Low-Cost Network Jammer for Wi-Fi Network in Civilian Areas

*Dr. Thangam S[1], Pradeep Kumar Gupta[2], Kartthikeyan N[3], Mukil LD[4], Niranjan D K[5]
[1,2,3,4,5]*Dept. of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Bengaluru, India*
* s_thangam@blr.amrita.edu[1], bl.en.u4cse21163@bl.students.amrita.edu[2], bl.en.u4cse21094@bl.students.amrita.edu[3], bl.en.u4cse21109@bl.students.amrita.edu[4], dk_niranjan@blr.amrita.edu[5]

***Abstract* – This application presents a novel approach to address the challenge of intercepting unmanned aerial vehicles (UAVs) operating within the 2.4 GHz frequency band. Jamming device operating at 2.4 GHz, with an Arduino Nano microcontroller and nRF24L01 module included. The device is designed to accurately search available wireless networks in a specific frequency range, focused on intercepting connections between drones in this spectrum Real-time system identifies networks and selects the channels, thus disconnecting targeted frequency devices Security measures in the presence of counter-drone activities are required This technology is an important tool for growth. Using Arduino Nano and nRF24L01 modules, the jamming device offers a flexible and scalable solution designed for network security professionals. The 2.4 GHz jammer provides precise interference, allowing targeted disruption of drones operating in a specific frequency band. In addition, the paper provides a detailed introduction to well-known drones operating in the 2.4 GHz frequency range, such as the DJI Phantom series and the Parrot Bebop series, and understanding these drones is crucial for planning effective countermeasures. The paper includes implementation data and results of experimental tests, providing insights into the efficiency and feasibility of a 2.4 GHz jammer designed to combat interference in UAV networks in a specific frequency band to be used.**

Keywords: Wi-Fi disturbance, 2.4 GHz, Security, Network disturbance.

I. INTRODUCTION

As unmanned aerial vehicles (UAVs) are increasingly being integrated into a variety of applications from surveillance to disaster management, checking security aspects in their communication networks is important Tracking communications reliability Ease of handling is essential to UAV mission success This paper provides a comprehensive analysis of drone network vulnerabilities of 2.4 GHz spectrum, with special emphasis on possible sensitivity to congestion Includes identifying points using communication systems, modulation techniques , and data on transfer analysis of the project as a reliable-time -saver for finding effects By highlighting light attenuation in the 2.4 GHz frequency band, this study contributes particularly to the discussion on the safety of UAV communication systems Furthermore, the study presents methods aimed at strengthening drone communications against the growing threat of intrusion proposes and tests attacks. It is poised to increase the understanding of network security and increase the resilience of these systems in critical applications.

The project is a hybrid of network scanning and jamming which provides powerful tools that can be used by both a serious network security professional as well as a hobbyist. It can scan the 2.4 GHz signal and show all networks of that range. We can also select a particular channel that we want to interfere with.

II. LITERATURE REVIEW

In this paper [1], the susceptibility of rate adaptation algorithms (RAAs) to pernicious jamming attacks in wireless networks is thoroughly examined. A new measure of speaker vulnerability, the Rate of Jamming (RoJ), is presented. Speakers with low RoJ values are more vulnerable to jamming. The study finds that despite the fact that numerous commonly used RAAs, including such familiar ones as ARF and Sample Rate, are highly vulnerable to jamming--as evidenced by their low RoJ scores--they are still widely used. This vital security issue is the subject of this paper, which presents a novel RAA called Randomized ARF (RARF) designed to improve robustness against jamming attacks. Moreover, a strict theoretical structure is constructed to assess the attack risks systematically. The authors support this theoretical analysis with ns-3 simulations showing empirical data. When faced with jamming attacks, RARF works far better than other RAAs, raising RoJ by 300 % at times.

