cell phone jammers across the globe, with that being said one should note that what we are presenting is totally with respect to gaining knowledge and mainly for educational purposes only and that there is no intention for us to manufacture or sell these devices in India, or elsewhere. In this project, using the device causes extensive disruption and involvement in mobile signal operation, by affecting coverage and a degradation of service for customers. In some cases, mobile users may not be aware of the blockade of its terminals as the above may not be evident until they make a call, case in which receive a warning, while not receive any communication on their mobile until they depart from the affected area. Considering the serious damage generated in the network and the allocation of user rights, it is understood critical control and restrict the supply of these teams, as well as limiting its sole use and exceptionally for public security cases such as in prisons. However, we believe that in this particular case, the real solution is that the controls should be increased and that the prison authorities in each country take necessary measures to prevent the introduction and use of cell phones in those precincts measures. Deauther are usually undetectable, and users may experience minimal effects such as poor signal

reception. Deauther devices may be used in any location but are typically deployed where cell phone use may be disruptive, such as in libraries and restaurants. Handheld deauther are capable of disrupting signals within nine to 30 meters, while more powerful Jammer create a huge bubble stretching as far as a mile or 1.6 kilometers.

1.2 HISTORY

Jammers have been around for many years and have been used for various purposes, ranging from military applications to civilian use. The first recorded use of a jamming device was during World War II, when the German military developed a device called the "Knickebein" to jam Allied radar signals. During the Cold War, jamming devices became increasingly sophisticated, with both the United States and the Soviet Union developing advanced jamming technology for military purposes. Jamming technology was used extensively during the Vietnam War to disrupt radio communications, and it has also been used in conflicts in the Middle East.

In recent years, the use of jammers has become more widespread in civilian settings, with some individuals using jamming devices to disrupt wireless signals in public places or to interfere with the operations of drones. However, the use of jammers is often illegal and can have serious consequences, including fines and imprisonment.

In response to the growing threat posed by jammers, governments and regulatory bodies around the world have taken steps to limit the availability and use of these devices. The Federal Communications Commission (FCC) in the United States, for example, has strict regulations governing the use of jamming devices, and individuals caught using or selling illegal jammers can face heavy fines and penalties.

The use of jammers in India has been a topic of concern for the government and regulatory bodies for several years. The first recorded use of jammers in India

was by the Indian military during the 1965 Indo-Pakistani War, when the military used jamming technology to disrupt Pakistani radio communications. Since then, the use of jammers has become more widespread in India, with some individuals using jammers to disrupt wireless signals in public places or to interfere with the operations of drones. However, the use of jammers is illegal in India, and the government has taken steps to curb their use and limit their availability. Overall, while jammers have a long history of use in military and civilian contexts, their use is generally frowned upon and can be illegal and unethical in many situations. It is important to promote responsible and lawful use of wireless technology and to respect the safety and rights of all individuals.

1.3 What is Signal Jammer?

A signal jammer is a device that emits radio frequencies (RF) on the same frequency bands used by wireless devices, such as cell phones, Wi-Fi routers, and GPS devices. This causes interference with the wireless signals, resulting in either complete loss of signal or degraded signal quality. Signal jammers can be designed to operate on specific frequency bands or on multiple bands simultaneously. A WiFi jammer is a type of signal jammer that is designed to disrupt the normal functioning of wireless networks, specifically those operating on the 2.4GHz and 5GHz frequency bands. A WiFi jammer is a device that emits radio frequencies on the same frequency bands used by WiFi networks, causing interference and disrupting the normal functioning of the wireless network. These devices can be designed to operate on specific frequency bands or on multiple bands simultaneously. Some WiFi jammers can also be programmed to target specific types of wireless networks, such as those using certain encryption protocols.



Fig 1.1: Jammer Devices

CHAPTER 2

LITERATURE SURVEY

M. Raveendranad , Mr. D.M.K. Chaitanya (2014) projected Mobile jammer is functioning utterly while not moving the signals from the network. In order that the user will be able to get the notifications relating to Calls and messages (SMS, MMS). The notifications regarding the calls are given to the user. If there's any imperative decision as we will get the notification we will leave from the coverage space and use our mobile because it is. No would like of licensing. Implementation of our freshly designed jammers is straightforward. As we tend to square measure employing a FPGA, our hardware will be changed whenever we would like. FPGAs offer a number of paradigms to speed up calculations in a hardware software co- design environment.

Swathy P. G. (2015) intended to prevent the usage of mobile phones in places inside its coverage without interfacing with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required restricted area reasonably. Although we must be aware of the fact that now a days lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices. These jammers include the intelligent jammers which directly communicate with the GSM provider to block the services to the clients in the restricted areas, but we need the support from the providers for this purpose.

Vishal U. Kanojiya and Jitendra B. Yadav (2015) presented a low-cost, non-invasive, small-size system and a jammer which helps to detect the driver's use of mobile phone not the phone used by the fellow passenger in the vehicle. It also helps in preventing the road accident due to distraction to a large extent. Though Engineers, researchers or scientist innovate various new technologies, methods or system to prevent road accident, but still road accident continues. To overcome this type of situation all people must educate, realize and give more attention along with newly innovated technology to decrease the rate of road accident.

Oyediran Oyebode Olumide, Ogunwuyi Ogunmakinde Jimoh , Lawal Akeem Olaide (2016) demonstrated that the effective jamming range was around 50 meters on AC and around 30metres on DC. From the research carried out on this paper, it was observed that as the distance between the cell phone and the base station increases, the effective jamming distance will increase. This is due to the fact that the amount of power reaching the cell phone from the base station decreases as the cell phone moves farther from the base station. This paper is effectively designed and tested working properly on 2G network. Hence, by designing this project GSM CDMA, 3G mobile phone signals are blocked within the given time schedule i.e. a range of 850MHz to 2170MHz frequencies are blocked.

Nsikan Nkordeh, Iwu C. Lawson, Francis Idachaba, Ibinabo Bob- Manuel (2016) stated that the mathematical analysis of frequency jamming was done using a QPSK-modulated signal. In order to discourage student from using mobile phones during lectures and around the library areas, a jammer system was built using VCO (PMB2110) processor which generates signal in the frequency range of GSM900 and DCS1800. Tests were carried out in the lecture room areas and in the library, and it was found out that mobile phones were shut out from service while the jammer was on. Oscilloscope plots were taken, which shows that the noise level of the received mobile signals increased tremendously while the jammer was on. The success of this project has in shutting down mobile services within the vicinity where it is not needed has open communication with some industry that may result in mass production of the device.

Diana Starovoytova Madara , Edwin Ataro and Simiyu Sitati (2016) highlight the design of a simple, low-cost mobilephone-jammer and aims to present a solution for the problem of inappropriate-use of the cell-phones in restricted and prohibited-areas. The main concept of jamming is the releasing of signal (noise) of the same-frequency which is using by mobile-service-provider to overpower and destruct the user-signal. The fabrication of the jammer involved uncomplicated discrete components, resistors, capacitors, inductors and transistors to generate the required frequency (noise) and then amplifies the frequency generated to range of 800 MHZ to 1.4 GHZ in order to match the frequency of the mobile-phone being transmitted by the base-station. Relatively- satisfactoryjamming of a mobile-signal was confirmed by the blocking of the signals of the mobile-phones in 2G and 3Gnetworks (UMTS / WCDMA) operated via Safaricom, Airtel, Orange, and YU service-providers, when the phone indicated “no network”, thereby allowing no call to go through, with no-interference to other communication-means observed. Overall recommendation is that further and more deeper-research is needed to produce more-sophisticated and better jamming devices, as not to affect the other base-station-transmission systems.

Saurabh Singh, Krishna Yadav, Rishabh Singh, Akash Soni, Harjeet Matharuf and Pranay Rao (2017) built the project that was tested against the two GSM-900 Networks and has proven success with average range of 10 m. Due to power supply variation with load current, so to improve the jammer a more stable power supply should be designed for robust operation of the device. Also the power supply was not capable to deliver the needed current for the power amplifier and the reason for the actual coverage range of the device was not the same as designed for. Testing in different location shows the dependence of the jamming range on the signal strength. In general the jamming attack was protected by network signal power, and having large power jamming device the GSM network will be jammed for sure and from this observation it can be concluded that the protection against jamming attack in the GSM system was very weak and couldn't withstand the simplest jamming techniques. The main disadvantage of the mobile jammer is that the transmission of the jamming signal which is prohibited by law in many countries, for instance the fines for this offense can be very high. Despite the legal issues the transmission of high power signal may affect the operation of some critical devices, such as hearing impairment hardware solution.

Dr. Ibrahim Patel , Ashok Shigli , V Sripathi Raja , Dr. Raghavendra Kulkarni (2018) proposed a device that stops phones from ringing, which proved to be a complete success. This gadget could be utilised in locations where ringing at specified times is not desired since it might disturb nearby residents. Due to a lack of current supplied to the power amplifier and the requirement for a more reliable power supply for reliable operation, the effective jamming range was not as anticipated. To prevent cell phone signals from entering or leaving the area, use materials like wall paper or construction materials that contain metal shards.

According to the analysis of **Oluwole Arowolo and Adefemi Adekunle (2019)**, this project could jam the e-commercial broadcasting TV networks which cover from 300 to 800 MHz, with the right Transistor 'I' then will be able to achieve the 900MHz to 1800MHz. Although the device can operate as expected, but the radius of the antenna did not meet the expectation. The radius should be more than 4 meter obtained in the result. The project work finds its applications in School Library, Examination and religion Centers.

Esat Elezi , Goksel Cankaya, Ali Boyaci and Serhan Yarkan (2019) In this work a GPS signal is generated using Simulink in order to test different kind of Electronic Jammers. The C/A code and the navigation data are generated independently. Afterwards they are combined together and lastly modulated onto a carrier having the frequency of 1575.42 MHz. Four different Electronics Jammers are analyzed by quantifying their BER for different J/S ratios. The results show that Spot Noise Jamming has the highest BER when compared to the other electronic jamming signals.

CHAPTER 3

OBJECTIVES & PROTOCOLS

3.1 Objectives:

- To maintain privacy and to ensure that no mobile devices are present in a particular area.
- To comply with regulatory requirements and prevent unauthorized mobile communication.
- To block all kinds of mobile phones usage at all places such as Banks, libraries, movie theaters, meeting rooms and others so as to maintain the required silence in respective place.
- To prevent people from connecting to their network and potentially stealing sensitive information and to block distracting Wi-Fi signals in public places.

