University Journal of Research: Computer Science and Applications

Rogue Access Point: The Jamming Tool for FHSS

Raval Vidhan Yagneshkumar[a], Dr. Kashyap C. Patel[b], Dr. Sachinkumar Anandpal Goswami[c], Dr. Shital Bhagubhai Patel[d], and Sonal J. Patel[e]

[a]Student, Faculty of Computer Applications, Ganpat University, Gujarat, India

[b]Assistant Professor, Faculty of Computer applications, Ganpat University, Gujarat, India

[c]Assistant Professor, Faculty of Computer applications, Ganpat University, Gujarat, India

[d]Assistant Professor, Faculty of Computer applications, Ganpat University, Gujarat, India

[e]Assistant Professor, Faculty of Computer applications, Ganpat University, Gujarat, India

Corresponding Author Email: vidhanraval984@gmail.com

Abstract

The advantage of Frequency Hopping Spread Spectrum (FHSS) over interference and unauthorized access in the continuously changing wireless scenario makes it stand out. Yet, despite all these advantages, Rogue Access Points (Rogue AP) provide great vulnerabilities with the increasing application environment based on FHSS technology. In this paper, we explore the duality of rogue APs as a security threat and a jamming tool that effectively hampers the operations of FHSS. We begin by introducing jamming techniques-continuous wave jamming, pulse jamming, and selective jamming, which can breach integrity in wireless communications. Then we talk about Rogue AP architecture and the operational mechanisms through which they can mimic legitimate networks to lure unaware victims and carry out a jamming attack. A comparison analysis describes the performance of FHSS networks at two points before and after the Rogue AP-based attacks. With observed data and simulation results, we discuss the extent to which Rogue APs interfere with the performance of FHSS networks further analyzing degradations in data throughput, latency, and the possibility of losing connectivity. Finally, we discuss future improvements focused on mitigation techniques and the extent of destructiveness that AI describes that should counter Rogue APs. And so, the implications of our results emphasize proactive measures to protect FHSS networks against such Rogue AP based threats and end up with reliable and safe wireless communications.

Keywords: Rogue Access Point, Signal Jamming, Frequency-Hopped Spread Spectrum

1. Introduction

Wireless communication technologies have transformed the way we connect, share information, and conduct business. Among various transmission methods, FHSS [1] [2] [18] [23] has gained prominence due to its inherent advantages in resisting interference and enhancing security. By rapidly switching frequencies during transmission, FHSS minimizes the risk of eavesdropping and provides a reliable means of communication in crowded and noisy environments. However, the increasing sophistication of cyber threats has raised concerns about the vulnerabilities inherent in these systems. One such threat is posed by Rogue Aps [3] [6]-[11], which are unauthorized devices that can impersonate legitimate network access points. These Rogue APs can exploit weaknesses in wireless protocols, particularly in FHSS environments, to conduct various attacks, including jamming [1]-[5] [19]-[22] [24]-[27]. Jamming refers to the deliberate disruption of communication signals, rendering wireless networks ineffective. Understanding the various jamming techniques—such as broadband jamming, partial band jamming, pulse jamming and sweep jamming—is crucial in assessing the full scope of the threat posed by Rogue APs. This research work aims to explore the role of Rogue AP as security threats and jamming tools in FHSS networks. We will examine how this malicious tool operates and the specific jamming techniques they employ to disrupt communication. Additionally, we will compare the performance of FHSS [18] [23] networks before and after Rogue AP-based attacks, highlighting the impact on network reliability and user experience. Finally, we will discuss potential future enhancements in security protocols and detection methods that could mitigate the risks associated with Rogue APs. Through this comprehensive examination, we seek to contribute to the ongoing discourse on wireless security and provide insights into the vulnerabilities that Rogue AP introduce into FHSS networks, ultimately advocating for proactive measures to safeguard against these emerging threats. [1]-[5] [19]-[22] [24]-[27]

2. Jamming Techniques: Broadband Jamming, Partial Band Jamming, Pulse Jamming, Sweep Jamming

Jamming attacks on FH radios are one of the paramount problems in wireless communication systems. FH is taken as the countermeasure against jamming attacks, where the transmitter rapidly switches between many frequency channels based on a pseudo random sequence known as a hopset. [1]-[5] [12] [13] [26] [27]

2.1 Effects of Jamming Radio

Jamming attacks on Frequency Hopping (FH) radios [18] can be highly destructive to communication. The following section considers some impacts caused by jamming on FH radios based on three fundamental parameters: SNR reduction, BER increase, and range of communication diminution. [1]-[5] [12] [13] [26] – [28]

- **Reduction in Signal-to-Noise Ratio (SNR)**

  SNR is the abbreviation of signal-to-noise ratio, which is an important measure of the quality of the communication signal. It is indicative of the ratio of desired signal power to background noise power. In FH radios, the injection of intentional noise through jamming lowers the SNR. Some of the implications arising out of a reduced SNR are:

