Science Forum (Journal of Pure and Applied Sciences)

Journal Homepage: https://atbuscienceforum.com.ng/index.php/jpas

Design And Construction of Frequency Hopping Circuit in a Wireless Communication Network

Dakaya Ibrahim Yahaya[1,2], Auwalu Musa[1], Salisu Hussaini Musa[3]

[1]Department of Physics, Bayero University, Kano, Nigeria

[2]National Institute of Security Studies (NISS), Abuja, Nigeria

[3]Dept. of Physics, Sa'adatu Rimi College of Education, Kumbotso, Kano, Nigeria

Abstract

This study presents the design and implementation of a cooperative wireless communication network that employs the Frequency Hopping (FH) technique as a countermeasure against interference and malicious attacks. In frequency hopping, both transmitting and receiving circuits dynamically change operating frequencies within predetermined time intervals. This approach significantly reduces the risk of interception and disruption by untrusted nodes, thereby ensuring that confidential information remains secure between legitimate endpoints. The inherently open nature of wireless networks exposes them to security threats such as jamming, eavesdropping, and unauthorized access, which compromise both the confidentiality and reliability of transmitted signals. To address these challenges, a Frequency Hopping Anti-Jammer system was developed using an ESP32 microcontroller. The microcontroller executes the program logic for message generation, transmission, and reception while simultaneously controlling the frequency-hopping sequence. By rapidly and unpredictably altering carrier frequencies, the system effectively mitigates jamming attacks and makes unauthorized interception extremely difficult. The proposed design has practical applications in scenarios where highly secure communication is critical, particularly for security agencies, defense operations, and top-level government officials whose engagements demand maximum confidentiality and resilience against wireless attacks. This work demonstrates that frequency hopping, when combined with low-cost embedded hardware, can provide a robust, scalable, and energy-efficient solution for securing wireless networks in sensitive communication environments.

Keywords
Eavesdropping, Anti Jammer, Frequency Hopping, Microcontroller

Corresponding Author: Dakaya Ibrahim Yahaya, Department of Physics, Bayero University, Kano, Nigeria
Email: amusa.phy@buk.edu.ng, ibrahimyahayadakaya@gmail.com

Introduction

Wireless communication has revolutionized the way people connect and share information, enabling seamless connectivity across various devices. However, this increased reliance on wireless networks has also made them susceptible to malicious interference, commonly perpetrated through devices known as jammers. Jamming can cause Denial-of-Service (DoS) problem which may result in several other higher-layer security problems, although these are often not adequately addressed (Wood et al, 2017).

Recently, cooperation-based physical layer security has emerged as an attractive solution to improve the secrecy of low-power single-antenna wireless systems (Bassily et al., 2017). Traditionally, the secrecy is guaranteed mostly relying on the cryptographic techniques and protocols at the upper layers of wireless networks (Kartalopoulos, 2016).

Jain and Garg (2019) used hybrid anti-jamming system by combining three (3) defense techniques: Base Station (BS) replication, base station evasion and multipath routing between base stations. The replication scheme implies that multiple replicated base stations are present in the network. Evasion scheme refers to the spatial retreat of a base station when jamming is detected. Eight (8) Multipath routing takes place when there are multiple data routes between a node and a base station. These countermeasure techniques can be used to deal with jamming at base stations, either individually or collectively.

One main drawback of these existing techniques is the complex mathematics computation in the secret key generation, distribution and management. In this work, we discuss one of the most common cooperative schemes in physical layer security, which is frequency hopping technique, where transmitting and receiving signals interchange upon sensing interference from untrusted nodes, so as to degrade the wiretap channel for greatly enhancing the secrecy rate. In addition, node cooperation is also beneficial to enhance the spectral efficiency and power utilization.

THEORIES AND PROBLEM FORMULATION

Effect of Jamming as illustrated in Figure 1, is a serious threat to our interconnected world of communication.