3.2 Jamming Techniques:

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too. In this section, we elaborate on various types of jammers and the placement of jammers to maximize the jammed area.

- **Constant jammer** emits continuous, random bits without following the CSMA protocol (Xu et al, 2005). According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmitting. If the medium is continuously idle for a DCF Interframe Space (DIFS) duration, only then it is supposed to transmit a frame. If the channel is found busy during the DIFS interval, the station should defer its transmission. A constant jammer prevents legitimate nodes from

communicating with each other by causing the wireless media to be constantly busy. This type of attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications to the point that no one can communicate at any time.

- **Deceptive jammer** continuously transmits regular packets (Xu et al, 2005) instead of emitting random bits (as in constant jammer). It deceive other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. Compared to a constant jammer, it is more difficult to detect a deceptive jammer because it transmits legitimate packets instead of random bits. Similar to the constant jammer, deceptive jammer is also energy inefficient due to the continuous transmission but is very easily implemented.
- **Random jammer** intermittently transmits either random bits or regular packets into networks (Xu et al, 2005). Contrary to the above two jammers, it aims at saving energy. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a tradeoff between jamming effectiveness and energy saving because it cannot jam during its sleeping period. The ratios between sleeping and jamming time can be manipulated to adjust this tradeoff between efficiency and effectiveness.
- **Reactive RTS/CTS jammer** jams the network when it senses a request-to-send (RTS) message is being transmitted from a sender. It starts jamming the channel as soon as the RTS is sent. In this way, the receiver will not send back clear-to-send (CTS) reply because the RTS packet sent from a sender is distorted. Then, the sender will not send data because it believes the receiver is busy with another on-going transmission. Alternatively, the jammer can wait after the RTS to be received and jams when the CTS is sent by the receiver. That will also result in the sender not sending data and the receiver always waiting for the data packet.

- **Reactive Data/ACK jammer** jams the network by corrupting the transmissions of data or acknowledgement (ACK) packets. It does not react until a data transmission starts at the transmitter end. This type of jammer can corrupt data packets, or it waits until the data packets reach the receiver and then corrupts the ACK packets (Pelechrinis et al, 2011). The corruptions of both data packets and ACK messages will lead to re-transmissions at the sender end. In the first case, because the data packets are not received correctly at the receiver, they have to be re-transmitted. In the second case, since the sender does not receive the ACKs, it believes something is wrong at the receiver side, e.g. buffer overflow. Therefore, it will retransmit the data packets.
- **Follow-on jammer** hops over all available channels very frequently (thousand times per second) and jams each channel for a short period of time (Mpitiopoulos et al, 2007). If a transmitter detects the jamming and switches its channel, the follow-on jammer will scan the entire band and search for a new frequency to jam again. Or, it may follow a pseudo-random frequency hopping sequence. This type of jammer conserves power by limiting its attack to a single channel before hopping to another. Due to its high frequency hopping rate, the follow-on jammer is particularly effective against some anti-jamming techniques, e.g. frequency hopping spread spectrum (FHSS) which uses a slow-hopping rate.
- **Channel-hopping jammer** hops between different channels proactively (Alnifie and Simon, 2007, 2010). This type of jammer has direct access to channels by overriding the CSMA algorithm provided by the MAC layer. Moreover, it can jam multiple channels at the same time. During its discovery and vertex-coloring phases, the jammer is quiet and is invisible to its neighbors. Then, it starts performing attacks on different channels at different times according to a predetermined pseudo-random sequence.
- **Pulsed-noise jammer** can switch channels and jam on different

bandwidths at different periods of time. Similar to the random jammer, pulsed-noise jammer can also save energy by turning off and on according to the schedule it is programmed for. Unlike the elementary proactive random jammer which attacks only one channel, pulsed-noise jammer can attack multiple channels. Moreover, it can be implemented to simultaneously jam multiple channels.

- **Control channel jammers** work in multi-channel networks by targeting the control channel, or the channel used to coordinate network activity (Lazos et al, 2009). A random jammer that targets the control channel could cause a severe degradation of network performance, while a continuous jammer targeting the control channel might deny access to the network altogether. Furthermore, future control channel locations can be obtained from the compromised nodes.
- **Implicit jamming attacks** are those that in addition to disabling the functionality of the intended target, cause denial-of-service state at other nodes of the network too (Broustis et al, 2009). This attack exploits the rate adaptation algorithm used in wireless networks, where the AP (Access Point) caters to the weak node by reducing its rate. Due to this process, the AP spends more time communicating with this weak node than the other nodes. Therefore, when the implicit attacker jams a node which is communicating with the AP, the rate adaptation effect will increase the AP's focus on the jammed node while causing other clients to suffer.
- **Flow-jamming attacks** involve multiple jammers throughout the network which jams packets to reduce traffic flow. As implemented by Tague et al (2008), these attacks are launched by using information from the network layer. This type of jamming attack is good for the resource-constrained attackers. If there is centralized control, then the minimum power to jam a packet is computed and the jammer acts accordingly. In a non-centralized jammer model, each jammer shares information with neighbour jammers to maximize efficiency.

CHAPTER 4

PROPOSED METHODOLOGY

4.1 Existing System:

A voltage controlled oscillator (VCXO) generates radio frequency (RF) signals that will interfere with the cellular phone signal. A VCXO uses an input voltage to determine its oscillation frequency. This technique was used in implementation. A noise generator is a circuit that produces electrical noise which is a random and non-deterministic signal. It uses a zener diode in reverse bias, turning the zener diode to exhibit avalanche effect which is a noise generator and industrial (man-made) noise readily in the environment. The power system comprises of all subsystems working together to produce desired voltage levels which drive various circuit sections of the jammer. These include: Bridge rectifier, filter circuit, voltage regulators, and fuse. Antenna Feed-line comprises of all components that makes the jamming signal arrive and radiate at the antenna efficiently and successfully. Hence, by designing it GSM CDMA, 3G mobile phone signals are blocked within the given time schedule.

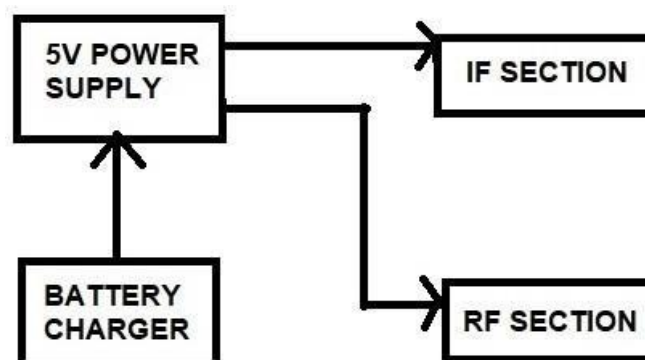


Fig. 4.1 Existing System

4.2 Proposed System:

- In the proposed system, both the designs are assembled to form a simple, compact, flexible and intuitive design.
- It consists of detector and jammer circuits, which can detect RF signals during incoming and outgoing calls, messages, and video transmission.
- This design detects the signal around the distance up to 20m for the GSM signals.
- The proposed system can operate on battery and hence is easily portable.
- This system has a low power rating and can store energy for a long time.
- It prevents against cyber-attack initiated by hackers by using spamming techniques.
- It also contains innovative components like efficient LED, lightning system that can be used for further LED based applications.

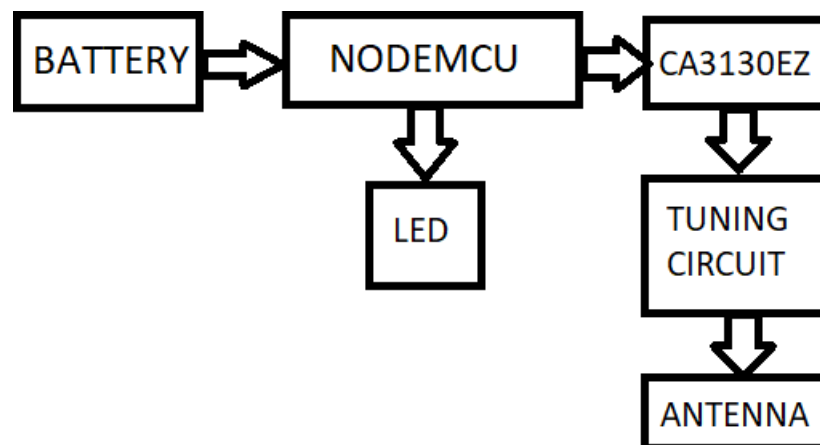


Fig 4.2 Block Diagram

CHAPTER 5

REQUIREMENT SPECIFICATION

5.1 HARDWARE REQUIREMENTS:

5.1.1 ESP8266 NODEMCU:



Fig 5.1 NodeMCU

The NodeMCU (Node Microcontroller Unit) is an open-source software and hardware development environment built around an inexpensive System-on-a-Chip (SoC) called the ESP8266. The ESP8266, designed and manufactured by Espressif Systems, contains the crucial elements of a computer: CPU, RAM, networking (Wi-Fi), and even a modern operating system and SDK. That makes it an excellent choice for Internet of Things (IoT) projects of all kinds.

However, as a chip, the ESP8266 is also hard to access and use. You must solder wires, with the appropriate analog voltage, to its pins for the simplest tasks such as powering it on or sending a keystroke to the “computer” on the chip. You also have to program it in low-level machine instructions that can be interpreted by the chip hardware. This level of integration is not a problem using the ESP8266 as an

embedded controller chip in mass-produced electronics. It is a huge burden for hobbyists, hackers, or students who want to experiment with it in their own IoT projects.

WHY ESP8266 NODEMCU:

- Low-cost: you can get ESP8266 boards starting at \$3 (or less) depending on the model.
- Low-power: the ESP8266 consumes very little power when compared with other microcontrollers and can even go into deep sleep mode to consume less power.
- Wi-Fi: the ESP8266 can generate its own Wi-Fi network (access point) or connect to other Wi-Fi networks (station) to get access to the internet. This means the ESP8266 can access online services to make HTTP requests or save data to the cloud, for example. It can also act as a web server so that you can access it using a web browser and be able to control and monitor your boards remotely.
- Compatible with the Arduino “programming language”: those that are already familiar with programming the Arduino board, were happy to know that they can program the ESP8266 in the Arduino style.
- Compatible with Micro Python: you can program the ESP8266 with Micro Python firmware, which is a re-implementation of Python 3 targeted for microcontrollers and embedded systems.