  Bad SNR: The receiver will often fail to distinguish between the desired signal and the noise due to the jamming. Detection thus can be partially or completely unsuccessful. [13]

  Increased Processing Complexity: In order to improve the poor SNR, receivers may turn towards even more complex signal processing techniques, for example, more complex filtering algorithms or signal enhancements. Such sophisticated processing increases processing delay and resource utilization. [13]

  Robustness Impact: FHSS is designed to be jam resistant but can be jammed by intense jamming. As SNR decreases frequency hopping can lose a lot of its effectiveness in beating jamming. [13]

- **Rising Bit Error Rate (BER)**

  The BER is measured as the percentage of incorrect bits arriving at the receiver, relative to the total number of bits sent. Reasons for BER to be high due to jamming attacks are given below:

  Interference with data integrity: Since the jamming noise would interfere with the transmitted signals, chances of errors in bits rise. At the receiver end, data might be wrongly understood, and thus, corruption in the decoded information may occur. [13]

  Increased Retransmissions: More BER increases data packets retransmission to ensure proper reception of information. This severely worsens network congestions and reduces the throughputs within the networks; hence, more time and added efforts are taken in correcting errors. [13]

Thresholds for Error Correction: All communications systems use error correction codes to reduce the BER. However, when jamming is high, even the most sophisticated error correction cannot recover the data, thereby completely losing critical information. [13]

- Reduced Communication Range

Jamming may seriously degrade the effective range of FH radios. This degradation can be in the following ways:

Signal Attenuation: As a jamming signal travels, it causes attenuation to the intended signals. This results in a less effective range, so making it hard to set up, or even establish/maintain, connections especially in areas where one has to communicate long distances. [13]

Interconnection Rate: Jamming noises always find a way into the communication system and may cause frequent disconnections since a device can't easily communicate. This is a major problem in applications such as remote monitoring or control systems where connectivity should be quite constant. [13]

Operational Limitations: For mobile applications, reduced communication range becomes a limitation to the operational capability of devices. In critical situations such as emergency response or military operations while being used, it severely restricts the ability of the devices to ensure an uninterrupted connection. [13]

So, jamming attacks on FH radios provide significant and multifaceted impacts on the performance of communication. Diminishing SNR, BER's rise, and effective communication distance decline are aspects of SNR degradation and BER increase that undermine the reliability and integrity of wireless communications. Therefore, understanding these impacts is very important for developing better ways of countering FH radio systems against jamming attacks and maintaining their effective performance in different applications. Robust security protocols and enhanced mechanisms of detection would be crucial in mitigating the risks associated with jamming attacks in FHSS environments. [1]-[5] [12] [13] [26] – [28]

2.2 Analysis of Jamming Techniques

- **Broadband Jamming:**

The second type is called broadband jamming, which is a transmission of noise at a broad range of frequencies simultaneously. This is used to interfere with the communication taking place within the wide band of frequencies in use, thereby blocking several channels at once. A broadband jammer transmits a continuous wave of noise or signals across a very wide frequency band. It can be achieved through a noise generator that produces a signal which is not intelligible but strong enough to interfere with the legitimate communications. [1]-[5] [12] [13] [26] – [28]

Example: Consider the case of a malicious user activating a broadband jammer to disable a 2.4 GHz Wi-Fi network. The jammer generates noise over the entire 2.4 GHz band, 2.4 to 2.5 GHz, which may forbear connections or prevent users from maintaining a connection to the network. It thus leads to dropped connections, high latency, and an inability to utilize the network in the right way.

Implication: Broadband jamming often causes a strong degradation of communication systems but is less targeted and impacts all devices in its range, thus causing collateral damage within the multi-channel environment.

- **Partial Band Jamming:**

  Partial band jamming takes out specific portions of the frequency spectrum rather than the entire range. This method jams some frequencies while leaving others functional. In a partial band jammer, the jamming target is to select one or more specified channels in the frequency band. Noise is transmitted on such selected frequencies, but the adjacent channels remain unjammed. [1]-[5] [12] [13] [26] – [28]

  Example:

  In FHSS military communications, a partial-band jammer could jam a certain set of hopping frequencies critical to communication but leave others open. Assuming the system hops between frequencies 1.0 GHz, 1.2 GHz, and 1.4 GHz, the jammer could target 1.2 GHz, thus selectively inhibiting the communication without full crippling the system.

  Implications:

  Partial band jamming is definitely less interfering than broadband jamming, yet it still holds the capability to cripple communication, whereby it can exploit certain frequency vulnerabilities; therefore, it becomes a strategic and purposeful kind of attack.

- **Partial Band Jamming:**

  Pulse jamming is another form of jamming, wherein pulses of jamming signals are transmitted at regular intervals. Such interference can interfere with legitimate signals because this causes bursty injection of noise at intervals that match the times when data would normally be transmitted. [1]-[5] [12] [13] [26] – [28]

The jammer emits high-power pulses that over saturate the communication channel over the short period during which legal signals are transmitted. The period of these pulses can next be optimized to produce maximum interference.