Wireless networks and mobile devices have been studied [2]. Network security, privacy and regulatory compliance are more important than ever. Among these worries is the exposure of Wi-Fi networks to physical layer attacks like jamming. This paper looks at the threat jamming poses for Wi-Fi, and on sensitive devices. Software-defined radio (SDR) devices, such as the HackRF One, are inexpensive and becoming commonplace. By way of experiments or even malicious intent, it is possible to test for these vulnerabilities. The study, which stresses in-depth experiments and research into Wi-Fi network performance, conducts a series of tests using an off-the-shelf SDR, HackRF, and a directional antenna. These results show that even if the channels are partially jammed by a Wi-Fi jamming device, upload and download speeds obviously suffer, particularly when the jamming position is near to the target device. These security considerations are also critical in healthcare and defense domains, the research points out, and it calls for further work

on router configurations, Wi-Fi standards, and jamming mitigation strategies.

This paper considers the crucial problem of jamming attacks in wireless sensor networks[3]. During such attacks, an adversary jams or disrupts the transmission between network nodes, so that performance is reduced to unsatisfactory levels or even completely compromised. To do so, the paper introduces DEEJAM, a new MAC-layer protocol designed to defeat covert jammers. To hide communications, and thwart jamming attempts as well as mute the results of such attacks, DEEJAM uses four different mechanisms. The contributions of the paper are to define classes of jamming attack, suggest complementary solutions and provide real-world implementation and evaluation results. It points out the relevance of improving in these areas when it comes to security problems in fields such as healthcare and defense, and how further study on router settings, Wi-Fi standards, and smart use jamming countermeasures is needed.

In this project [4] they develop an inexpensive, easily carriable jammer detector to deal with the growing dissatisfaction related to Radio Frequency Interference (RFI). RFI sources either intended or unintended cause interference to key communications used by first responders and public safety agencies. The above-proposed device employs robust algorithms that perform parallel detection of the several main forms of Radio Frequency Interference (RFI). These algorithms use Kurtosis and Fractional Fourier Transform combined with diamond power to effectively improve detection probability. Revolutionizing emergency rescue The purpose of this innovation is to help telecommunications firms improve the spectrum interference monitoring capability for first responders so that they can better deal with RFI disruptions in their protection areas during disaster relief. Jammer detection and localization is a rich field of research, and there are many different techniques in use as potential solutions. The development of this device is an attempt to make communication systems used by first responders and public safety agencies more resilient and reliable.

This paper [5]examines how successful jamming attacks in wireless networks are; it also puts forward methods to accomplish such an attack with low energy consumption and less chance of being detected. A. Focusing on Denial of Service (DoS) attacks and intelligent wireless jamming, it investigates various performance metrics for jamming. The study also shows how jammers, especially protocol-aware jammers, can temporarily stop control packets and completely shut down net throughput. Compared to the Macaofon jammer this method is both more effective and stealthier. For military applications, this means that interference from jamming nodes can shut down an opponent's networks; and in the civilian context, it may be necessary to disrupt wireless hotspots or other important communications systems. Understanding these vulnerabilities will require better network defense strategies.

This survey focuses on[6]the problems of cyber-attacks in cordless networks, exposing concerns caused by wireless channels including their openness and interoperability. From a satellite or WLAN network to cellular and many more, this book takes readers on an in-depth exploration of jamming attacks and non-jamming plans. This article offers readers a well-rounded idea of these techniques and emphasizes that other research still needs to be done so as to defend the wireless networks. The research attaches importance to the need to address these security concerns in arenas such as health care and defense.

In this paper [7] a novel approach is suggested an effective protocol-aware jamming system for Unmanned aerial vehicle remote control. The system is implemented using a software-defined radio platform, aiming to curb the unauthorized usage of unmanned aerial vehicles (UAVs) in sensitive areas. The experimental results demonstrate that this jamming system efficiently neutralizes UAV remote control systems, requiring relatively low jam-to-signal ratios and impacting other communication systems less compared to traditional sweep jammers. The flexibility and adaptability of this approach make it a promising solution for UAV security challenges, particularly when dealing with proprietary communication protocols and various RF parameters.

This paper presents [8] a study on the impact and feasibility of various jamming techniques against wireless networks. The authors analyze the bit error rate of systems under attack using different jamming waveforms. MATLAB simulations validate the analytical findings. The study introduces "JamRF," a jamming toolkit that utilizes the HackRF software-defined radio (SDR) for real-world implementations. The results demonstrate that protocol-aware jamming can significantly impact IEEE 802.11n networks while remaining flexible and low-cost.