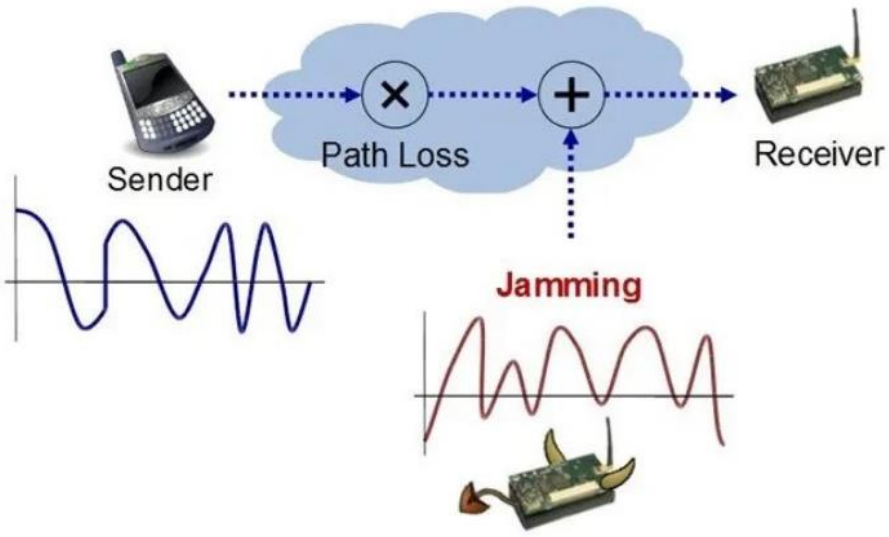

Figure 1: Jamming Attacks in Wireless Network. Ben (2023)

It is assumed that the total system bandwidth is W, and the symbol period is Ts. Thus, the Degree of Freedom (DoF) of the communication signal space is 2TsW, namely, all the communication signals can be expressed as the combination of 2TsW normalized.

Orthogonal primary functions ϕk (k = 0, 1, . . ., 2TsW − 1) (Simon et al., 2022). As such, after dividing the signal space of CSSAJ into K subspaces, the DoF of each subspace is D = 2TsW/K. In each timeslot, the transmitter randomly selects one of the subspaces for communication, i.e.

$$sk = \sum_{i \in Ak} ai\varphi i, \qquad (1)$$

Where Ak = {i: (k − 1) D ≤ i < kD}, and {ai} is the set of the transmitted symbol. Then, the power of sk is

$$E_S^t = \sum_{i \in A_k} a_i^2, \qquad (2)$$

Besides, the received signal can be expressed as

$$r_k = s_k + J, \qquad (3)$$

Where J is the jamming signal.

Note that the effects induced by the natural channel noise are ignored in the above equation for brevity. In order to launch effective jamming attacks without the knowledge of the communication signal subspace, the jammers should distribute their power in signal spaces as many as possible (Yao, 2021; Simon et al., 2022), i.e.,

$$J = \sum_{i=0}^{2T_sW-1} J_i\varphi_i + J_0 \quad (4)$$

Where $\{J_i\}$ and J_0 are the jamming signals inside and outside the communication signal subspace, respectively. Thus, the power of the jamming signal is

$$E_J^t = \sum_{i=0}^{2sW-1} J_i^2 \quad + E_{J_0} \quad (5)$$

After filtering the received signal r_k by using the set of the primary functions $\{\phi Ak\}$ synchronously, the output signal is

$$r_k^{out} = a_i + J_i, i \in A_k \quad (6)$$

Where the power of the communication signal and the jamming signal are

$$E_s^r = \sum_{i\in A_k} a_i^2 \quad (7)$$

$$E_J^r = \sum_{i\in A_k} J_i^2 \quad (8)$$

Define the spread spectrum processing gain Gp as the ratio of output and input signal-to-jamming energy ratio at receiver (Yao, 2021; Simon et al., 2022), namely,

$$G_p = \frac{E_s^r}{E_J^r} \Big/ \frac{E_s^t}{E_J^t} \quad (9)$$

Comparing Eq. 5 with 7, it can be observed that the power of the communication signals does not change after spread spectrum processing, i.e., Et s = Er s . Thus, Eq. 9 can be simplified into Gp = Et J /Er J . Assuming that J_0 = 0 and jamming power is distributed in the K subspace uniformly, we can obtain Gp = K by comparing Eq. 5 with 8. In other words, the essence of CSSAJ is to disperse the jamming power by expanding the legitimate signal subspace. However, with the significant increase of devices and the advancement of electromagnetic jamming attacks, it is challenging to obtain satisfactory anti-jamming performance by using CSSAJ, which calls for the new capability of Anti-Jamming communications.

