e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704036 |

WIFI JAMMER: using ESP8266 Microcontroller

Dhage Vidyasagar[1], Walunjkar Tejas [2], Hase Dhanashri[3], Prof.Sachin.P. Vidhate[4]

Student, Department Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India[1,2,3]

Department Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra, India[4]

ABSTRACT: A WiFi jammer is a device that disrupts wireless network signals, typically by emitting radio frequency interference on the same frequencies used by WiFi devices. Its abstract concept involves interfering with WiFi communications, rendering them ineffective within a certain range. it's essential to note that using WiFi. jammers is illegal in many countries due to their potential for causing network disruptions and privacy violations. They are typically employed for malicious purposes and can result in severe legal consequences. we investigate the impact of jamming attacks on the performance of smartphones regarding their WIFI access and propose a real-me jamming detection method based on the received signal strength indicator and the packet loss rate of WIFI signals, which can be easily implemented on Android smartphones. Experiments are performed to evaluate the proposed jamming detect on method, in which universal soware radio peripherals are used as jammer to block the WIFI signals between smartphone phones and wireless routers. Experimental results show that the proposed applicaton can detect jamming attacks with small false alarmrate and miss detection rate. It is true that every technology has its advantages and disadvantages regardless of its complexity and perfectness. It is true in case of jamming also. It has many advantages in battles, cold conflicts between two nations. In many countries, deauthers are illegal, except in the military, law enforcement and other government agencies, where deauthers are largely used to prevent bomb detonation or to isolate suspects in hostage situation.There is, in fact, a way to create a Node-MCU Wi-Fi jammer although technically, this is adeauther and a jammer. A jammer sends out noise on the Wi-Fi frequency spectrum (2.4 GHz) while the program in this tutorial sends packets that disrupts the normal functions of your WiFi router. So if the aim is to block WiFi to users and other features are to block unknown users using our network, Clone a wi-fi into may to get confuse of hackers
.

I. INTRODUCTION

A Wi-Fi is a trade mark term used for IEEE 802.11 set of LAN protocols that implements wireless local area network in various frequencies. The IEEE 802 protocol specifies physical layer (PHY) and media access control layer (MAC) protocols to implement LAN.The Wi-Fi works on the RF (radio frequency) technology since there is no physical connection between the sender and the receiver. It functions when a frequency within the electromagnetic spectrum associates with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The wireless connection has an end point named as the Access point (AP).The key job of an access point is to broad casta wireless signal that computers can detect and "tune"into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters. Wi-Fi is supported by many applications and devices including video game consoles,home networks, PDAs, mobile phones, major operating systems and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" by the Wi-Fi Alliance are certified as inter operable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified"and indicates the radio frequency band used (2.5GHz for 802.11b, 802.11g, or 802.11n,and 5GHz for 802.11a).A Deauther allows you to disconnect devices from a WiFi network . Even if you're not connected to that network. Deauther take advantage of aweakness in the 802.11protocol which allows the sending of deauthentication frames by unauthorised devices.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704036 |

II. LITERATURE SURVEY

Title: Quadcopter Design and Implementation as a Multidisciplinary Engineering Course

Description: Main objective is the design and implementation of quadrotor helicopter system.Only Design For Quadcopter not for Provide any stabilization..

Title: Secure Two-Way Transmission via Wireless Powered Untrusted Relay and External Jammer

Description: In this paper, we propose a two-way secure communication scheme where two transceivers exchange confidential messages via a wireless-powered untrusted amplify and-forward relay in the presence of an external jammer. We take into account both friendly jamming (FJ) and Gaussian noise jamming (GNJ) scenarios

Title: Jamming Detection of Smartphones for WiFi Signals

Description: In this paper, we investigate the impact of jamming attacks on the performance of smartphones regarding their WiFi access and propose a real-time jamming detection method based on the received signal strength indicator and the packet loss rate of WiFi signals, which can be easily implemented on Android smartphones. Experiments are performed to evaluate the proposed jamming detection method,

III. WORKING MODULE

The Arduino IDE can be downloaded and set up freely from Arduino. cc website.
First, need to Install the Arduino IDE & open it.
After that Go to File Option –> Preferences.
Need to add esp8266 packages to the extra board's manager URLs.
Next open Tools –> Board –> Boards Manager
Search for esp8266 after that install the board.
Lastly, IDE needs to restart.
Need to download the repository (Release Version 1.5) from GitHub.
Take out the downloaded folder & find the way to the following path for opening the file within Arduino IDE.
Open Tools –> Board and choose the suitable board that you are utilizing.
Open Tools –> Port –> and choose the right comm. port.
Click the upload button.
Once the tab alerts that uploading is done then the device is ready to use.Now module needs to be connected through a power supply with a micro USB connector or a battery.
Once this module is connected to a WiFi with the name of "pwned" then you have to connect to this WiFi network using a phone/laptop & enter the secret word as "deauther".Once it is connected to the device, then open a browser & navigate to the IP address 192.168.4.1. Because this is the main website from wherever you can control all
At last, choose the WiFi connection you wish to attack.