This paper [9] introduces "JamSense," an extension of "SpeckSense," designed to detect and classify jamming attacks in low-power wireless networks while applying them to resource-constrained IoT devices. They use RSSI (Received Signal Strength Indicator) sampling to identify jamming through a combination of clustering techniques and temporal properties. They carried out a number of experiments to show that JamSense actually can discriminate between genuine jamming attacks and Bluetooth or Wi-Fi interference that gets misclassified as jamming. In terms of the IOT era, this work has value for improving the security of low-power wireless networks.

They have recently developed an anti-drone system [10] employing a Three Dimensional Frequency Modulated Continuous Wave Multiple Input Multiple Output radar and a directional jammer operating at 2.4 GHz. It scans a given area with the radar and uses an algorithm to track drones. The system is designed to detect and jam small drones. Note: Toward a possible threat the directional jammer is steered to point in that direction, disrupting the drone's communication link. This system is an effective way to protect against drones that have already been introduced into the marketplace, by using Wi-Fi frequencies or GPS for transmission of control instructions and payload. Its practical applications and field demonstration are considered.

This paper introduces [11] a wireless-powered friendly jammer for secure communication in the presence of an eavesdropper. The proposed protocol involves wireless power transfer from the source to the jammer in the first phase, and in the second phase, the source transmits the information signal protected by a jamming signal generated by the jammer using the harvested energy. The study analyzes the long-term behavior and derives the throughput of this protocol while optimizing rate parameters to maximize

throughput under secrecy constraints. The authors highlight the significant difference in throughput performance between single-antenna and multi-antenna jammers. This work has implications for enhancing the security of wireless communication systems.

In wireless sensor networks, a low-cost solution for jammers is proposed in paper [12], which makes use of batteryless Radio-Frequency Identification tags (RFID). The proposed design then makes use of the energy harvested from the jammer's signal to carry out efficient and economical jammer localization. Using extensive simulations to show its effectiveness, the paper provides hope for this approach in jamming attack countermeasures of crucial infrastructures. Furthermore, the work examines whether such a system can be put into practice with commercially available equipment. It is noted that this power-efficient system requires almost no electricity consumption.

A new navigation system that questions the effectiveness of jamming as an anti-drone technique is introduced by this study [13]. It is called JAM-ME. The Wireless Sensor Network (WSN) system provided by JAM-ME allows drones to use adversarial jamming signals and establish an emergency navigation system. Even in areas crowded with people this WSN is able to behave and exist like a normal WSN. The paper points out the limits of jamming and shows JAM-ME 's effects by simulation calculations. It also provides a novel approach to drone security and navigation, as it covers possible measures of abatement and future research directions.

This paper examines [14] the security problems associated with wireless mesh networks when they are used in swarms of Unmanned Aerial Vehicles. The study pinpoints security holes in today's cutting-edge mesh protocols. addressed against UAV swarm contexts, covering threats as well. It presents a security-oriented architecture for Unmanned Aerial Vehicle (UAV) mesh communications, as well as discusses research prospects in this budding area. Moreover, this work offers an initial insight into the security problems inherent in UAV swarm communication and provides a platform for further research in this area.

Herein [15] proposed a new method of detecting and measuring chirps' signals-especially for use in their reception in electronic warfare (EW) receivers. The method uses a frame-based fast Fourier transform. This method differs from the traditional approaches, which are based on threshold-detection methods. The detection threshold of this method is independent of signal power and increased sensitivity is achieved with multiple frames FFT. Simulations and experimental data are presented which demonstrate the effectiveness of the proposed method, showing clearly that its chirp rate estimate is more accurate than those obtained by traditional magnitude-based techniques. This novel way of thinking holds promise for real-time EW operations.