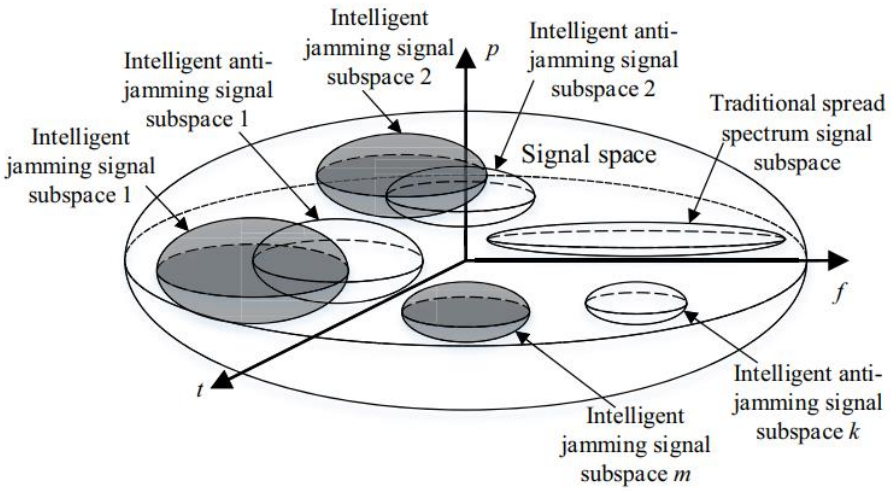

Figure 2: Relationship between Jamming and Anti-Jamming, (Yao, 2021; Simon, et al., 2022)

However, as the jamming power increases and the jamming pattern becomes more unpredictable, the performance gain of the existing anti-jamming techniques decreases significantly. When there exists another signal subspace besides frequency f, time t, and power p, the signal space in Figure 3 becomes a hypersphere.

MATERIALS AND METHODS

This work focusses on design and construction of Intelligence Anti- jamming as shown in Figure 3, where jamming recognition and intelligent decision (Anti-Jamming) modules are embedded at microcontroller of both the transmitter and receiver of IAJ. Carrier Frequencies at the Transmitting and Receiving ends are designed to hop, when interference is noticed, making it difficult for signal jamming.

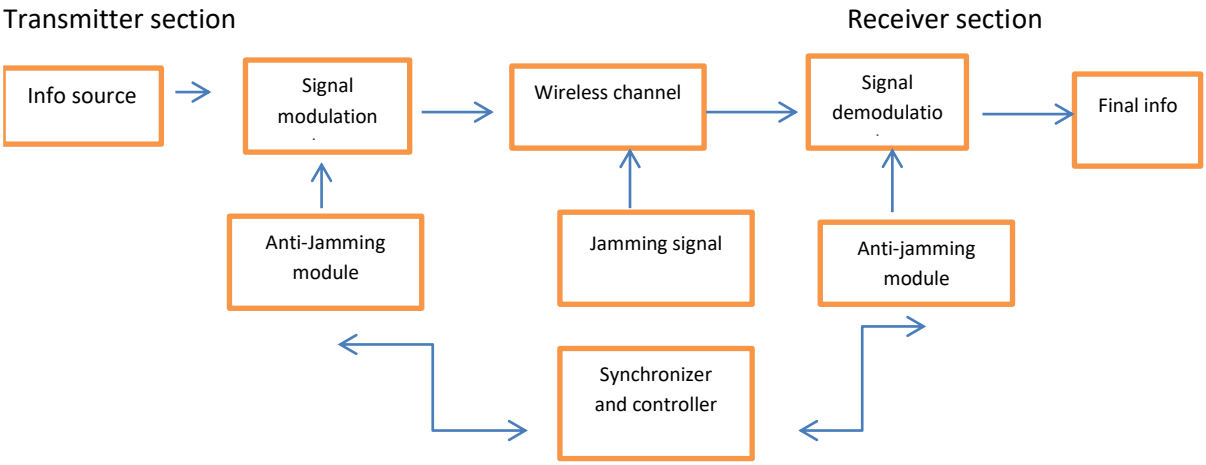

Figure 3: Intelligence Anti-jamming

System Architecture

The Circuit can be simplified in a block form as shown in Figure 4.