SPECIFICATION:

- The onboard ESP8266 chip manufactured by Espressif Systems has an ESP8266EX core Wi-Fi SoC and a Tensilica L106 32-bit processor in the same chip.
- It has 2.4GHz 802.11b/g/n Wi-fi with on-board antenna which supports WPA/WPA2.
- It has 17 GPIO, 11 are usable(6 are used for communication with the onboard flash memory chip) and some of them support PWM. This GPIO can be used to interface NodeMCU with the external environment through sensors and actuators.
- It also has UART, SDIO, SPI, I2C, I2S, and IR remote control peripheral interface.
- It operates on 2.5-3.6V and average 80mA current with temperatures ranging from -40 to 125 C.
- It comes in a QFN 32-pin (5mm* 5mm) package.
- It supports firmware upgrades via UART download/ OTA (via network).
- It also has SDK for customized development/cloud server development.

PIN LAYOUT:

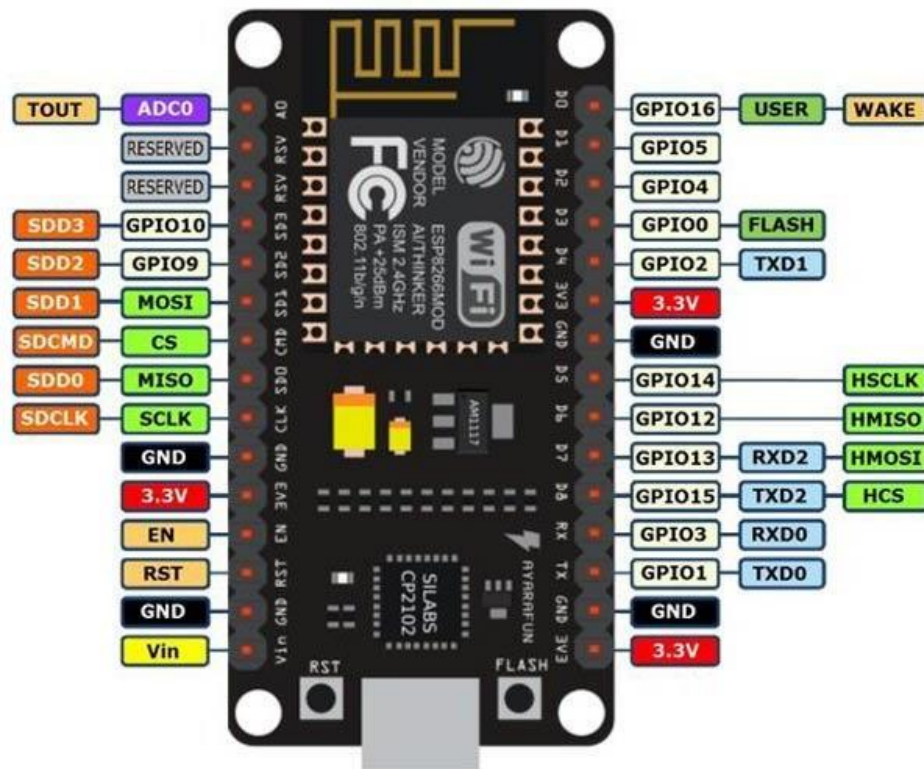


Fig 5.2 Pin Layout

- **Power Pins** There are four power pins. VIN pin and three 3.3V pins.
 - VIN can be used to directly supply the NodeMCU/ESP8266 and its peripherals. Power delivered on VIN is regulated through the onboard regulator on the NodeMCU module – you can also supply 5V regulated to the VIN pin
 - 3.3V pins are the output of the onboard voltage regulator and can be used to supply power to external components.
- **GND** are the ground pins of NodeMCU/ESP8266

- **I2C Pins** are used to connect I2C sensors and peripherals. Both I2C Master and I2C Slave are supported. I2C interface functionality can be realized programmatically, and the clock frequency is 100 kHz at a maximum. It should be noted that I2C clock frequency should be higher than the slowest clock frequency of the slave device.

- **GPIO Pins** NodeMCU/ESP8266 has 17 GPIO pins which can be assigned to functions such as I2C, I2S, UART, PWM, IR Remote Control, LED Light and Button programmatically. Each digital enabled GPIO can be configured to internal pull-up or pull-down, or set to high impedance. When configured as an input, it can also be set to edge-trigger or level-trigger to generate CPU interrupts.

- **ADC Channel** The NodeMCU is embedded with a 10-bit precision SAR ADC. The two functions can be implemented using ADC. Testing power supply voltage of VDD3P3 pin and testing input voltage of TOUT pin. However, they cannot be implemented at the same time.

- **UART Pins** NodeMCU/ESP8266 has 2 UART interfaces (UART0 and UART1) which provide asynchronous communication (RS232 and

RS485), and can communicate at up to 4.5 Mbps. UART0 (TXD0, RXD0, RST0 & CTS0 pins) can be used for communication. However, UART1 (TXD1 pin) features only data transmit signal so, it is usually used for printing log.

- **SPI Pins** NodeMCU/ESP8266 features two SPIs (SPI and HSPI) in slave and master modes. These SPIs also support the following general-purpose SPI features:
 - 4 timing modes of the SPI format transfer
 - Up to 80 MHz and the divided clocks of 80 MHz
 - Up to 64-Byte FIFO

- **SDIO Pins** NodeMCU/ESP8266 features Secure Digital Input/Output Interface (SDIO) which is used to directly interface SD cards. 4-bit 25 MHz SDIO v1.1 and 4-bit 50 MHz SDIO v2.0 are supported.

- **PWM Pins** The board has 4 channels of Pulse Width Modulation (PWM). The PWM output can be implemented programmatically and used for driving digital motors and LEDs. PWM frequency range is adjustable from 1000 μ s to 10000 μ s (100 Hz and 1 kHz).

- **Control Pins** are used to control the NodeMCU/ESP8266. These pins include Chip Enable pin (EN), Reset pin (RST) and WAKE pin.
 - EN: The ESP8266 chip is enabled when EN pin is pulled HIGH. When pulled LOW the chip works at minimum power.
 - RST: RST pin is used to reset the ESP8266 chip.
 - WAKE: Wake pin is used to wake the chip from deep-sleep.

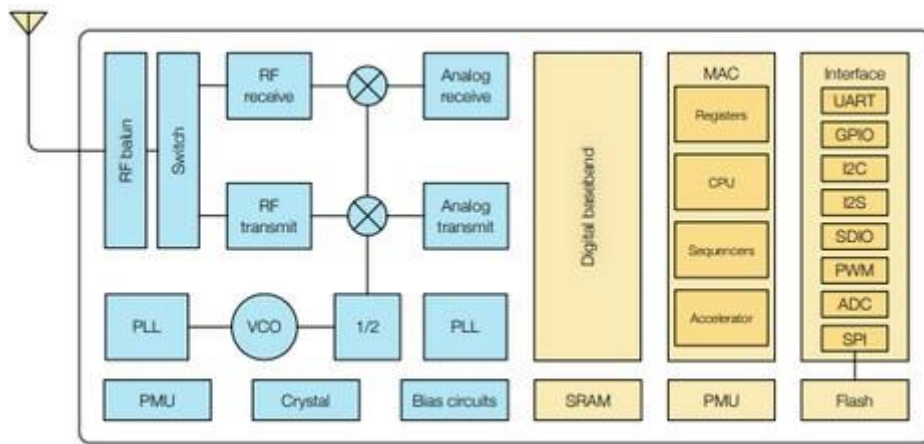


Fig. 5.3 Architecture of Chip

5.1.2 CA3130 EZ:

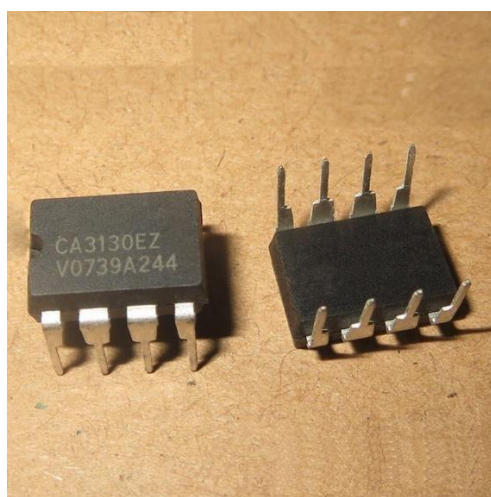


Fig 5.4 CA3130 MOSFET OP-AMP

The CA3130 is a BiMOS Operational Amplifier with MOSFET. The term BiMOS implies that it combines the advantage of both Bipolar and CMOS op-amp technology. Bipolar op-amps perform well under high bandwidths (fast switching) and CMOS op-amps perform well by consuming less current. So the CA3130 being a BiMOS op-amp has the advantage of high bandwidth operation and less current consumption.

The op-amp is built using MOSFETS and hence it has high input impedance. Meaning, when a sensor's output voltage is connected to the inverting or non-inverting pin of the op-amp, the op-amp will not act as a load to the sensor and thus the output voltage from sensor will not be disturbed.

Like all voltage Comparators the CA3130 also has an Inverting Pin and a Non-Inverting Pin. If the voltage at the Non-Inverting Terminal (pin 3) is high than the Inverting Terminal (pin 2) the output (pin 7) will also be high else the output will be low.

The CA3130 can work in a Single supply voltage or in a dual supply mode. For now let's concentrate on the +5V supply voltage circuit since this is the most used design for digital circuits. In this type, the VCC+ (pin 8) is connected to +5V supply voltage and the VCC (pin 4) is grounded to hold it at 0V potential. The special ability of this op-amp is to work with high frequencies; it has a CMRR of 80dB and the rise time is as low as 0.09uS. This makes it ideal for voltage followers and other switching related applications.