Example:

Let's say a sensor network sends out one packet per second. A pulsed jammer, in that case, can synchronize in transmitting jamming pulses at the time when the network is sending out a packet. Let's say the network is sending a packet at 10 seconds; it can send out a pulse at 10 seconds, thus 'blinding' the legitimate receiver and thus losing the packet.

Impacts:

Pulse jamming is highly effective against time-sensitive communications because of its nature that does not involve continuously blocking the whole frequency band but is designed to interfere only with certain transmissions. It may cause increased error rates and retransmissions, thus degrading the performance of the communication system.

- **Sweep Jamming:**

  Sweep jamming takes place when the jammer, in an orderly manner, broadcasts noise throughout a given frequency band sweeping across. As it moves its signal down the spectrum, the jammer impairs communication. A sweep jammer, however, continuously changes its jamming frequency so that it sweeps through all the available spectrum and sparsely jams as it passes through each frequency. This would spread over a wide range of frequencies within time. [1]-[5] [12] [13] [26] – [28]

  Example:

  Suppose an attacker wants to jam a frequency-hopping system that changes frequency every few seconds. The jammer may work by scanning the frequencies in use and briefly jam each one as it moves to the next one. For example, if the system frequency-hopped between 900 MHz, 910 MHz, and 920 MHz, the jammer may sweep across those frequencies once per second, briefly breaking communications on each of those channels.

  Implications:

Sweep jamming is highly effective against frequency-hopping systems because it could potentially jam each of the frequencies that the system might need. It, however, is very sensitive to timing considerations and requires a powerful transmitter capable of reaching the desired distance.

Understanding such jamming techniques will help in the implementation of operational countermeasures against these jamming techniques in a wireless communication system. Each method has its own operational characteristic, strengths, and weaknesses; their impact varies widely with specific communication environments and protocols in use. Organizational comprehensive understanding of all types of jamming techniques would better prepare their systems against the attacks and ultimately enhance security in wireless communications. [1]-[5] [12] [13] [26] – [28]

3. Rogue Access Point: A Jamming Tool

Rogue APs have presented significant challenges to the network landscape integrity and security in wireless communications. Rogue APs are unauthorized devices that mimic legitimate access points, thereby being used maliciously in intercepting data or manipulating traffic and causing communications disruptions. One of the most insidious applications of Rogue APs is their employment as jamming devices, especially as part of the FHSS scheme. This section will thus describe how Rogue APs are capable of being a good jamming tool, how it is done, and what implications it has for the FHSS networks.

3.1 Setting up Rogue AP lab

To set up a Rogue AP lab, we will have certain hardware and software requirements. A laptop or PC with a Kali Linux operating system, a wireless network adapter that supports both monitor mode and packet injection-prone modes (something like an Alfa card), and several Access Points or wireless routers to represent both legitimate and rogue networks are necessary. This includes Rogue AP software packages like Hostapd, dnsmasq for DHCP services, and Wireshark for traffic analysis. [6]-[11]

The deauthentication attacks will require the Aircrack-ng suite. Wifiphisher or Fluxion, if a phishing simulation is to be performed, may be included as well. [6]-[11]

With these tools in place, set up the Rogue AP. First, stop NetworkManager to prevent interference by the network interface with the wireless interface. [6]-[11]

Next, create the hostapd configuration file where user will specify the SSID, perhaps "RogueNetwork," and setup security settings including WPA2, for example. [6]-[11]

Next, set up dnsmasq to supply the DHCP server, an IP range (such as 192.168.150.x), gateway, and DNS. Make sure IP forwarding is on and NAT set to allow the rogue AP to give the Internet to the client. [6]-[11]

Now, configure this Rogue AP. Now having configured, start the hostapd to begin broadcasting the rogue SSID. Begin dnsmasq to hand over IP addresses for all the clients that connect to the network. This should now be fully functional rogue AP. From here, you may use Wireshark to monitor and then analyze the traffic coming out from your own rogue AP clients. [6]-[11]

A rogue AP could be a critical element in the jamming of FHSS by acting as an attacking base to launch deauthentication or jamming attacks. While the FHSS systems are resistant by nature to simple interference due to constant frequency hopping, a rogue AP can be used in a strategic sense to disrupt communication, force clients to disconnect or possibly use as a pivot point for more sophisticated attacks like man-in-the-middle (MITM) or denial-of-service (DoS) attacks. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]

Below is an explanation of how a rogue AP works and its contribution to jamming an FHSS system, the nature of how the rogue AP interacts with the legitimate network, and the technical details of the FHSS jamming.