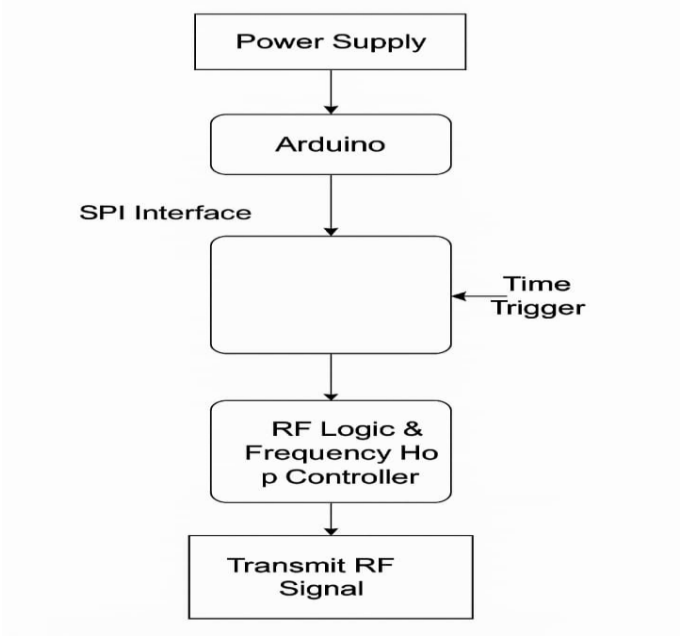

Figure 4: Block Diagram of Frequency Hopping Transmitter

a. **Power Supply Section**: The section provides the expected 9volt voltage to energize the Circuit system. The section comprises both DC Voltage supplier, Voltage Regulator and Bulk Converter. $V = IR$ (10)

The Value is fed into LM7809 regulator, which further regulate the supply from voltage source, the 100μf capacitor remove the ripple voltage and block fluctuations while the LM2596 bulk converter is connected to step down the voltage value to between 3 and 4volt, suitable for the microcontroller.

b. **ESP32 Microcontroller**: The Microcontroller is programmed such that, it runs a code that generates and reads the message to be transmitted. 10nf bypass capacitor is connected at the enable pin of the microcontroller IC to decouple the sub-circuit from voltage spike. 1kΩ is used as pull-up or pull-down resistor for microcontroller. The code as reflected below enables the Circuit to function as Frequency Hopper.

CODES FOR ESP32 TRANSMITTER

```
include <RadioLib.h>
CC1101 radio = new Module(5, 4, 2); // NSS, DIO0, DIO1
#define BASE_FREQ_MHZ 433.0   // or 915.0 depending on your module
#define CHANNEL_SPACING 0.2
#define NUM_CHANNELS 8
#define HOP_INTERVAL_MS 1000
uint8_t currentChannel = 0;
unsigned long lastHopTime = 0;
uint32_t packetCount = 0;
unsigned long lastSendTime = 0;
void setChannel(uint8_t channel) {
  float freq = BASE_FREQ_MHZ + channel * CHANNEL_SPACING;
  radio.setFrequency(freq);
  Serial.print("TX hopping to: "); Serial.println(freq);
}
void setup() {
  Serial.begin(115200);
  int state = radio.begin(BASE_FREQ_MHZ);
  if (state == RADIOLIB_ERR_NONE) {
```

```
    Serial.println("CC1101 initialized");
  }
 else {
    Serial.print("Init failed, code: ");
    Serial.println(state);
    while (true);
  }
  // Optional tuning
  radio.setRxBandwidth(100.0);    // Must match receiver
  radio.setBitRate(4.8);          // Must match receiver
  radio.setOutputPower(10);       // dBm
  setChannel(currentChannel);
}
void loop() {
  if (millis() - lastHopTime >= HOP_INTERVAL_MS) {
    currentChannel = (currentChannel + 1) % NUM_CHANNELS;
    setChannel(currentChannel);
    lastHopTime = millis();
  }
  if (millis() - lastSendTime >= 1500) {
    String msg = "Hi #" + String(packetCount++);
    int state = radio.transmit(msg);
    if (state == RADIOLIB_ERR_NONE) {
      Serial.print("Sent: "); Serial.println(msg);
    }
else {
      Serial.print("TX failed, code: "); Serial.println(state);
    }
    lastSendTime = millis();
           }
```

c. **RF Logic & Freq Hop Controller :** at this section, both functions of programmable logic controller and wireless communication using Radio Frequency signals are combined, using frequency = BASE_FREQ + (channel_index * CHANNEL_SPACING).

d. **CC1101 RF Module:** This is where the message (signal) is finally transmitted at the set frequency. The module supports a wide supply voltage range of 1.8v to 12v, ensuring compatibility with different power sources. It frequency band is 315, 433, 868 and 915 MHz but can still be programmed for operation at other frequencies.

The Module is designed with this equation

$$F = \frac{Fosc}{2^{16}} \times (C + Fx) \quad (11)$$

Where F is the desired frequency to be transmitted

F_{osc} is the crystal oscillator frequency with value of 26 MHz

C is an integer between 0 and 65535 called frequency register value

F_x is a fractional value.