Specifications:

- Op-amp coupled with MOSFET at output
- Wide power supply Range
- Single supply - 5V to 16V

- Dual supply - $\pm 2.5\text{V}$ to $\pm 8\text{V}$
- Input Terminal current: 1mA
- Maximum Output Voltage: 13.3V
- Maximum source current: 22mA
- Maximum sink current: 20mA
- Supply current: 10mA
- Common Mode Rejection Ration (CMRR): 80dB

Pin Configuration:

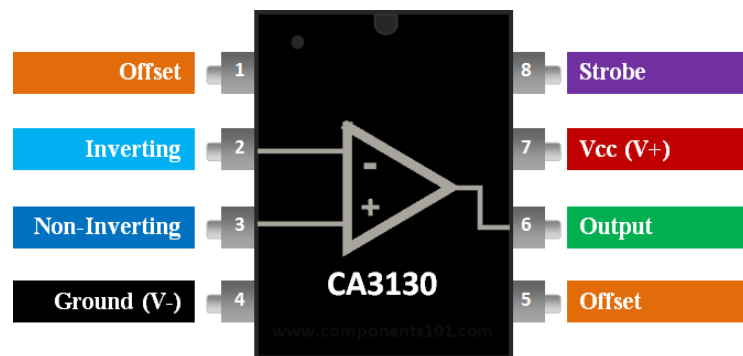


Fig 5.5 CA3130 Pin Layout

Table 5.1 Pin Layout of CA3130:

Pin Number	Pin Name	Description
1,5	Offset Null Pins	Optionally used to remove the offset voltage at the output pin to make it perfect 0V during off state.
2	Inverting Input (IN-)	The Inverting pin is also given a fixed voltage which is compared with the (IN+)

3	Non-Inverting Input (IN+)	The Non-Inverting Pin of the comparator is give a variable voltage to compare
4	Ground (VCC-)	This pin is connected to the ground of the system (Negative voltage can also be used)
6	Output	This is the output pin of the op-amp
7	VCC+	Provide the operating voltage for the Op-Amp. For CA3130 it is upto +16V
8	Strobe	Allows you to turn off output stage

CA3130EZ Manufacturer:

Renesas and Intersil will merge on January 1, 2018, resulting in a considerable increase in semiconductor inherent capabilities. Intersil's market-leading expertise in high-performance power management and precision analog devices is combined with Renesas' globally regarded MCU and SoC technologies. As a result, organic expansion in the automotive, industrial, and broad-based industries occurs, allowing the new company to respond more quickly to clients' system requirements.

The merger of Renesas and Intersil began on February 24, 2017, with the completion of the acquisition, and the unified "One Global Renesas" went into operation across all markets the following July, bringing together the strengths of both companies in anticipation of customer needs in a rapidly changing market environment. This genuinely worldwide company has a tremendous amount of synergy. Join Renesas as it improves its position as the world's premier semiconductor manufacturer.

Applications:

- Frequency Generator/Distorter
- Mobile jammers
- Voltage follower circuits
- DAC circuits
- Peak Signal/Noise detectors
- Oscillator circuits

Schematic Circuit:

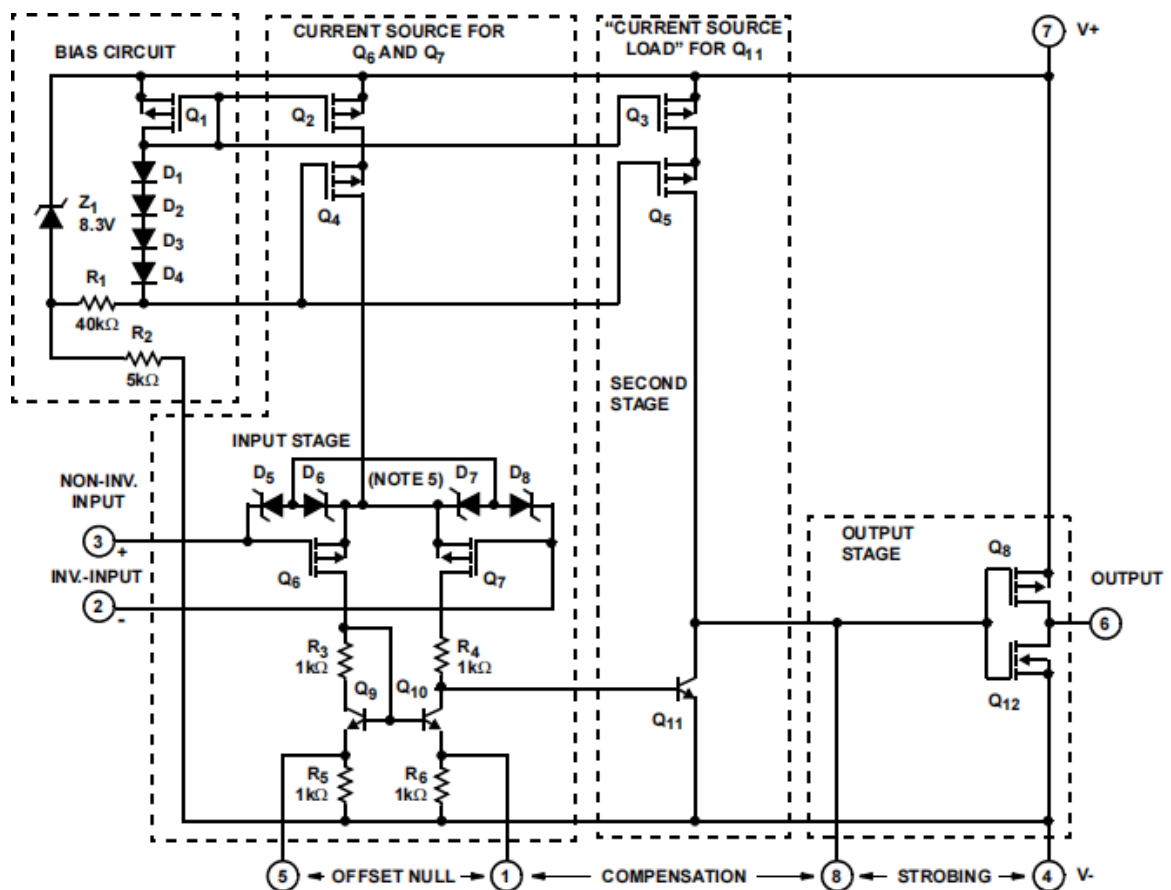


Fig 5.6 Schematic Diagram

Figure 5.7 is a block diagram of the CA3130 Series CMOS Operational Amplifiers. The input terminals may be operated down to 0.5V below the negative supply rail, and the output can be swung very close to either supply rail in many applications. Consequently, the CA3130 Series circuits are ideal for single-supply operation. Three Class A amplifier stages, having the individual gain capability and current consumption shown in Figure 5.7, provide the total gain of the CA3130. A biasing circuit provides two potentials for common use in the first and second stages. Terminal 8 can be used both for phase compensation and to strobe the output stage into quiescence. When Terminal 8 is tied to the negative supply rail (Terminal 4) by mechanical or electrical means, the output potential at Terminal 6 essentially rises to the positive supply-rail potential at Terminal 7. This condition of essentially zero current drain in the output stage under the strobed “OFF” condition can only be achieved when the ohmic load resistance presented to the amplifier is very high (e.g., when the amplifier output is used to drive CMOS digital circuits in Comparator applications).

Input Stage:

The circuit of the CA3130 is shown in the schematic diagram. It consists of a differential-input stage using PMOS field-effect transistors (Q6, Q7) working into a mirror-pair of bipolar transistors (Q9, Q10) functioning as load resistors together with resistors R3 through R6. The mirror-pair transistors also function as a differential-to single-ended converter to provide base drive to the second-stage bipolar transistor (Q11). Offset nulling, when desired, can be effected by connecting a 100,000 Ω potentiometer across Terminals 1 and 5 and the potentiometer slider arm to Terminal 4. Cascade-connected PMOS transistors Q2, Q4 are the constant current source for the input stage. The biasing circuit for the constant-current source is subsequently described. The small diodes D5 through 8 provide gate-oxide protection against high-voltage transients, including static electricity during handling for Q6 and Q7.

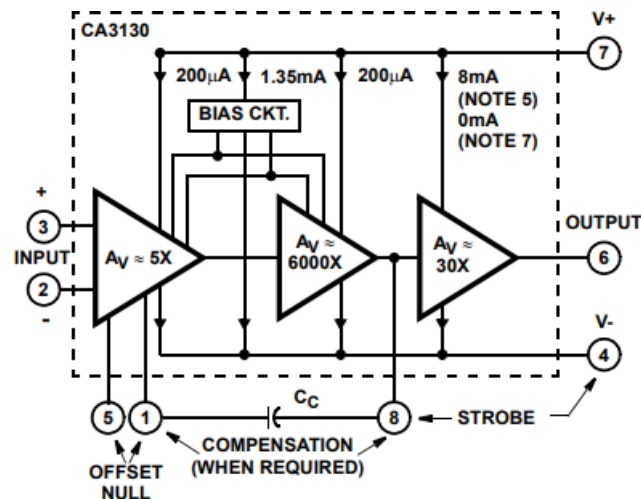


Fig 5.7 Block Diagram of CA3130 Series

NOTE:

- Total supply voltage (for indicated voltage gains) = 15V with input terminals biased so that Terminal 6 potential is +7.5V above Terminal 4.
- Total supply voltage (for indicated voltage gains) = 15V with output terminal driven to either supply rail.

Second Stage:

Most of the voltage gain in the CA3130 is provided by the second amplifier stage, consisting of bipolar transistor Q11 and its cascade-connected load resistance provided by PMOS transistors Q3 and Q5. The source of bias potentials for these PMOS transistors is subsequently described. Miller Effect compensation (roll-off) is accomplished by simply connecting a small capacitor between Terminals 1 and 8. A 47pF capacitor provides sufficient compensation for stable unity-gain operation in most applications.