- **Pseudocode Algorithm for Rogue AP**

```
Start:
  1. Obtain permission from the IT department and administration.
  2. Set up an isolated network for the lab using VLANs or separate physical networks.
  3. Gather necessary hardware:
     Laptop/PC with Kali Linux.
     Wireless network adapter supporting monitor mode and packet injection.
     Install Hostapd, dnsmasq, Wireshark, and other necessary tools.
  4. Configure Rogue AP:
     Stop conflicting network services.
     Set up Hostapd configuration (SSID, WPA settings).
     Set up dnsmasq configuration (IP range, gateway, DNS).
```

```
        Enable IP forwarding and NAT for internet access.
    5. Launch Rogue AP:
        Start Hostapd to broadcast rogue SSID.
        Start dnsmasq to assign IP addresses.
    6. Perform Deauthentication Attack:
        Scan for the legitimate AP (BSSID, channel).
        Use aireplay-ng to deauthenticate clients from legitimate AP.
        Monitor client connections to the rogue AP using Wireshark.
    7. Optional: Simulate Phishing Attack:
        Launch Wifiphisher or Fluxion to set up a fake captive portal.
        Capture login credentials from connected clients.
    8. Perform FHSS Jamming:
        Set wireless adapter in monitor mode.
        Use mdk3 or aireplay-ng to send deauth packets across multiple frequencies.
        Monitor the impact of jamming on FHSS communications.
End
```

3.2 Rogue AP as an Attack Vector for FHSS Systems

A rogue AP can be an access point set up by an attacker to:

- Mimic the legitimate FHSS network. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]
- Confuse clients by broadcasting a similar SSID. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]
- Force legitimate clients off their original network. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]
- Capture sensitive information such as data packets or credentials when clients unknowingly connect to it. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]

Once the rogue AP is established, it can serve as a platform for launching jamming attacks on FHSS systems by exploiting protocol weaknesses. Below are the methods a rogue AP can use to jam or interfere with FHSS communications.

3.3 Real Time Scenario:

It's a busy coffee shop with many customers connected to the coffee shop's Wi-Fi network. Such a network will employ FHSS. This will help in decreasing interference and hence communication errors. Now, KC is a malicious person who wants to disrupt the network and create mayhem.

Objective for KC: KC intends to jam the Wi-Fi network such that no customer will be able to access the Internet or communicate with other customers. He will do this by creating a Rogue AP that is able to transmit a jamming signal based on the frequency hopping pattern of the legitimate AP.

KC's Equipment: KC has software-defined radio (SDR) equipment and a laptop running a custom-built program that can generate a jamming signal. Additionally, she has a Wi-Fi adapter through which she can sniff the coffee shop's Wi-Fi network in order to ascertain its frequency hopping pattern.

Explanation of Scenario:

- **Sniffing Network:** In the case of sniffing network, KC uses her Wi-Fi adapter to sniff the coffee shop's Wi-Fi network, captures the packets and analyzes the frequency hopping pattern. He reveals the hopset sequence and the frequency range used by the network.
- **Signal Generation through Jamming:** KC uses her laptop and SDR to generate the jamming signal based on the frequency hopping pattern of legal network. He specifies the strength of her jamming signal so that signal strengths of the legitimate get overwhelmed.
- **Rogue AP Configuration:** KC configures her Rogue AP so that it propagates in an identical frequency range where the legal network operates. He guarantees that the signal strength of her Rogue AP is better than that of legitimate and authenticate AP.
- **Signaling of Jamming:** KC begins signaling the jamming signal, with which interference also starts with the legal network. The customers of the network start facing connectivity problems, and the network becomes non-reliable.
- **Network Interference:** As soon as the jamming signal is transmitting, it causes a significant network disruption. Customers would be completely unable to get onto the internet, and the Wi-Fi network of a coffee shop essentially goes dark.

Effects: Customers are getting frustrated and unable to work or access the internet. The reputation of the shop has been damaged; the owner may lose business. Alice's acts of malice have unleashed harm onto the coffee shop and its customers.

Here is the pseudocode algorithm for real time scenario:

```
BEGIN
  // Step 1: Define parameters for the hopset
  SET hopset_length TO 100  // Number of frequency channels
  INITIALIZE hopset_sequence AS an array of random integers from 0 to hopset_length
  // Step 2: Define parameters for the jamming signal
  SET jamming_signal_power TO 100  // Power of the jamming signal
  SET jamming_signal_frequency TO 2.4e9  // Frequency of the jamming signal
  // Step 3: Generate the jamming signal
  INITIALIZE jamming_signal AS an array of zeros with length hopset_length
  FOR i FROM 0 TO hopset_length - 1 DO
    // Create a jamming signal using a sine wave
    jamming_signal[i] = SIN(2 * π * jamming_signal_frequency * i / hopset_length)
  END FOR
  // Step 4: Synchronize the jamming signal with the hopset
  INITIALIZE synchronized_jamming_signal AS an array of zeros with length hopset_length
  FOR i FROM 0 TO hopset_length - 1 DO
    // Map the jamming signal to the hopset sequence
    synchronized_jamming_signal[i] = jamming_signal[hopset_sequence[i]]
  END FOR
  // Step 5: Transmit the synchronized jamming signal
  // Note: Actual transmission would require interaction with hardware (e.g., SDR)
  PRINT "Transmitting synchronized jamming signal: ", synchronized_jamming_signal
END
```

Fig 1. Rogue APs jamming a FHSS network.