Since our desired transmitting Frequency (F) is around 633MHz

$C+Fx$ *can be written as* $\left(\frac{F}{Fosc}\right) \times 2^{16}$ (13)

$$C + Fx = \left(\frac{433}{26}\right) \times 65535 = 1084827$$

$$C = \frac{1084827}{2^{16}} = 16.5$$

$$Fx = 1084827 - 16.5$$

$$Fx = 1084810.5$$

Antenna Theory: For optimal transmission, the antenna length should be approximately one-quarter of the wavelength at 433 MHz, calculated as:

$$L = \frac{C}{4 \cdot f} \quad (14)$$

where c is the speed of light, and f is the frequency.

Therefore,

$$\mathrm{L} = \frac{3 \times 10^8}{4} \times 433 \times 10^6 \quad (15)$$

$$L = 0.17m$$

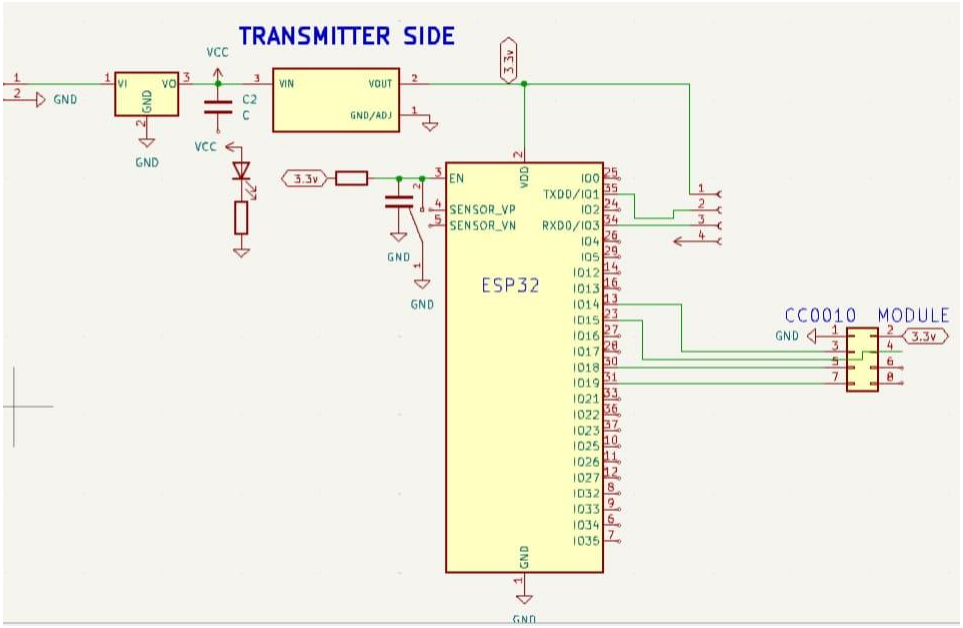

Figure 5: Schematic Diagram of Frequency Hopping Circuit

RESULT AND DISCUSSION

The LM7805 regulate the voltage obtained from DC Source while the 100μF capacitor remove the ripple voltage and block fluctuation. ESP32 microcontroller and CC1101 RF transmitter are energized through the voltage value from output of LM2596 Bulk Converter. 1kΩ is used as pull-up or pull-down resistor for microcontroller.

ESP32 Microcontroller thereafter runs a program which generates or reads the message to be transmitted. It sets the current frequency using radio.setFrequency() and also sends the message using radio.transmit () on the current frequency. The RF Controller hops the frequency at every predefined interval (e.g., every 10 second) using: frequency = BASE_FREQ + (channel_index * CHANNEL_SPACING).

The signal is finally sent to CC1101 module at the set frequency. The module supports a wide supply voltage range of 1.8v to 12v, ensuring compatibility with different power sources. It frequency band is 315, 433, 868 and 915 MHz but can still be programmed for operation at other frequencies.

The Plate 1 shows the signal generated during the working of 433MHz transmitter of the Frequency Hoping Circuit.