Bias-Source Circuit:

At total supply voltages, somewhat above 8.3V, resistor R2 and Zener diode Z1 serve to establish a voltage of 8.3V across the series-connected circuit, consisting of resistor R1, diodes D1 through D4, and PMOS transistor Q1. A tap at the junction of resistor R1 and diode D4 provides a gate-bias potential of about 4.5V for PMOS transistors Q4 and Q5 with respect to Terminal 7. A potential of about 2.2V is developed across diode-connected PMOS transistor Q1 with respect to Terminal 7 to provide gate bias for PMOS transistors Q2 and Q3. It should be noted that Q1 is “mirror-connected (see Note 8)” to both Q2 and Q3. Since transistors Q1, Q2, Q3 are designed to be identical, the approximately 200 μ A current in Q1 establishes a similar current in Q2 and Q3 as constant current sources for both the first and second amplifier stages, respectively. At total supply voltages somewhat less than 8.3V, Zener diode Z1 becomes nonconductive and the potential, developed across series-connected R1, D1-D4, and Q1, varies directly with variations in supply voltage. Consequently, the gate bias for Q4, Q5 and Q2, Q3 varies in accordance with supply voltage variations. This variation results in deterioration of the power-supply-rejection ratio (PSRR) at total supply voltages below 8.3V. Operation at total supply voltages below about 4.5V results in seriously degraded performance.

Output Stage:

The output stage consists of a drain-loaded inverting amplifier using CMOS transistors operating in the Class A mode. When operating into very high resistance loads, the output can be swung within millivolts of either supply rail. Because the output stage is a drain-loaded amplifier, its gain is dependent upon the load impedance. The transfer characteristics of the output stage for a load returned to the negative supply rail are shown in Figure 2. Typical op amp loads are readily driven by the output stage. Because large-signal excursions are non-linear, requiring feedback for good waveform reproduction, transient delays may

be encountered. As a voltage follower, the amplifier can achieve 0.01% accuracy levels, including the negative supply rail.

5.1.3 BC548



Fig 5.8 BC548 NPN Transistor

BC548 is a NPN transistor so the collector and emitter will be left open (Reverse biased) when the base pin is held at ground and will be closed (Forward biased) when a signal is provided to base pin. BC548 has a gain value of 110 to 800, this value determines the amplification capacity of the transistor. The maximum amount of current that could flow through the Collector pin is 500mA, hence we cannot connect loads that consume more than 500mA using this transistor. To bias a transistor, we have to supply current to base pin, this current (I_B) should be limited to 5mA.

When this transistor is fully biased, it can allow a maximum of 500mA to flow across the collector and emitter. This stage is called Saturation Region and the typical voltage allowed across the Collector-Emitter (V_{CE}) or Base-Emitter (V_{BE}) could be 200 and 900 mV respectively. When base current is removed the transistor becomes fully off, this stage is called as the Cut-off Region and the Base

Emitter voltage could be around 660 mV.

Technical specifications:

- Package Type: TO-92
- Transistor Type: NPN
- Max Collector Current (I_C): 500mA
- Max Collector-Emitter Voltage (V_{CE}): 30V
- DC Current Gain range (h_{FE}): 110 - 800
- Max Collector-Base Voltage (V_{CB}): 30V
- Max Emitter-Base Voltage (V_{EBO}): 5V
- Low Noise: <10 dB
- Max. Collector Dissipation (P_C): 625 milliwatt
- Max Transition Frequency (f_T): 150 MHz
- Max Storage & Operating temperature Should Be: -55 to +150°C

Pin Configuration:

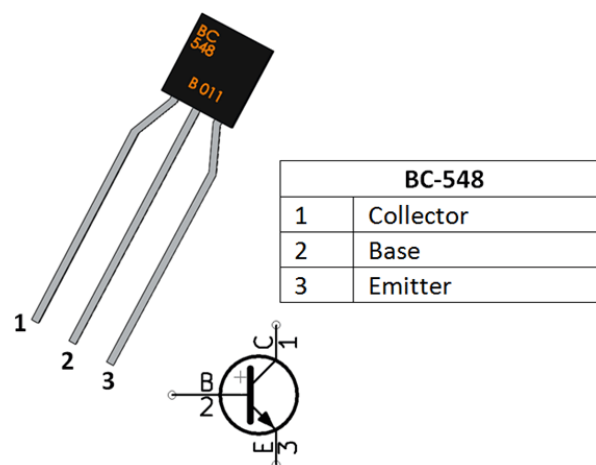


Fig 5.9 BC548 Pinout

Table 5.2 BC548 Pin Layout:

Pin Number	Pin Name	Description
1	Collector	Current flows in through collector
2	Base	Controls the biasing of transistor
3	Emitter	Current Drains out through emitter

Modes of Operation of BC548:

Like every other transistor BC548 transistor works in three regions:

- Cut off Region
- Saturation Region
- Active Region

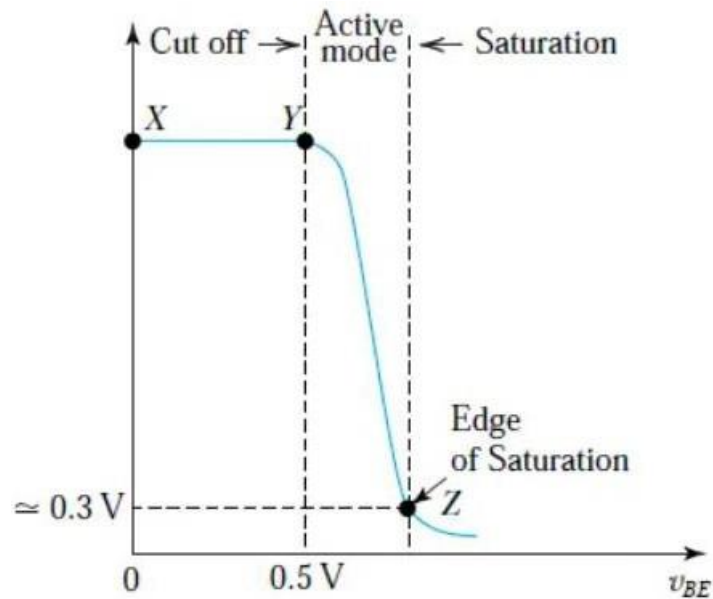


Fig 5.10 Modes of Operation

a. Cut-off Region:

In the cut-off region, transistor works as an open circuit or open switch. The base, collector and emitter currents are all zero in this region. In the cut-off region, both the collector and emitter junctions are reverse biased. Hence in the cut-off region, the base, emitter, and collector current are zero. This gives $I_C = I_E = I_B = 0$. Here I_C = collector current, I_E = emitter current, and I_B = base current.

b. Saturation region:

In the saturation region, transistor works like a short circuit or closed switch. The collector and Emitter currents are maximum in this region. In the saturation region, both the collector and emitter junctions are forward biased. In other words, the transistor operates as a short circuit or closed switch carrying maximum current which implies, $I_C = I_E$;

here I_C = collector current and I_E = emitter current.

c. Active region:

The active region lies between the cut-off and saturation regions. In the active region, the transistor emitter junction is forward biased and the collector junction is reverse biased. In the active region, the collector current is β times the base current, i.e.,

$$I_C = \beta I_B$$

here, I_C = collector current

β = current amplification factor

I_B = base current

So the collector current increases in proportional to the base current.

Transistor as a Switch:

The region responsible for a transistor to work as a switch are Saturation Region and the Cut-off Region. When we apply a high enough current at the base of the transistor, it makes a path for the collector current to go through the base towards the emitter.

In order to use the transistor as a switch, it must be driven into the saturation region with enough base current. And a transistor operates as a closed switch under the saturation region. As soon as a positive signal (in form of voltage and current) is removed across the base of the transistor, the flow of electric current between the collector and emitter becomes zero. And the transistor behaves like an open switch under the cut-off region.

This simply implies if we apply signal (voltage/current) across the collector and emitter but not across the base, the transistor will not work. But a small signal across the base is enough to make it work.

Transistor as a Amplifier:

A transistor acts as an amplifier by increasing the strength of a weak signal applied at its base. Transistors work as an amplifier in the active region or linear region. The figure given below shows how to use a transistor as an emitter amplifier.

In this region, with the increase in the base current, the collector current also increases proportionally according to the formula:

$$I_C = \beta I_B$$

Here, I_C = collector current

β = current amplification factor

I_B = base current

Thus, a small input signal results in a large output, which implies that the transistor works as an amplifier.

Circuit Applications:

- Sensor Circuits
- Audio Preamplifiers
- Audio Amplifier Stages
- Switching Loads under 500mA
- Darlington Pairs

5.1.4 LED:

LED (Light Emitting Diode) is an optoelectronic device which works on the principle of electro-luminescence. Electro-luminescence is the property of the material to convert electrical energy into light energy and later it radiates this light energy. In the same way, the semiconductor in LED emits light under the influence of electric field.

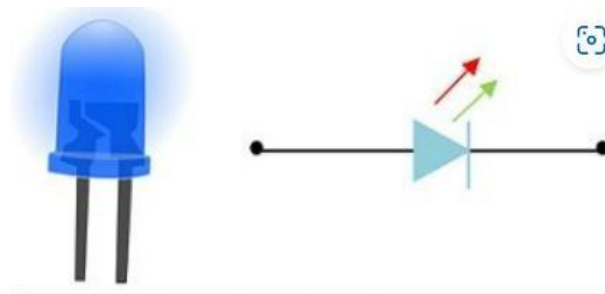


Fig 5.11 LED

The “Light Emitting Diode” or LED as it is more commonly called, is basically just a specialised type of diode as they have very similar electrical characteristics to a PN junction diode. This means that an LED will pass current in its forward direction but block the flow of current in the reverse direction.

Construction of LED:

The semiconductor layer of P-type is placed above N-type because the charge carrier recombination occurs in p-type. Besides, it is the surface of the device, thus, the light emitted can be easily seen on the surface. If P-type will be placed below the light will be emitted from the surface of P-type but we will not be able to see it. This is the reason that P-type is placed above.