The above figure illustrates the real time scenario of compromising FHSS through Rogue AP based jamming.

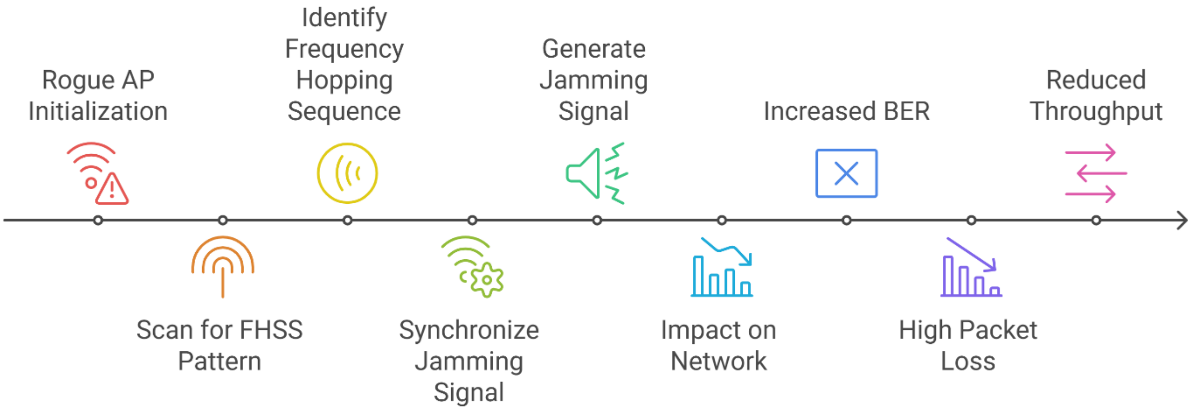

Fig 2. Rogue APs jamming a FHSS network – Step by Step.

The above figure illustrates step by step state of FHSS through Rogue AP based jamming.

Breakdown of this pseudocode algorithm:

Parameter Setup: It first sets the size of hopset and some random sequence, which is going to illustrate the pattern of frequency hopping.

Jamming Signal Setup: It defines power and frequency of jamming signal, which will cause interference against communication.

Generating Jamming Signal: A jamming signal is generated using sine function. This signal simulates the desired jamming frequency over the size of hopset.

Synchronization: The generated jamming signal is synchronized to the hopset sequence, so the jamming occurs at the same frequencies as the legitimate signals.

Transmission: Lastly, the pseudocode reveals that the jamming signal will be transmitted. This is a simplification of the transmission part because it could only be done with real hardware capabilities.

3.4 Deauthentication Attacks

Deauthentication is a very strong attack tool used by a rogue AP to attack the management frames of wireless communication, which are not encrypted in most Wi-Fi systems. Though FHSS can hop from one frequency to another, deauthentication attack works at a protocol level, which does not depend on the value of any specific frequency that may be present at any time. [3] [6]-[11] [14]-[17][19]-[22] [24] [25]

- **Steps of the Attack:**

  Scan for the network: The rogue AP or attacker starts scanning the wireless environment by using a tool called airodump-ng to locate the BSSID, which is just another name for MAC address, of the legitimate FHSS access point and its associated clients. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25]

  Send deauthentication packets: Using the aireplay-ng tool, the rogue AP continuously sends deauth packets to both the client and the legitimate AP. These packets are set up to force the client to disconnect from the network. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25]

  Client disconnection: The legitimate client is forced to roam out and re connect, either to the rogue AP or back to the legal network. But recurring disconnection and reconnection cycles may jeopardize the normal functioning of the FHSS system and could effectively jam it by breaking the communications protocol. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25]

  Transmission at various frequencies and Exploitations: FHSS generates transmission at various frequencies, but an attack through deauthentication exploits the protocol-level management frames that continue to be broadcast irrespective of the frequency hopping. Therefore, even FHSS systems are open to such attacks, and continuous deauth messages effectively jam the client with the legitimate AP. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25]

- **Swept and Broadband Jamming**

A rogue AP could also be used as a basis for launching sweeping or broadband jamming attacks. These can be used to interfere with the entire frequency band used by the FHSS system, thereby degrading its performance or making communication impossible. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25] [28]

Swept Jamming: Rogue AP uses a device connected through it (with a tool like mdk3 or any similar packet injection tool) to send interference signals over multiple frequencies in rapid succession. This is sweeping jamming to break the legitimate FHSS system each time it moves to a jammed frequency. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25] [28]

Implementation: A rogue AP can transmit continuous deauthentication or noise signals over a wide range of frequencies, more likely to interfere with the hopping pattern of the FHSS system.

