SIGNAL JAMMER

MARKANDEY, NALIN RAJ
Dept. of Electronics and Communication Engineering
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

Dr. S. BARANI , M.E., PhD, Associate Professor
Dept. of Electronics and Communication Engineering
Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

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. To address this problem, a suggested system has been proposed that can effectively operate in areas where the cell phones are restricted. This system is designed to identify spying and unauthorized video transmissions, as well as incoming and outgoing calls and messages, even when the mobile phone is in silent mode. Also, to enhance security in private networks or block unwanted access to wireless networks. The system is composed of a small-sized detector-jammer circuit that utilizes CA3130EZ to detect RF transmission signals within the frequency ranges and then block the Wi-Fi signals.

Keywords: Mobile Detector, RF Signal, Wi-Fi Jammer, and oscillator.

I. INTRODUCTION

A WiFi jammer is a type of signal jammer which is created to interfere with the regular operation of wireless networks, specifically those operating on the 2.4GHz and 5GHz frequency bands. In this research paper, we will explore the technology behind WiFi jammers, their applications, and potential legal issues associated with their use. Initially, mobile jammers were developed with the intention of assisting law enforcement and the military in interrupting communication among criminals and terrorists, as well as preventing the activation of particular explosives that can be detonated from a distance. However, as public annoyance over the use of mobile phones in public places became more evident, the potential civilian applications of mobile jammers also became apparent. In present times, cellular devices have become an essential instrument in our everyday routines. For example, in India, there are numerous mobile network carriers such as Airtel, VI, Jio, etc. that operate on GSM 900 frequency. While the widespread use of phones can cause various issues, a ringing phone can also be bothersome in certain situations. This is where cell phone signal jammers come in. The jamming equipment sends out a packets to interfere with the Wi-Fi signal. This leads to a message on the cell phone screen indicating that no network is

available.

II. OBJECTIVE OF THE PROJECT

The objective of a signal jammer is to disrupt wireless communication by emitting radio frequencies on the same frequency bands used by wireless devices, such as cell phones, Wi-Fi routers, and GPS devices. This interference results in either complete loss of signal or degraded signal quality. Signal jammers are primarily used in situations where wireless communication needs to be disrupted, such as in military operations, security applications, and prisons. They can also be used by individuals who want to block wireless signals, such as during exams or in movie theaters. The objective of using signal jammers is to prevent unauthorized communication, protect confidential information, and enhance security in certain situations. However, their use is highly regulated due to potential legal and safety issues.

III. PROPOSED SYSTEM

The suggested system involves integrating two designs to create a straightforward, compact, adaptable, and user-friendly design, consisting of both detector and jammer circuits. The system utilizes an LM358 IC OP-AMP that can recognize the existence of mobile phones and obstruct signals in the GHz range for mobile networks. The proposed detector can detect RF signals during incoming/outgoing calls and messages. This design can block signals within a radius of up to 50m for GSM signals and contains components such as NodeMCU, presets, copper antennas, capacitors, and resistors. Since the system operates on battery, it is highly handy. Additionally, it has a low power rating, can store energy for an extended period, and includes innovative features like efficient LED and lightning systems. It also prevents against cyber-attack initiated by hackers by using spamming techniques.

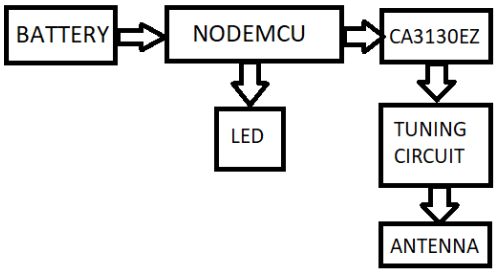


Fig 1. Proposed Design

3.1 NodeMCU

NodeMCU is an open-source development board and firmware specifically designed for Internet of Things (IoT) usage. This platform is built upon the ESP8266 microcontroller, which is an economical Wi-Fi chip with complete TCP/IP stack and microcontroller functionalities. NodeMCU provides an easy-to-use platform for developing and prototyping IoT devices, allowing developers to write Lua scripts or C++ programs to interact with various sensors and actuators.

Fig 2. NodeMCU

3.2 LM358 IC

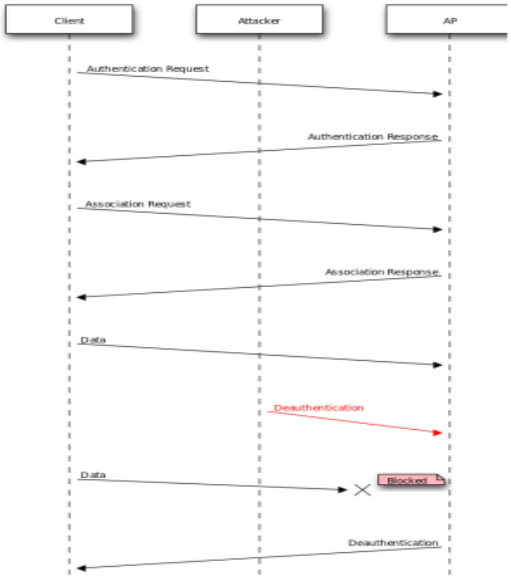
The LM358 has a high gain bandwidth product of 1 MHz and a low input bias current of 20 nA, making it suitable for low-power applications. The LM358 has a wide supply voltage range of

3-32V, making it compatible with a wide range of power supply voltages.