IV. ADJUSTING THE JAMMING RADIUS AND POWER

One of the key aspects of effective WiFi jamming with the ESP8266 microcontroller is being able to precisely control the jamming radius and power output. This allows you to disrupt wireless communications within a specific target area without affecting nearby networks or devices that you do not intend .

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704036 |

50M		**100M**
200M		**Jamming Radius**

By adjusting the transmit power of the ESP8266, you can tune the jamming radius to cover just the desired target area. Lower power settings will result in a smaller jamming radius, while higher power will extend the disruption over a wider area. It's important to find the right balance to avoid unwanted interference

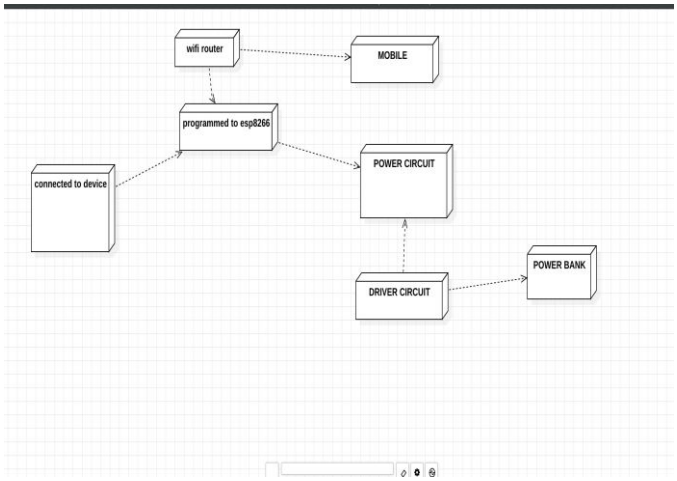
10W	**20W**
50W	**Jamming Power**

The jamming power is another critical factor to control. Higher power settings can overwhelm and disrupt wireless signals over a larger area, but also consume more energy and risk legal issues if the jamming extends beyond your immediate vicinity. Carefully calibrating the power level allows you to achieve the desired jamming effects while staying within safe and lawful limits.

IV. CONCLUSION

Jammers are very usefull to the society from the anti-social elements. We can save our national leaders. We can restrict the communication network between the anti-social elements by using the cell phone jammers. Cell phone jammers prevent the students from carrying cell phones to the colleges. As everything goes fifine, it is very necessary to implement in all the colleges.

.



| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704036 |

REFERENCES

[1] A. Yenner and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814– 1825, Sep. 2015.
[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[3] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. L- Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32– 39, ec.2015.
[4] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Inf. Theory Workshop*, 2001, pp. 87–89.
[5] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer Security game: Interaction between source ,eaves dropper and friendly jammer, " *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 452907-1–45290710, Mar. 2009.
[6] D. Fang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Cooperative jamming protocols in two-Hop amplify-and- forward wiretap channels," in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, pp. 2188–2192, Nov. 2013.
[7] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.
[8] K. Wang, L. Yuan, T. Miyazaki, S. Guo, and Y. Sun, "Anti-eavesdropping with selfish jamming in wireless networks: A bertrand game approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6268–6279, Jul. 2017.
[9] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Globecom*, New Orleans, LA, USA, Dec. 2008, pp. 1–5.
[10] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.
[11] A. Kuhestani, A. Mohammadi, and M. Noori, "Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay," *IET Commun.*, vol. 10, no. 8, pp. 962–968, May 2016.
[12] J.-B. Kim, J. Lim, and J. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866–3876, Jul. 2015.
[13] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 341–355, Feb. 2018.
[14] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for Two way untrusted relaying with friendly jammers,"*IEEETrans.Veh.Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.
[15] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.
[16] J. Huang and A. L. Swindle hurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Nov. 2013, pp. 1555–1559.
[17] H. Xu, L. Sun, P. Ren, and Q. Du, "Securing two-way cooperative systems with an untrusted relay: A onstellation-rotation aided approach," in *Proc. IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2270–2273, Dec. 2015.
[18] A. Kuhestani, P. L. Yeoh, and A. Mohammadi, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying," *IEEE Global Commun. Conf.*, Singapore, pp. 1–6, 2017, doi: 10.1109/GLOCOM.2017.8254424.
[19] M. L. Ku, W. Li, Y. Chen, and K. J. Ray Liu, "Advances in energy harvesting communications: Past, present, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1384–1412, Apr./Jun. 2016.
[20] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2363– 2367.
[21] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607–1622, May 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com