III. METHODOLOGY

A. OVERVIEW OF UAV AND DRONE INTERCOMMUNICATION

The communication infrastructure between drones occupies a central place in the dynamic world of unmanned aerial vehicle (UAV) systems, and it plays an indispensable role in joint missions and smooth coordination. The whole exploration is centered on reviewing the intricacies of inter-drone communication, particularly focusing upon the 2.4 GHz frequency band, which is a widely used spectrum for UAV communications. However, though the 2.4 GHz frequency is optimal for fast transmission of data, it's not invulnerable to attack. Since this frequency band is so universally used in drone communications, the fact that it's highly subject to interference and creates possible security threats is an area worth looking at more deeply. The vulnerability analysis focuses on a wide range of risk areas including signal jamming and eavesdropping as well as unauthorized access, pointing out the security problems involved with 2.4 GHz inter-drone communications. To make this finding more comprehensible, we also include various visual representations, such as figures and graphs. These not only tell people what the experimental setups were like, but they can also show them very clearly just what the results of each experiment looked like. The goal with this research is to provide a thoughtful understanding of the particular problems faced by UAVs intended to fly in the 2.4 GHz spectrum, and perhaps these results will help improve secure and robust inter-drone communication protocols. Moreover, this incorporation of visual elements helps make this methods and results more transparent. This, in turn, gives us a full picture of the intricacies of priming UAV communications for emergency response in this key frequency band.

B. ALGORITHM

The algorithm for Scanning and Jamming the 2.4 GHz Signal Frequency.

```
1. **Initialization:**
   a. Include necessary libraries: SPI, Wire, Adafruit_GFX,
      Adafruit_SSD1306, RF24, nRF24L01.
   b. Define constants: CE_PIN, CHANNELS, radio, display,
      and other relevant parameters.

2. **Setup Function:**
   a. Begin serial communication.
   b. Initialize OLED display.
   c. Configure and start RF24 radio in listening mode.
   d. Set up SPI communication.
   e. Set initial NRF24L01 configurations (e.g., EN_AA, RF_SETUP).

3. **Helper Functions:**
   a. `getRegister(byte r)`: Read register value from NRF24L01 module.
   b. `setRegister(byte r, byte v)`: Set register value on NRF24L01 module.
   c. `powerUp()`: Power up NRF24L01 module.
   d. `powerDown()`: Power down NRF24L01 module.
   e. `enable()`: Enable module.
   f. `disable()`: Disable module.
   g. `setRX()`: Configure module for receiving.
   h. `scanChannels()`: Scan signal strength on all channels.
   i. `outputChannels()`: Display signal strength on OLED display.
   j. `printChannels()`: Print channel layout to the serial monitor.
   k. `jammer()`: Transmit noise to interfere with communication on
                  a specific channel.

4. **Main Loop:**
   a. Clear OLED display.
   b. Check for serial commands (toggle jamming, change channel).
   c. If jamming is enabled:
      i. Display jamming information on OLED.
      ii. Configure RF24 for jamming parameters.
      iii. Transmit noise on the current channel for a specified
           duration.
      iv. Turn off jamming after the specified duration.
   d. Scan channels and output signal strength.
   e. Periodically print the channel layout.

5. **End Algorithm.**
```

IV. IMPLEMENTATION

A. Hardware Components

The following hardware components were used for THIS research work.

Arduino Nano: For the control unit in this project, a microcontroller called the Arduino Nano is employed for control purposes and to carry out the required processing operations.

NRF24L01 Module: The NRF24L01 module is a transceiver operating at the frequency of 2.4 GHz, and thus makes it possible to transmit and receive information. It is used to detect and disrupt wireless connections within the scope of this work.

OLED 0.96 Display: Network scanning results, including jamming, are displayed on the OLED 0.96 screen clearly and understandable graphs of the network data.

B. Library Installation

To streamline Arduino IDE development, install the Adafruit SSD1306 Library for OLED display communication and the GFX Library for graphics functions. The former facilitates seamless interaction with the display, while the latter provides essential tools for creating and manipulating graphical displays, enhancing the project's visual appeal and user interface. Integrating these libraries is crucial for efficient and successful project development.

C. Steps Required for Implementation

1. Setup of Hardware Components:

The Components pin and connection details are given Table 1 below.