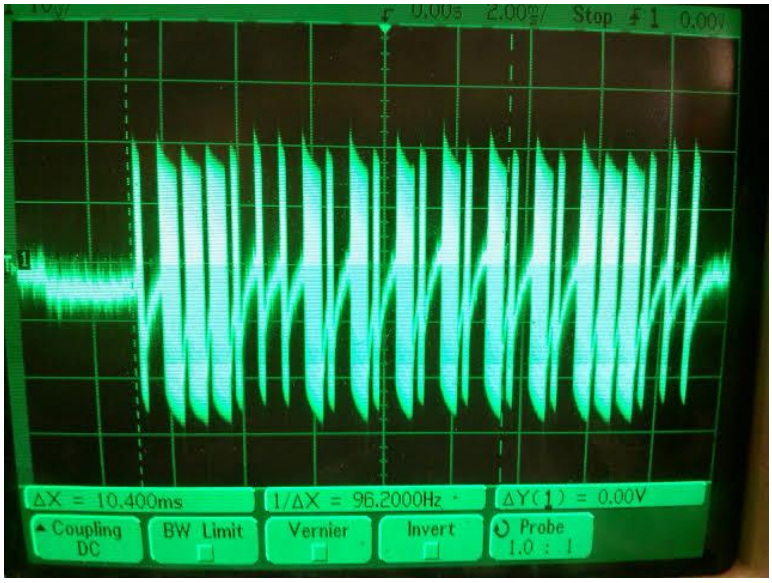

Plate 1: Transmitting output Signal

Plate 2 presents the Arduino 1.8.7 IDE (Integrated Development Environment) for the design of Frequency Hopping Circuit and the generated output.

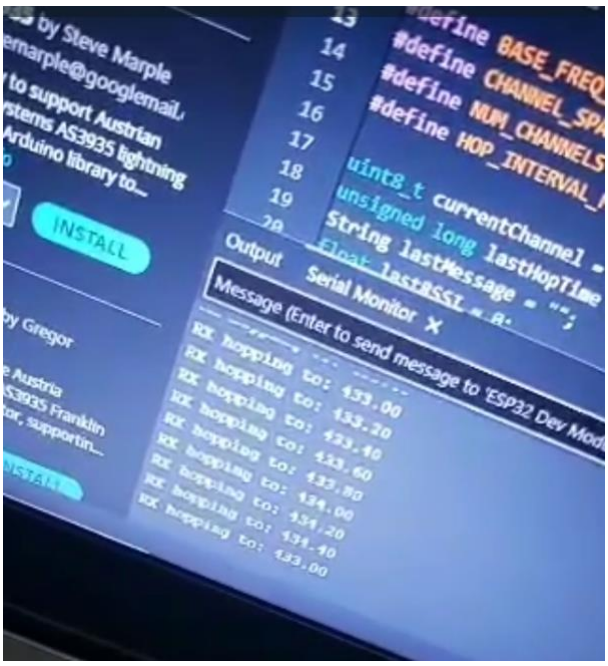

Plate 2: Programming and Simulation of the Frequency Hopping Circuit

The Figures below show pictorial test evidence and step by step processes of operation of Frequency Hopping Circuit, to further buttress the working of the project as illustrated in Plate 2.

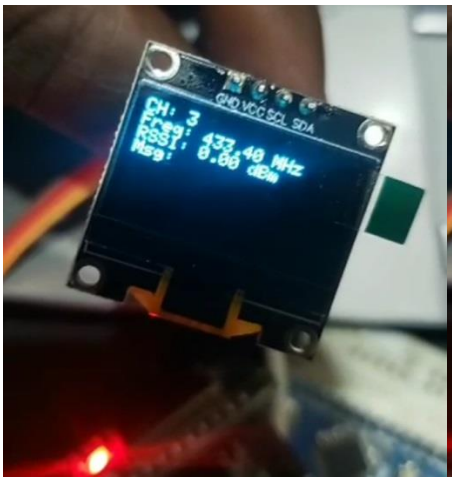

Plate 3 (a)

Plate 3 (b)

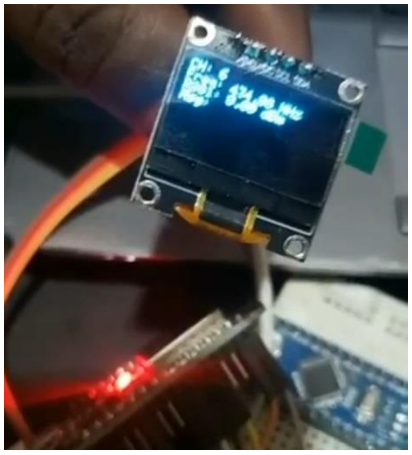

Plate 3 (c)

Table 1 explained the output of the Frequency Hopping Circuit, which changes its own Frequency within interval of time.