Broadband Jamming: Instead of trying to hit specific frequencies, broadband jamming transmits high-powered interference across the entire spectrum range used by the FHSS system. The rogue AP can orchestrate this attack using external jamming devices or software tools to flood the spectrum with noise, thereby making it difficult to communicate across any frequency. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25] [28]

Implementation: By employing tools such as mdk3 or aireplay-ng, the Rogue AP can continually jam across multiple frequencies. This will flood out the usable spectrum in the FHSS band. [3] [6]-[11] [14]-[17] [19]-[22] [24] [25] [28]

3.5 Recent FHSS-Specific Anti-Jamming Studies and Real-World Incident Reports

- **Recent FHSS – Specific Anti-Jamming :**

Published in 2024, the paper "Effective Index Modulation Based on FHSS: An Anti-Jamming Viewpoint Unified" presents a simple IM-FHSS (Index Modulation–Frequency Hopping Spread Spectrum) system meant to improve anti-jamming capacity. Especially under demanding jamming conditions, the suggested system uses various sequences and constantly changing frequency hopping patterns together with index modulation to enhance communication performance. The method essentially reduces interference by changing the frequency hopping patterns in real-time, therefore guaranteeing more dependable and safe communication.[28].

Aimed at reducing jamming in complicated situations, the year 2025 paper "Multi-Sequence Frequency-Hopping Communication Framework" offers an intelligent FHSS (Frequency Hopping Spread Spectrum) framework. The suggested method uses numerous frequency sequences and reactive jamming methods to improve communication resistance against several jamming mechanisms. The framework considerably increases the dependability and resilience of communication networks by dynamically changing the frequency sequences in response to interference [29].

- **Real-World Incident Reports**

Rising GPS Jamming Incidents in Norway (2024): Northeastern Norway suffered continuous GPS jamming, therefore compromising aircraft safety. Norwegian authorities raised serious questions regarding aeroplane navigation since they linked these interferences to outside causes [30]. The International Air Transport Association (IATA) reported a 175% increase in aircraft navigation system disruptions in 2024, comprising signal interruptions, jamming, and GPS spoofing events. This concerning tendency emphasises the increasing risk to aircraft safety. One of the first civil aviation accidents connected to such interference, an Azerbaijan Airlines Embraer 190 had a GPS jamming event in December 2024. This event underlines the grave effects on flight safety of GNSS disturbances [31].

For FHSS-based systems, though they recover quickly from momentary interference, continuous broadband or sweeping jamming could adversely affect the network performance in terms of packet loss, increased latency, and possible disconnection of clients. The effectiveness of such action rises if the rogue AP is placed within the proximity area of the FHSS system's clients or legitimate AP, thereby increasing the interference level.

4. Comparison of FHSS : Before and After Rogue AP based Attack

Before a jamming attack, communication quality is smooth, reliable, and interference-resistant. Narrowband jamming causes slight degradation with occasional packet loss, while wideband jamming leads to severe degradation or failure, affecting devices like military radios and smart home systems. [1]-[5] [12] [13] [26] [27]

- Quality of communication is smooth, reliable and interference-resistant prior to jamming attack. After a narrowband jamming attack, slight degradation with few packet losses occurred on the jammed frequencies. In contrast, wideband jamming results in serious degradation or even complete communication failure. This will highly impact devices with military radios and smart home devices. [1]-[5] [12] [13] [26] [27]

- The synchronization between transmitter and receiver is perfect before an attack. After the jamming attack, in a narrowband case, synchronization is mostly maintained except while jamming on the specific frequency. However, while wideband jamming is in full swing, synchronization is lost completely because of interference on all frequencies. The most affected are devices such as tactical radios and walkie-talkies. [1]-[5] [12] [13] [26] [27]
- This is because the frequency hopping, which is the functionality in aiding the evasion of interference, is efficient both before and after narrowband jamming, only with minor disruptions. However, in the case of wideband jamming, multiple frequencies get jammed, hence making frequency hopping ineffective. This affects devices such as drones and wireless sensors. [1]-[5] [12] [13] [26] [27]
- The frequency hopping and error correction mechanisms make it minimal before a jamming attack. After the attack using a narrowband approach, little packet loss occurs on jammed frequencies. On the other hand, wideband jamming causes high packet loss and data corruption with the potential for total communication failure which drastically impacts satellite communication systems. [1]-[5] [13] [26] [27]
- Correcting minor errors and recovery mechanisms handle errors well before an attack. In case of a narrowband attack, with a short jamming burst on certain frequencies, they recover from these errors. However, in wideband attacks, the number of frequencies jammed is so large that it renders these mechanisms ineffective. This applies to industrial IoT devices as much as it does to SCADA systems. [1]-[5] [12] [13] [26] [27]
- Normal power consumption for transmission and reception prevail prior to the jamming attack. In a narrowband attack, power consumption increases by a little, that is, due to some retransmissions. If adaptive power control is in effect in wideband jamming attacks, power consumption will increase significantly, which severely impacts low power consuming devices such as wireless medical devices, pacemakers, and insulin pumps. [1]-[5] [12] [13] [26] [27]
- The net effect of jamming is unbroken, hardy communication before the attack. Subsequent a narrowband attack, there is minor disruption that is mostly recoverable. In wideband jamming, there is a major communication breakdown with unrecoverable

errors severely crippling public safety communications such as police, fire, and EMS radios. [1]- [13] [26] [27]