Table 1. Components Pins and Connection Details

ARDUINO NANO	NRF24L01	OLED 0.96
9	CE	-
13	SCK	-
12	MISO	-
10	CSN	-
11	MOSI	-
3v3	VCC	-
GND	GND	GND
A4	-	SDA
A5	-	SCK
VIN	-	VDD

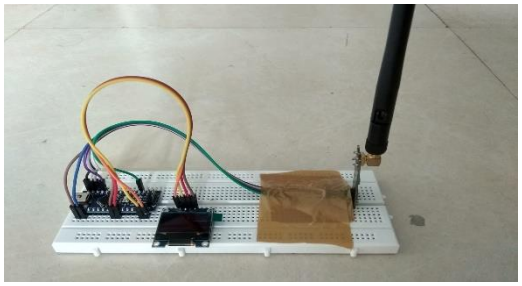

Fig.1 Hardware connections made.

2. Software Implementation:

In terms of software implementation, the Arduino needs to be coded as follows for the NRF24L01 module to perform spectrum scanning. This is comprehensive, including capturing and interpreting data from the module in terms of both Wi-Fi activities and non-Wi-Fi activities. Adafruit's SSD1306 and GFX libraries are also used to display this data graphically on the OLED 0.96 display to raise user attention. With this thorough approach, the module is properly utilized and The captured RF information turns up in text on the connected OLED screen.

3. Data Presentation:

Here in the Data Presentation, we Display Wi-Fi and non-Wi-Fi activity on the OLED screen, using graphs that represent power consumption based on input data.

The Arduino serial plotter shows a clear picture of what is happening in the frequency and signal strength as shown in *Fig. 2*

The first yellow line on the x-axis is a clear indication of a significant shift in the corresponding parameter at that specific point. This could be attributed to several factors, such as a change in signal strength, noise levels, or any other monitored parameter within your code. On the other hand, the second red line remains consistent throughout, signaling a stable or unchanging parameter. This may represent a threshold or a constant value within your system. As for the third green and fourth blue lines, they display noticeable fluctuations, indicating a continuous variance in these parameters over time. These lines could potentially represent dynamic data, such as signal strength or noise levels, within your network scanner and jammer. It's worth noting that the x-axis of the graph represents time or sample counts.

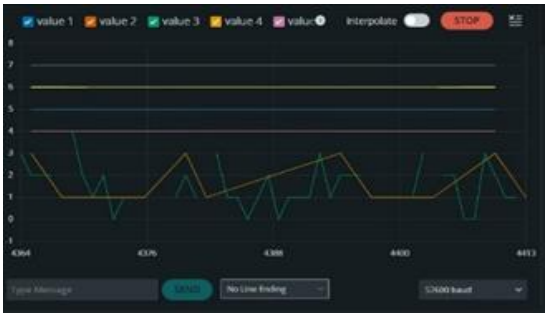

Fig. 2 Arduino Serial Plotter showing Network Data.

4. Testing and Calibration:

To determine whether the Wi-Fi Network Jammer works or not, extensive testing in a variety of environments is done, to ensure that scans are as accurate as possible and display activity as correctly as possible. By carrying out calibrating steps, the device's ability to distinguish and discriminate among different types of signals with high accuracy is strengthened. Testing and calibration: The testing of the Wi-Fi Network Jammer takes place in a variety of application scenarios, ultimately aiming to

bring its reliability and effectiveness up to nearly 100 %, so it can perform at peak levels when being used.

VI. RESULT AND DISCUSSION

The results obtained from this Wi-Fi jamming experiment using Arduino Nano, nRF24L01, and a 0.96 OLED display as in *Fig.4* revealed a substantial impact on network performance. Before the jamming attack, Ookla Speedtest in Fig 3 shows the recorded download speed of 13.16 Mbps and an upload speed of 5.56 Mbps and channel 8 frequency went to the height of 63(maximum signal strength) However, during the jamming attack, these metrics dropped significantly to 1.25 Mbps for download and 2.26 Mbps for upload as shown in *Fig.6* and channel 8 frequency dropped to 40(maximum signal strength) as shown in Fig.6 besides that multiple testing on different other platforms has been done to test the Wi-Fi speed before and during Jamming we got similar kind of expected output. This marked reduction in network performance underscores the effectiveness of the implemented Wi-Fi jammer in deliberately disrupting normal communication.