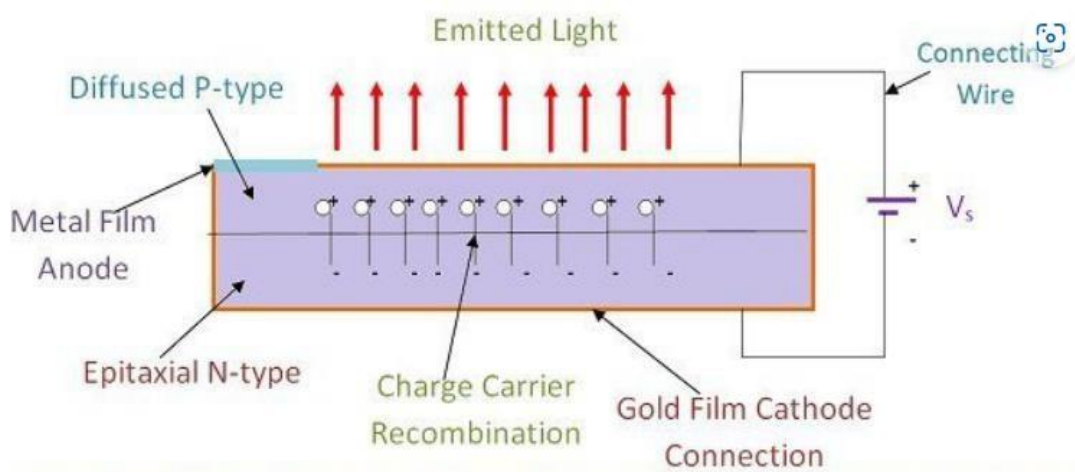


Fig 5.12 Cross-sectional View

The P-type layer is formed from diffusion of semiconductor material. On the other hand in N-type region, the epitaxial layer is grown on N-type substrate. The metal film is used on the P-type layer to provide anode connection to the diode. Similarly, Gold-film layer is coated on N-type to provide cathode connection.

Working:

The electrons are majority carriers in N-type and holes are majority carriers in P-type. The electrons of N-type are in the conduction band and holes of P-type are in the valence band. The energy level of the Conduction band is higher than the energy level of the Valence band. Thus, if electrons tend to recombine with holes they have to lose some part of the energy to fall in lower energy band.

The electrons can lose their energy either in the form of heat or light. The electrons in Silicon and Germanium lose their energy in the form of heat. Thus, they are not used for LEDs as we want semiconductor in which electrons lose their energy in the form of light.

Table 5.3 LED Colors:

MATERIALS IN CONSTRUCTION	COLOUR	FORWARD VOLTAGE (IN VOLTS)
GaP	Green/Red	2.2
GaAsP	Yellow	2.2
GaAsP	Red	1.8
GaN	White	4.1
GaN	Blue	5.0
AlInGaP	Amber	2.1
AlInGaP	Yellow	2.1

Advantages of LED:

- **Temperature Range:** It can be operated over a wide range of temperature ranging from 00C -700C
- **Switching Time:** The Switching time of LEDs is in order of 1ns. Thus, they are useful in dynamic operations where a large number of arrays are used.
- **Low Power Consumption:** They consume less power and they can be used even if the dc power supplied is low

- **Better Controlling:** The radiant power of LEDs is the function of the current flowing in it. Thus, the light intensity of LED can be controlled easily.
- **Economical and Reliable:** LEDs are cheap and they possess a high degree of reliability.
- **Small Size and Portability:** They are small in size and can be stacked together for the formation of alphanumeric displays.
- **Higher Efficiency:** The efficiency of LEDs to convert power to light energy is 10-50 times greater than that of the tungsten lamp. The response time of LED is 0.1ns while in the case of tungsten lamp it is in tens or hundreds of milliseconds.

Disadvantages of LED:

- **Overvoltage or Overcurrent:** The LEDs may get damaged when the current is increased beyond a certain limit.
- **Overheating due to radiant power:** It gets overheated with an excessive increase in radiant power. This may lead to damage of LED.

Applications:

- Picture phones and digital watches
- Camera flashes and automotive heat lamps
- Aviation lighting
- Digital computers and calculators
- Traffic signals and Burglar alarms systems

- Microprocessors and multiplexers

5.2 SOFTWARE REQUIREMENTS:

5.2.1 Arduino IDE:

The Arduino IDE is an open-source software, which is used to write and upload code to the Arduino boards. The IDE application is suitable for different operating systems such as Windows, Mac OS X, and Linux. It supports the programming languages C and C++. Here, IDE stands for Integrated Development Environment.

The program or code written in the Arduino IDE is often called as sketching. We need to connect the Genuino and Arduino board with the IDE to upload the sketch written in the Arduino IDE software. The sketch is saved with the extension '.ino.'

IDE Interface:

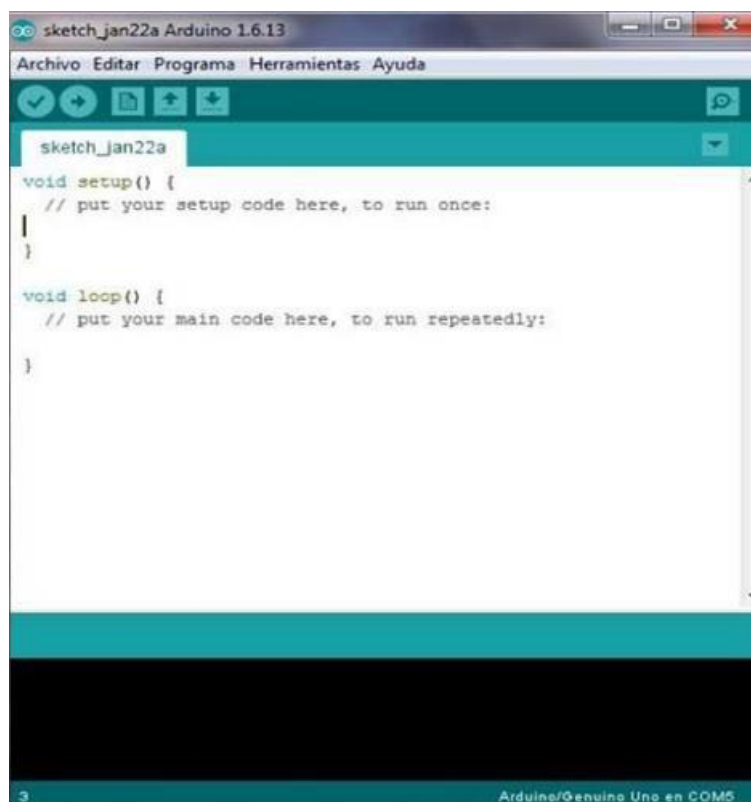


Fig 5.13 Arduino IDE

1. **Menu section:** Menus are the main menus of the program, and they are 5 menus (File, Edit, Sketch, Tools, Help), and they are being used to add or modify the code that you are writing.
2. **Toolbar section:** The toolbar is the most important section in the Arduino software, because it contains the tools that you will use continuously while programming the Arduino board. These tools are:
 - Verify: this button use to review the code, or make sure that is free from mistakes.
 - Upload: this button is use to upload the code on the Arduino board.
 - New: this button use to create new project, or sketch (sketch is the file of the
 - code)
 - Open: is use when you want to open the sketch from sketchbook.
 - Save: save the current sketch in the sketchbook.
 - Serial monitor: showing the data which have been sent from Arduino.
3. **Code editor section:** Code editor is liberator of codes, is the white space in the program, in which codes are been writting, and modifying on it.
4. **Status bar section:** Status bar is a space can be found down the code editor, through it showing the status of operation's completion (compiling, uploading, ... etc).
5. **Program notifications section:** Program notifications this program showing you the mistakes of codes, and some problems that can be face you during the programmation process. And clarifies to you the type of the mistake or the problem which happened and it reason.

And it presents some instruction through it, which you have to apply to process the mistake or the problem.

6. **Serial port & Board selections:** Serial ports selections is a space in which the program showing you the type of the port which is used to connect the arduino by computer.

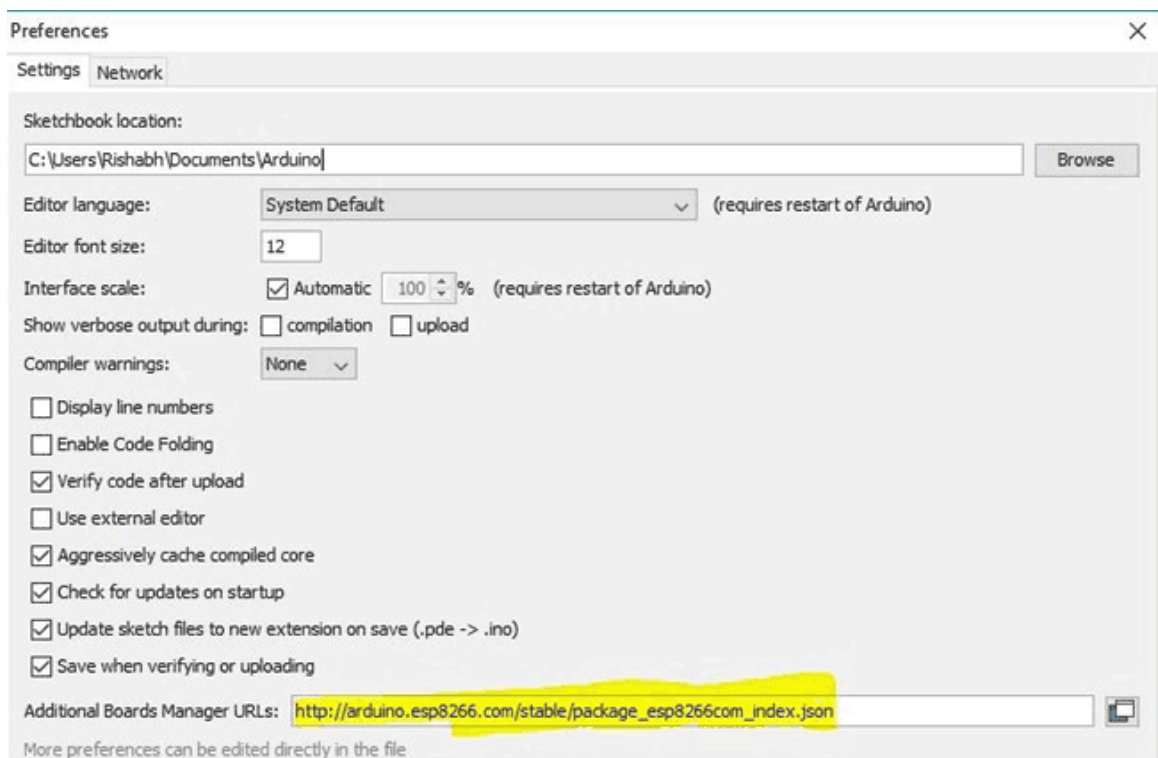
Board selections is a space in which the program showing you the type of the arduino board.