- **Methodology:** Key performance indicators including Bit Error Rate (BER), Packet Loss Rate, Signal-to-- Noise Ratio (SNR), Latency, and Throughput will be assessed both before and after the jamming attack in order to assess Rogue AP jamming on FHSS networks. Wireshark and iPerf let one record BER and packet loss rate; GnuRadio allows one to compute SNR. Using the ping and iperf programs correspondingly will allow one to assess latency and throughput. Using hostapd and synchronised to the FHSS hopping pattern found via signal analysis with GnuRadio, the Rogue AP will be configured. MDK3 and Scapy will be used to launch jamming attacks sending deauthentication and interference signals. Python allows one to validate the relevance of performance decrease by means of statistical analysis using t-tests and ANOVA. Graphs and tables let one visually see the effects of jamming on FHSS network performance.

Table 1. Before and After Rogue AP Jamming: FHSS Network Performance Measures

Metric	**Before Jamming**	**After Narrowband Jamming**	**After Narrowband Jamming**
BER	Measured log from Wireshark (0.02%)	Increased BER brought on by interference (5%)	Really high BER resulting from extensive covering (25%)
Packet Loss Rate (%)	Calculated using iPerf. (0.1%)	More loss brought on by partial blocking (8%)	Extreme packet loss brought on by complete blocking (45%)
Latency (ms)	Calculated with Ping (20ms)	notable delay resulting from interference (50ms)	Extreme delay brought caused by network congestion (200ms)

Throughput (mbps)	Evaluated with iPerf (50mbps)	Diminished by interference (30 mbps)	Much lowered due to network breakdown (5 mbps)
SNR (dB)	Calculated with GnuRadio (30dB)	Less owing to jamming's noise. (15dB)	severely broken from wideband jamming (5dB)

- **Calculation:**

BER=(Number of incorrect bits / Total Bits Transmitted)×100

Packet Loss Rate = (Lost Packets / Total Packets Sent) ×100

SNR (db) = 10 $log_{\{10\}}$ (Signal Power / Noise Power)

The bit error rate increased from 0.02% to 5% under narrowband jamming and reached 25% under wideband jamming. A paired t-test confirmed the statistical significance of the performance degradation (p-value < 0.001). Latency increased from 20 ms to 200 ms (F-statistic = 25.7, p-value < 0.05), demonstrating the severe impact of jamming on FHSS communication.

5. Quantify the financial or operational consequences of Rogue AP attacks

- **Financial Effect**

Depending on the size and sector of the company, network downtime can be expensive—estimates range from $100,000 to over $540,000 per hour [34].

Penalties for data breaches—that is, violations of data protection laws including the General Data Protection Regulation (GDPR)—may be rather hefty. Penalties for egregious violations can be up to €20 million or 4% of the company's whole worldwide annual turnover, whichever is larger [35].

- **Operational Effect**

Military Systems: Rogue AP strikes may cause communication breakdown in tactical systems, therefore endangering national security and mission success.[6]-[11] Healthcare: Network vulnerabilities allow interference with linked medical equipment including infusion pumps, therefore compromising patient safety.[6]-[11]

IoT Systems: Rogue AP assaults might interfere with linked devices in smart homes, therefore compromising control and maybe resulting in security breaches. Calculating these operational and financial effects emphasises the great requirement of strong network security to guard against Rogue AP assaults.[6]-[11][32][33]

6. Future Enhancement

Some possible future improvements of this research could concentrate on these points to provide better understanding and mitigation against the Rogue AP threat in FHSS systems. In addition to better rogue AP detection, mitigation enhances accuracy through real-time machine learning, and hybrid detection systems will further increase precision. Dynamic frequency-hopping algorithms can jam rogue APs as with self-healing networks such that devices can share intelligence for collaborative defense. Identifying vulnerabilities and testing countermeasures in simulating advanced rogue AP tactics and jamming scenarios is also considered. FHSS control signals and hop patterns may be protected by building a strengthening security approach of encryption, multi-level authentication and obfuscation. Research should be conducted to find AI-driven defenses and quantum-resistant protocols for greater resilience also in terms of measuring impacts of rogue AP on 5G and IoT networks. Contact with regulators regarding standardization of such countermeasures while working towards proper legal frameworks of monitoring and response will contribute to the shape protection to be taken from rogue AP threats.

7. Conclusion

In conclusion, Rogue AP pose a serious security threat to FHSS, exploiting vulnerabilities on several grounds using jamming techniques. This attack degrades the network's performance through sending signals at low quality and increases the bit error rate and disrupts the range of communication. Through this attack, its operation is degraded though FHSS is designed to resist interference. Such risks can be combated by improved detection systems, encryption, and AI-based defenses. Advanced security protocols and adaptive frequency-hopping techniques may provide further support against Rogue APs in the future.