Fig 3. Before Jamming

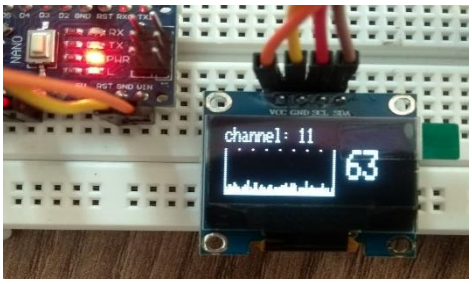

Fig. 4 Wi-fi speed test on Ookla speed test and Wi-Fi Network Frequency on channel 11 before Jamming.

Fig. 5 During Jamming.

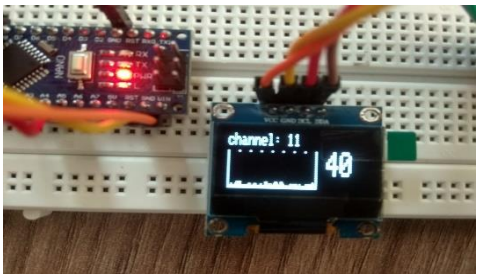

Fig. 6: Wi-fi speed test on Ookla speed test and Wi-Fi Network Frequency on channel 11 During Jamming.

Table 2. Different Networks Download and Upload Testing and Results on Different Timings Details

	Before Jamming				During Jamming			
Sno	**Date/ Time**	**Download (Mbps)**	**Upload (Mbps)**	**Service Provider**	**Date/ Time**	**Download (Mbps)**	**Upload (Mbps)**	**Service Provider**
1	21-12-2023 (9:06 AM)	13.16	5.56	Tata Teleservices	21-12-2023 (9:04 AM)	1.25	2.26	Tata Teleservices
2	21-12-2023 (10:29 AM)	11	14	Airtel Mobile	21-12-2023 (10:32 AM)	6.4	13	Airtel Mobile
3	22-12-2023 (11:05 AM)	12	13	Airtel Mobile	22-12-2023 (11:08 AM)	5.25	10	Airtel Mobile
4	22-12-2023 (11:30 AM)	8.2	7.25	Tata Teleservices	22-12-2023 (11:33 AM)	3.2	2.35	Tata Teleservices
5	22-12-2023 (11:40 AM)	9.6	5.5	Tata Teleservices	22-12-2023 (11:33 AM)	2.95	1.96	Tata Teleservices

.

Table.2 showcases the results of testing on the jamming capabilities of different service providers. Our analysis reveals notable differences between the conditions pre-jamming and during jamming.

Table 3. Power and Current consumption of Wi-Fi Jammer

COMPONENT	MAX POWER CONSUMED	MAX CURRENT CONSUMED
NANO	12V	19 mA
NRF24L01	3.6V	12.3 mA
OLED 0.96	5V	60 mA

For any electrical device, Power and Current Consumption cause a difference in efficiency and performance, *Table.3* clearly showcases the max power and corresponding max current consumed by this device.

Table 4. Comparison table between the Commercial and this Jammer with specifications.

SPECS	THIS JAMMER	CT-3024N WIFI 2.4Ghz 20W	CT-3024525
Max range	1100 m	1500	1200m
Power consumption	20.6v	20W	20W
Portability	No	Yes	No
Price	$ 15.54	$ 550	$ 2,800

Table.4 shows the comparison between the commercial and our Jammer with different specifications such as Max range, Power Consumption, Portability and Price of each of them. With this comparison, we can understand that these types of frugal jammers are way cheaper to its counterparts and at the same time power efficient.

V. CONCLUSION AND FUTURE ENHANCEMENTS

In conclusion, this study has provided a comprehensive analysis of vulnerabilities within the 2.4 GHz frequency band, focusing on the increasingly pertinent threat of jamming attacks in the context of inter-drone communication. By scrutinizing communication protocols, modulation techniques, and data transfer mechanisms, we have identified critical vulnerabilities that may compromise the reliability and security of UAV communications. Experimental simulations further underscored the tangible impact of jamming on communication parameters, shedding light on potential risks in real-world scenarios. The proposed mitigation strategies have been examined for their efficacy in fortifying UAV communication against jamming problems. This research contributes substantively to the ongoing discourse on securing UAV communication systems, offering insights that are crucial for the development of resilient and secure UAV networks. As UAVs continue to play a pivotal role in critical applications, it becomes imperative to proactively address and mitigate vulnerabilities, ensuring the sustained integrity and effectiveness of inter-drone communication systems. This study serves as a foundation for future research endeavors, guiding the implementation of robust security measures to safeguard UAV communications within the 2.4 GHz frequency band.