Programming the NodeMCU using Arduino IDE:

Step 1: If you do not have an Arduino IDE download it and install it from arduino.cc. (make sure the Arduino Version is 1.6.5 or above)

Step 2: Go to File -> Preferences to open the below dialog box. In the “Additional Board managers URL” paste the below link as shown in the image. Then press OK

http://arduino.esp8266.com/stable/package_esp8266com_index.json



Step 3: Now, go to *Tool -> Boards -> Board Managers*. Search for ESP8266 by esp8266 community and click on install as shown in the below image.



Your installation will take some time, once completed we can proceed to our next step.

Step 4: Now, go to Tools -> Boards -> NodeMCU. You should be able to select NodeMCU board there.

CHAPTER 6

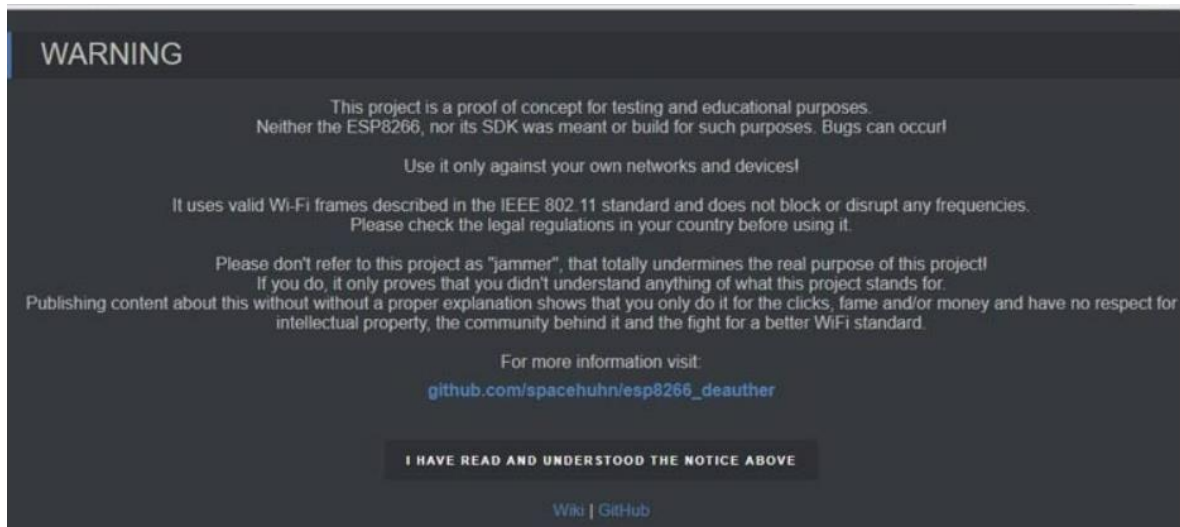
RESULTS & DISCUSSIONS

6.1 Working:

6.1.1 Deauther Attack:

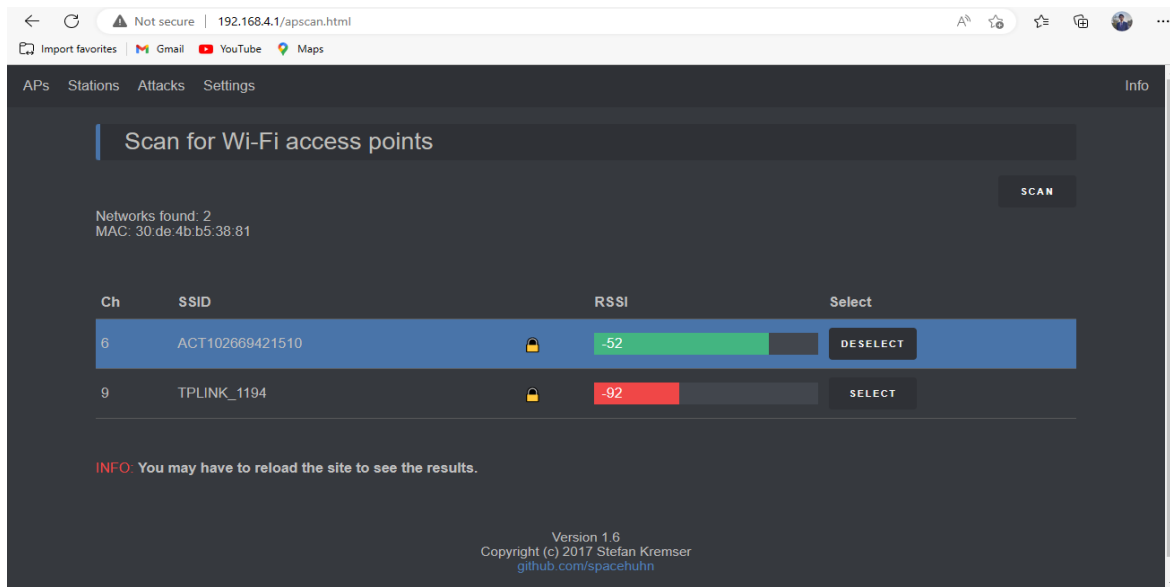
Step 1: Connect the laptop or smartphone with Access Point created by NodeMCU. Name of AP is (pwned) and password (deauther) .

Step 2: Next, open your browser and enter the address “192.168.4.1”. This will show you a warning. Read and click on ‘I have read and understood’.

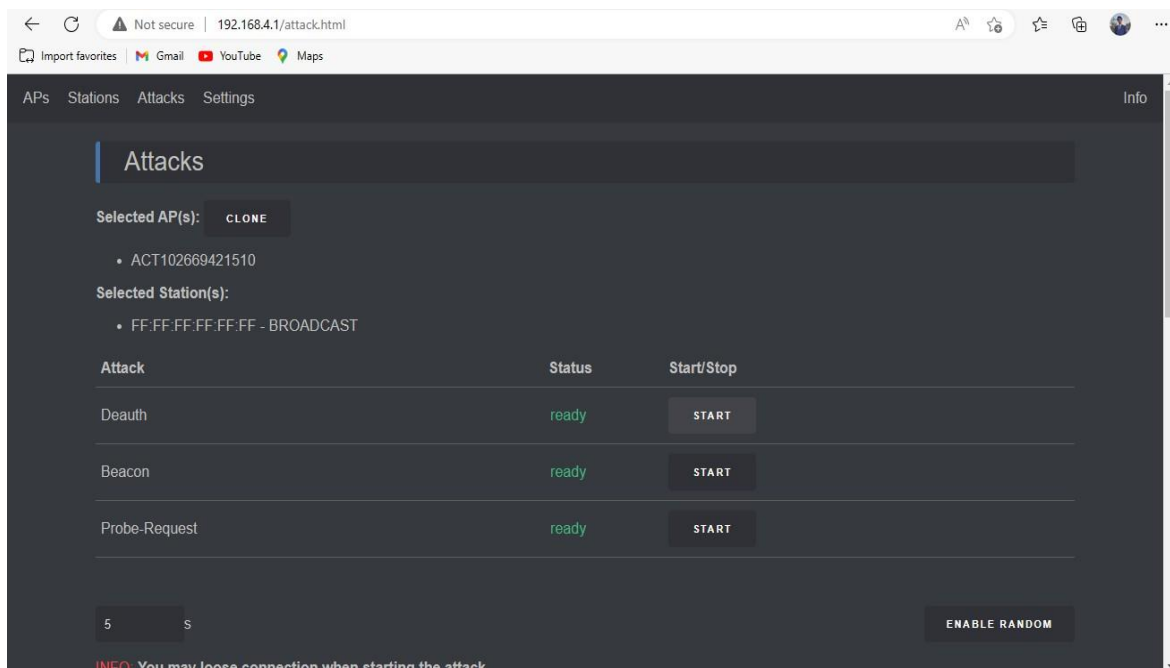


Step 3: Next, you will see a window. Select Scan Aps for available Wi-Fi networks.

Step 4: Click on the network you wish to jam.



Step 5: Now go to the 'Attacks' menu and you will see the chosen network. Click 'Start' and you will start the attack. Now reload and you will have jammed the network. You can stop the attack by clicking 'Stop'.



6.1.2 Beacon Attack:

- Also if we want to make fake WiFi networks i.e. Beacons. Click on SSIDs above and name the SSIDs as you want.
- Add and save it. Come back to Attacks menu and click on Start in front of Beacon.
- We can see the WiFi spam that we named and created.

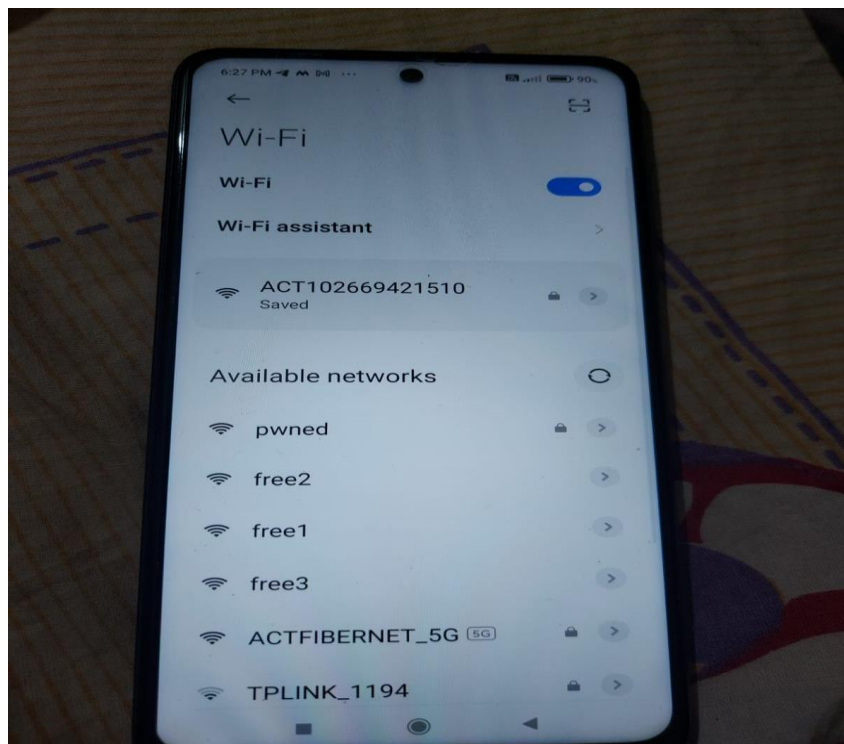


Fig 6.1 Beacon Attack

6.2 Results:

- In this system, we used NodeMCU and then we uploaded the jammer firmware using ESP8266 flasher.
- When the supply is given, LED is turned on to give the indication that the jammer has started.
- The jammer signal is transmitted using the antenna and the tank circuit is made to extend the range of jammer.
- So after attacking the selected Wi-Fi, device gets disconnected as shown in

the image. Unless the jammer is turned off , the device is not able to connect to the selected Wi-fi.