Fig 3. LM358 IC

IV. METHODOLOGY

Proposed System consists of detector and jammer circuits. Here we use LM358 IC, which identifies presence of mobile phones and can detect RF signals. The wifi jammer circuit, with help of jammer firmware uploaded to nodemcu, it dispatches packets to obstruct your Wi-Fi signals, resulting in the disturbance of your Wi-Fi router's regular functioning.



V. CALCULATION

Mobile phones operate on different frequency bands in various countries. In Canada, 1900 MHz is the primary band for urban locations, while 850 MHz is the fallback for rural areas. The United States, however, uses both 850 and 1900 MHz bands, depending on the region. European countries generally use GSM 900 and 1800 bands as their standard, which are also widely utilized in the Middle East, Asia, and Oceania. In certain countries like Russia, local carriers hold licenses for the 450 MHz frequency to offer CDMA coverage. Developing a jammer that can function on all frequencies becomes challenging due to the use of various frequencies in different regions. However, for the tank circuit, this formula can be used to calculate the values:

$$F = 1/(2*pi*sqrt(L1*C1))$$

Based on the frequency to block, the values of the inductance (L1) and capacitance (C1) can be changed.

VI. RESULTS

The result of a WiFi jammer is disruption of wireless communication on the targeted frequency band. When a WiFi jammer is activated, it emits radio frequency signals on the same frequency bands used by WiFi networks, causing interference and disrupting the normal functioning of the wireless network. This interference results in either complete loss of signal or degraded signal quality, making it difficult or impossible for devices to connect to the network or communicate effectively.

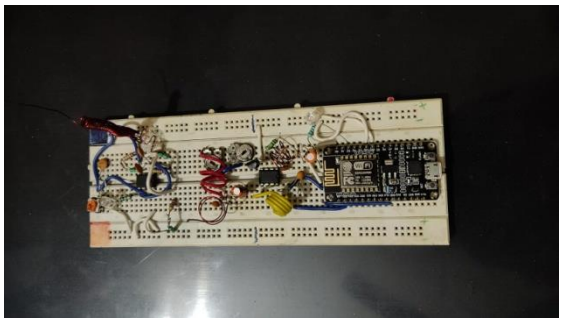


Fig 4. Signal Jammer Circuit

VII. CONCLUSION

The proposed system recommends using a new cascaded detector-jammer circuit to detect mobile phone signals in restricted areas. This portable device is small enough to fit in a pocket and can identify RF signals from mobile phones with transmission frequencies ranging from 0.9GHz to 2.5GHz, which fall within the 2G, 3G, and 4G network categories. The architecture has the capability to identify the exchange of information between the cellular device and the primary station, and can be combined with other user-friendly designs to create a comprehensive set of features. This design can be useful in a variety of places where mobile phones are prohibited, including petrol pumps, gas stations, theaters, hospitals, courts, military bases, as well as examination halls and confidential rooms. Additionally, combining the detector and jammer circuit in one system can fulfill the need for privacy and cyber-security applications.

VIII. REFERENCES

[1.] N. R. Krishnan, “Dual Band”, (IJMER) Vol. 3, Issue. 4, Jul - Aug. 2013.

[2.]https://electronicslovers.com/2019/01/a-simple-homemade-wi-fi-jammer-by-using-an-esp8266-diy-project.html

[3.] Hongbo and Wenyuan Xu , Jammers in Wireless Signals vol. 1, Issue 6 May 2013 .

[4.] Hartley, RF PC Board Design and Layout, Avionics Systems.

[5.]https://circuitdigest.com/microcontroller-projects/diy-wifi-jammer-using-nodemcu-esp12

[6.]Puzar, Microwave Engineering, John Wiley, Tony Roon, 555 timer tutorial,2015.

[7.]The Mobile & Personal Communications Committee, for blocking PCS, cellular, and related services.

[8.]www.techtarget.com/searchnetworking/definition/American-Wire-Gauge

[9.] Multitopic conferences, 2008. INMIC 2008.IEEF international

[10.]www.electronicshub.org/cell-phone-detector-circuit/

[11.] Ahmad Jesrawi, ”GSM 900 mobile jammer”, project,2006.

[12.] Sami Azam, Ahmed Hizazi, Ali Mahmudy.” jammer for mobile phone system”

[13.]www.renesas.com/us/en/document/dst/ca3130-ca3130a-datasheet

[14.] www.jammer.co.in

[15.]https://github.com/SpacehuhnTech/esp8266_deauther/wiki/FAQ