In the next releases, the main focus will be to enhance security features and prevent any unauthorized use of jamming activities. We are committed to implementing authentication programs and strengthening security measures. With our update capabilities, users will have access to real-time updates of signal strength and potential disturbances through a monitoring system. Not only that, but the advanced OLED display will provide live graphs and signal waveforms, allowing users to better understand their wireless environment. In addition, we prioritize range expansion and optimization of power consumption and the transition from 2.4 GHz to 5 GHz by examining external sources. These developments will undoubtedly be highlights of the efforts.

VIII. REFERENCES

[1] Orakcal, Cankut, and David Starobinski. "Jamming-resistant rate adaptation in Wi-Fi networks." *Performance Evaluation* 75 (2014): 5068.

[2] Sârbu, Annamaria, and Dumitru Neagoie. "Wi-Fi jamming using software-defined radio." *International Conference Knowledge-Based Organization*. Vol. 26. No. 3. 2020.

[3] Wood, Anthony D., John A. Stankovic, and Gang Zhou. "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks." *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2007.

[4] Jagannath, Anu, et al. "Developing a low cost, portable jammer detection and localization device for first responders." *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019.

[5] Thuente, David, and Mithun Acharya. "Intelligent jamming in wireless networks with applications to 802.11 b and other networks." *Proc. of MILCOM*. Vol. 6. 2006.

[6] Hussain, Ahmed, et al. "Energy-Harvesting Based Jammer Localization: A Battery-Free Approach in Wireless Sensor Networks." *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022.

[7] Pirayesh, Hossein, and Huacheng Zeng. "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey." *IEEE communications surveys & tutorials* 24.2 (2022): 767-809.

[8] Pärlin, Karel, Muhammad Mahtab Alam, and Yannick Le Moullec. "Jamming of UAV remote control systems using software-defined radio." *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018.

[9] Ali, Abubakar S., et al. "JamRF: Performance Analysis, Evaluation, and Implementation of RF Jamming Over Wi-Fi." *IEEE Access* 10 (2022): 133370-133384.

[10] Kanwar, John, et al. "Jamsense: Interference and jamming classification for low-power wireless networks." *2021 13th IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE, 2021.

[11] Multerer, Thomas, et al. "Low-cost jamming system against small drones using a 3D MIMO radar based tracking." *2017 European Radar Conference (EURAD)*. IEEE, 2017.

[12] Liu, Wanchun, et al. "Secure communication with a wireless-powered friendly jammer." *IEEE*

Transactions on Wireless Communications 15.1 (2015): 401-415.

[13] Di Pietro, Roberto, Gabriele Oligeri, and Pietro Tedeschi. "JAM-ME: exploiting jamming to accomplish drone mission." *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019.

[14] Lopez, Martin Andreoni, et al. "Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities." *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2021.

[15] Cheng, CHI-HAO, et al. "Chirp signal detection using FFT peak frequency difference [Correspondence]." *IEEE Transactions on Aerospace and Electronic Systems* 52.3 (2016): 1449-1453.

[16] B. Sukanya and V. Palliyembil, "Performance Improvement of Indoor Lifi Mobile Users with Random Orientation Using Hybrid Lifi and Wifi Networks (HLWNets)," 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2021, pp. 390-394, doi: 10.1109/WiSPNET51692.2021.9419442.

[17] Sunil, S., Mukhopadhyay, A., Gujjar, C. Multi-group Message Communication on Android Smartphones via WiFi Direct, (2017) 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, 2017-January, pp. 1994-1999, 2017

[18] Bhat, S., Mukhopadhyay, A., Sandhya Rani, B.K., Dynamic Media Selection between WiFi and LTE in Telemedicine Scenarios, (2017) 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, 2017-January, pp. 601-606, 2017

[19] Dr. Thangam S. and Dr. E. Kirubhakaran, “Analysis of various service discovery protocols for infra structureless networks”, International Journal of Computer Applications, vol. 12, 2010.