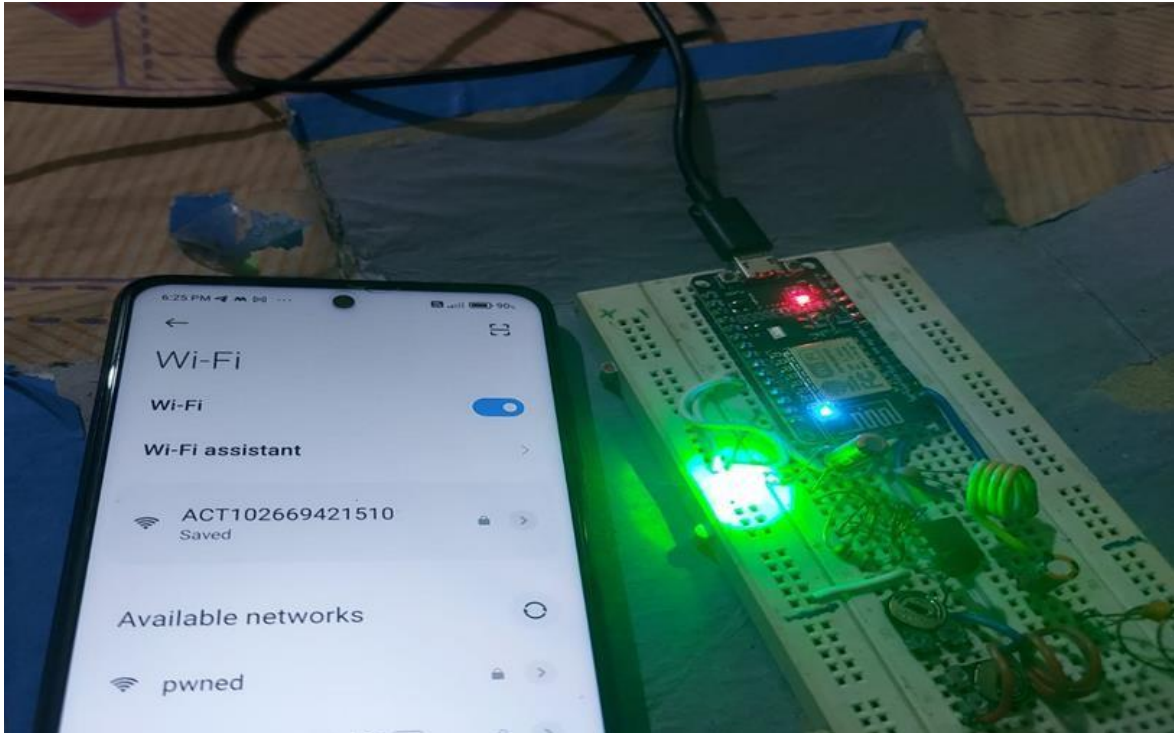


Fig 6.2 Working Model

6.3 APPLICATIONS:

- Easy to operate.
- It can also be used to detect the incoming and outgoing messages/calls on cell phones and electronic devices , which can be a security threat in certain environments.
- It could be used to block attempts to connect to a wireless network from unauthorized devices or individuals.
- It could be used to maintain a quiet and peaceful environment in places such as hospitals, schools, colleges, etc.
- It can also flood Wi-Fi networks which can serve as a preventive measure against cyber attacks initiated by hackers using spamming techniques.

6.4 LIMITATIONS:

- Tuning the presets of the tank circuit is a big challenge. With slight variation, the strength may change.
- It typically has a limited range, and their effectiveness decreases with distance. In addition, their range may be affected by obstacles, such as walls or other structures.
- It can interfere with other wireless technologies that operate in the same frequency band, such as Bluetooth, etc.
- The ESP8266 does not support 5GHz.
- There are some legality issues in few places and, using them can result in legal consequences, including fines.

CHAPTER 7

STANDARDS & CONSTRAINTS

7.1 STANDARDS:

IEEE 802.11- It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60Hz frequency bands. It is primarily concerned with the lower layers of OSI model. This standard is concerned most effective when it comes to the low power consumption of devices.

WiFi Deauther is a tool that allows for WiFi deauthentication attacks, which can be used to disconnect devices from a WiFi network. Since it is not an IoT device itself, it does not have any IoT standards specific to it.

However, WiFi Deauther can be used with other IoT devices that support the Wi-Fi standard. In that case, the IoT devices would need to adhere to the Wi-Fi standard, which is IEEE 802.11 b/g/n, just like NodeMCU. Additionally, the IoT devices would need to adhere to the security protocols that are in place on the network, such as WPA2 or WPA3.

IoT standards for NodeMCU:

Wi-Fi: NodeMCU supports the IEEE 802.11 b/g/n Wi-Fi standard, which is the most common standard for wireless networking.

MQTT: MQTT (Message Queuing Telemetry Transport) is a messaging protocol for IoT devices. NodeMCU can be programmed to use MQTT to communicate with other IoT devices or with a central server.

CoAP: CoAP (Constrained Application Protocol) is a lightweight protocol for IoT devices that are resource-constrained. NodeMCU can be programmed to use

CoAP to communicate with other IoT devices or with a central server.

HTTP: NodeMCU supports HTTP (Hypertext Transfer Protocol), which is the standard protocol for communication on the World Wide Web. NodeMCU can be programmed to send HTTP requests and receive HTTP responses.

TLS: TLS (Transport Layer Security) is a protocol for securing communication over the internet. NodeMCU can be programmed to use TLS to encrypt its communications.

IPv6: NodeMCU supports IPv6 (Internet Protocol version 6), which is the latest version of the Internet Protocol. IPv6 provides more addresses than IPv4, which is important for IoT applications that may involve many devices.

Devices using Wireless Communication:

While there are no specific IoT standards for signal detectors, there are some standards and protocols that are relevant for IoT devices that use wireless communication.

Wireless communication standards: IoT devices that use wireless communication typically adhere to a specific wireless standard, such as Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), or Zigbee (IEEE 802.15.4). A signal detector that is used to analyze these devices must be able to detect and analyze signals in the appropriate frequency range and modulation scheme.

Security protocols: IoT devices that use wireless communication typically implement some form of security protocol, such as WPA2 or WPA3 for Wi-Fi or AES-128 for Zigbee. A signal detector that is used to analyze these devices must be able to identify and analyze the security protocols in use.

Interoperability standards: There are various interoperability standards for IoT devices, such as MQTT or CoAP. A signal detector that is used to analyze these devices must be able to identify and analyze the relevant protocols and message

formats.

Network protocols: IoT devices typically use various network protocols to communicate with each other and with central servers. These protocols include TCP/IP, HTTP, and HTTPS. A signal detector that is used to analyze these devices must be able to identify and analyze these protocols.

Regulations for BC548 Transistor:

In general, electronic components such as the BC548 transistor are subject to various standards and regulations related to safety, performance, and environmental impact. These standards are established by organizations such as the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), and the Restriction of Hazardous Substances (RoHS) Directive.

7.2 CONSTRAINTS:

- The biggest concern about signal jammers is that they can block emergency communications and can result in reduced productivity.
- It can potentially violate various laws and regulations, including those that pertain to cybercrime, privacy, and network security. It is essential to understand and comply with these laws, as well as any policies and guidelines set by the network owner or administrator.
- Some newer devices may have improved security features that make them less vulnerable to WiFi deauther attacks, such as implementing stronger encryption or security protocols.
- At common places, people feel inconvenience if their network is blocked without their knowledge.

CHAPTER 8

CONCLUSION

- In the proposed system, a novel cascaded detector-jammer circuit is recommended to detect and block the devices from connecting in restricted areas.
- This handy pocket-sized system can detect the RF signals from a cell phone with transmission frequency ranging from 0.9GHz to 3GHz comes under the category within 2G, 3G and 4G networks.
- For deauther, we have flashed the jammer firmware into NodeMCU ESP8266.
- The Wi-Fi protocol called 802.11 acts as a deauthentication frame.
- It prevents unauthorized access to their wireless network.
- This suggested design can be made useful for more places where devices and network are prohibited such as Petrol pumps, Gas stations, Courts, Military bases, Theatres, Hospitals despite its use in Examination halls, Confidential rooms, etc.
- Moreover, the system with the detector and jammer circuit together can serve the need for trouble-free security applications.

PAPER PUBLICATION



REFERENCES

- [1.] N. R. Krishniah, "Dual Band", International Journal of Modern Engineering Research(IJMER) Vol. 3, Issue. 4, Jul - Aug. 2013.
- [2.] P. Raveendra Babu, International Journal of Science, Engineering and TechnologyResearch (IJSETR) Volume 2, Issue 9, September 2013.
- [3.] Hongbo Liu* and Wenyuan Xu , Localizing Jammers in Wireless Networks vol. 1, Issue 6 May 2013 .
- [4.] Rick Hartley, RF / Microwave PC Board Design and Layout, Avionics Systems.
- [5.] John Scourias, Overview of the Global System for Mobile Communications, University of Waterloo.
- [6.] Pozar, D., Microwave Engineering, John Wiley and Sons, Tony Van Roon, 555 timer tutorial, 2015.
- [7.] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada. Use of jammer and disabler. Devices for blocking PCS, Cellular & Related Services.
- [8.] Prasad, Sudarshan, and David J. Thuent. "Jamming attacks in 802.11 g—a cognitive radio based approach." MILITARY communications conference, 2011-MILCOM 2011. IEEE, 2011.
- [9.] Multitopic conferences, 2008. INMIC 2008. IEEF international
- [10.] www.howstuffwork.com/
- [11.] Ahmed Jisrawi, "GSM 900 mobile jammer", undergrad project, just, 2006.
- [12.] Sami Azzam, Ahmad Hijazi, Ali Mahmoudy. " smart jammer for mobile phone system"
- [13.] www.tangret.com
- [14.] www.mobilejammer.co.in
- [15.] academia.edu