Table 1: Output of Frequency Hopping Signal

Time (Sec)	Freq (MHz)
10	433
20	433.4
30	433.8
40	434.2
50	433.7
60	433.3
70	433.8
80	434.2
90	434
100	433.8
110	433.4

The result is further illustrated in a graph as seen in Figure 6, which shows behavioral pattern of frequency hopping signal against Time interval.

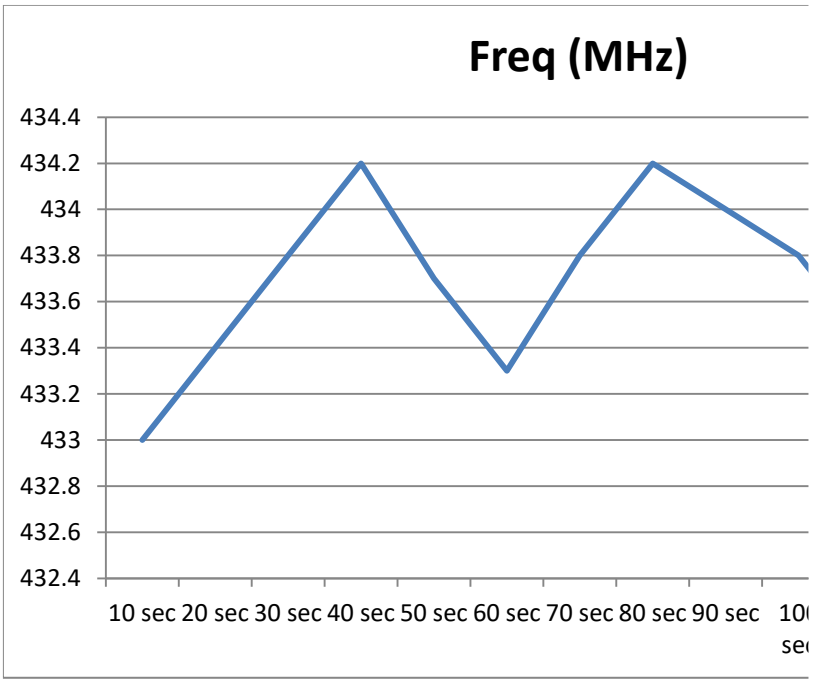

Figure 6: Graphical Representation of frequency hopping pattern

CONCLUSION

Jamming in wireless networks has historically been perceived as one of the most critical impediments to secure and reliable communication. It compromises signal integrity, increases error rates, and exposes legitimate users to denial-of-service vulnerabilities. Nevertheless, Gollakota and Katabi (2020) advanced an important paradigm shift by demonstrating that jamming can also be harnessed constructively. Their concept of *friendly jamming* illustrates how intentional interference at the physical layer can thwart eavesdropping, ensuring that adversarial entities are unable to demodulate or reconstruct legitimate transmissions. This reconceptualization reframes jamming not solely as a hostile act but also as a deliberate security enhancement mechanism.

Building on this perspective, the present work has demonstrated the efficacy of the frequency hopping spread spectrum (FHSS) technique as an anti-jamming and anti-interception approach. By rapidly and periodically altering carrier frequencies according to a predefined hopping sequence, FHSS effectively minimizes exposure to hostile interference and reduces the probability of unauthorized signal capture. This dynamic frequency agility not only limits the temporal window available for attackers but also ensures that legitimate nodes can sustain robust communication even in contested environments.

The findings of this study underscore the strategic importance of integrating adaptive spectrum management techniques such as frequency hopping with innovative defensive paradigms like friendly jamming. Together, these approaches establish a multi-layered resilience framework that enhances confidentiality, availability, and overall robustness of wireless communication systems. In light of the escalating sophistication of cyber-physical threats, the combination of proactive frequency diversity and controlled interference constitutes a promising pathway for advancing secure, resilient, and context-aware wireless networking architectures.

REFERENCES

Alnifie G, Simon R (2020) MULEPRO: a multi-channel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing 10(5):704–721

Bassily,R. Ekrem,E. He X. (2017) "Cooperative security at the physical layer: a summary of recent advances," IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 16–28, 2013.

Ben R. (2023) Jamming in Wireless Networks: Understanding the Menace Aug 6, 2023 | IoT

Bi, S. Ho,C. K. and R. Zhang, (2015)"Wireless powered communication: opportunities and challenges," IEEE Communications Magazine, vol. 53, no. 4, pp. 117–125.

Broustis I, Pelechrinis K, Syrivelis D, Krishnamurthy SV, Tassiulas L (2019) FIJI: Fighting implicit jamming in 802.11 WLANs. Security and Privacy in Communication Networks 19:21–40

Commander CW, Pardalos PM, Ryabchenko V, Shylo OV, Uryasev S, Zrazhevsky G (2018) Jamming communication networks under complete uncertainty. Optimization Letters 2(1):53–70

Fuqiang Y., Yonggang Z., Yifu S., and Wenlong G. (2023) Wireless communications "N + 1 dimensionality" endogenous anti-jamming: theory and techniques; Security and Safety, Vol. 2, 2023003 (2023) https://doi.org/10.1051/sands/2023003 sands.edpsciences.org

Gencer C, Aydogan EK, Celik C (2018) A decision support system for locating VHF/UHF radio jammer systems on the terrain. Information Systems Frontiers 10(1):111–124

Gollakota S, Katabi D (2020) iJam: Jamming oneself for secure wireless communication. Tech. rep., Massachusetts Institute of Technology

Huang H, Ahmed N, Pulluru S (2020) On limited range strategic/random jamming attacks in wireless ad hoc networks. In: IEEE 34th Conference on Local Computer Networks, pp 1–8

Jain SK, Garg K (2019) A hybrid model of defense techniques against base station jamming attack in wireless sensor networks. In: Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, pp 102–107

Kartalopoulos, S. V. (2016) "A primer on cryptography in communications," IEEE Communications Magazine, vol. 44, no. 4, pp. 146–151.

Lai L. and El Gamal, H.(2018) ",e relay-eavesdropper channel: cooperation for secrecy," IEEE Transactions on Information, eory, vol. 54, no. 9, pp. 4005–4019.

Misra S, Singh R, Mohan SVR (2020) Information warfare-worthy jamming attack detection

mechanism for wireless sensor networks using a fuzzy inference system. Sensors 10:3444–3479.

Mpitziopoulos A, Gavalas D, Pantziou G, Konstantopoulos C (2017) Defending wireless sensor networks from jamming attacks. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp 1 –5

Muraleedharan R, Osadciw LA (2016) Jamming attack detection and countermeasures in wireless sensor network using ant system. In: SPIE the International Society for Optical Engineering, vol 6248, p 62480G

Panyim K, Hayajneh T, Krishnamurthy P, Tipper D (2019) Jamming dust: A low power distributed jammer network. In: 27th Army Science Conference, pp 922–929

Pelechrinis K, Iliofotou M, Krishnamurthy S (2021) Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys Tutorials 13(2):245 –257

elechrinis K, Koufogiannakis C, Krishnamurthy SV (2009a) Gaming the jammer: is frequency hopping effective? In: Proceedings of the 7th International Conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp 187–196

Pelechrinis K, Koutsopoulos I, Broustis I, Krishnamurthy S (2019b) Lightweight jammer localization in wireless networks: System design and implementation. In: IEEE Global Telecommunications Conference, pp 1–6

Peng QH, Cosman PC and Milstein LB. (2021) Spoofing or Jamming Performance Analysis of a Tactical Cognitive Radio Adversary. IEEE J Sel. Areas Commun. 2021; 29: 903–11.

Pirayesh H and Zeng HC.(2022) Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey. IEEE Commun Surv Tutorials 2022; 24: 767–809.

Simon MK, Omura JK and Scholtz RA et al. (2022) Spread Spectrum Communications. New York: McGraw-Hill, Inc.

Strasser M, Danev B, Capkun S (2020) Detection ˇ of reactive jamming in sensor networks. ACM Transactions on Sensor Networks 7(2):16:1–16:29

Sun Y, Wang X (2019) Jammer localization in wireless sensor networks. In: 5th International Conference on

Wireless Communications, Networking and Mobile Computing, pp 1–4

Tague P, Slater D, Poovendran R, Noubir G (2018) Linear programming models for jamming attacks on network traffic flows. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops pp 207–216

Wood A, Stankovic J, Son S (2013) JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp 286–297

Wood A, Stankovic J, Zhou G (2017) DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4- based wireless networks. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp 60–69

Xiao L, Jiang DH and Xu DJ et al. (2018) Two-dimensional antijamming mobile communication based on reinforcement learning. IEEE Trans Vehicular Technol 2018; 67: 9499–512.

Xu W, Trappe W, Zhang Y, and Wood T (2015) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp 46–57

Yao FQ. (2021) Communication Anti-jamming Engineering and Practice (in Chinese). Beijing: Publishing House of Electronics Industry, 2012.