8. References

[1] Lakshminarayana, S., Karachiwala, J. S., Chang, S. Y., Revadigar, G., Kumar, S. L. S., Yau, D. K., & Hu, Y. C. (2018, June). Signal jamming attacks against communication-based train control: Attack impact and countermeasure. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 160-171).

[2] Priyadarshani, R., Park, K. H., Ata, Y., & Alouini, M. S. (2024). Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview. arXiv preprint arXiv:2403.19868.

[3] Aziz, I. T., & Yadav, S. K. (2013). Data Encapsulation To Prevent Jamming Attacks In Wireless Networks. International Journal of Computer Technology and Applications, 4(6), 976.

[4] Heo, J., Kim, J. J., Paek, J., & Bahk, S. (2018). Mitigating stealthy jamming attacks in low-power and lossy wireless networks. Journal of Communications and Networks, 20(2), 219-230.

[5] Alam, M. M., & Le Moullec, Y. JAMMING OF SPREAD SPECTRUM COMMUNICATIONS USED IN UAV REMOTE CONTROL SYSTEMS.

[6] Patel, K. C., & Patel, A. (2022, November). Rogue access point: The WLAN threat. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 943-950). IEEE.

[7] Patel, K. C., & Patel, A. (2022, March). Taxonomy and future threat of rogue access point for wireless network. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 679-688). IEEE.

[8] Patel, K. C., & Goswami, S. A. (2024). Rogue Access Points: A Critical Threat to Electric Vehicle Charging Station Security. COMPUTER, 24(7).

[9] Patel, Dr. K. C. (2024). International Journal of Scientific Research in computer science, engineering and information technology. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(3), 632–643. https://doi.org/10.32628/ijsrcseit

[10] Patel, Dr. K. C. (2022). RECOGNITION OF ROGUE ACCESS POINTS USING A MACHINE LEARNING APPROACH. INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS - IJCRT (IJCRT.ORG), 10(12), C663–C672. https://ijcrt.org/papers/IJCRT2212283.pdf

[11] Chaitanyakumar, P. K. An Experimental Study and Novel Approach for Detection and Suppression of Rogue Access Point in Wlan.

[12] Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE communications surveys & tutorials, 24(2), 767-809.

[13] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. IEEE communications surveys & tutorials, 11(4), 42-56.

[14] Gambiraopet, C. S. (2009). Security threats and intrusion detection models in WLAN (Doctoral dissertation, University of Bedfordshire).

[15] Jamaluddin, J., Edwards, R., & Coulton, P. (2003). Providing a Risk Analysis Framework for Potential Users of Wireless Technology. In PostGraduate Networking Conference (PGNet) Liverpool: John Moores University.

[16] Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5(3-4), 154-174.

[17] Davies, M., Furey, E., & Curran, K. (2019). Improving compliance with bluetooth device detection. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(5), 2355-2369.

[18] McCarthy, J., McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., ... & Sepassi, S. (2023). Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). US Department of Commerce, National Institute of Standards and Technology.

[19] Nyathi, T., & Ndlovu, S. Beacon Frame Manipulation to Mitigate Rogue Access Points: Case of Smartphone Rogue Access Points.

[20] Gupta, S., Arshi, O., & Aggarwal, A. (2023). Wireless Hacking. In Perspectives on Ethical Hacking and Penetration Testing (pp. 382-412). IGI Global.

[21] Royster, G. (2005). Wireless Security Hodgepodge.

[22] Curran, K., & Smyth, E. (2007). Addressing WiFi Security Concerns. In Business Data Communications and Networking: A Research Perspective (pp. 302-327). IGI Global.

[23] Thiessen, C. M. (2022). Redesigning the Counter Unmanned Systems Architecture.

[24] Pattam, S. (2006). Enhancing Security in 802.11 and 802.1 X Networks with Intrusion Detection.

[25] Rambally, R., & Abel, V. S. An Analysis of WiMax Security Vulnerabilities.

[26] Aziz, I. T., & Yadav, S. K. (2013). Data Encapsulation To Prevent Jamming Attacks In Wireless Networks. International Journal of Computer Technology and Applications, 4(6), 976.

[27] Liu, Y., & Ning, P. (2012, March). BitTrickle: Defending against broadband and high-power reactive jamming attacks. In 2012 Proceedings IEEE INFOCOM (pp. 909-917). IEEE.

[28] Y. Shi, X. Lu, K. An, Y. Li and G. Zheng, "Efficient Index-Modulation-Based FHSS: A Unified Anti-Jamming Perspective," in IEEE Internet of Things Journal, vol. 11, no. 2, pp. 3458-3472, 15 Jan.15, 2024, doi: 10.1109/JIOT.2023.3296605.

[29] T. Huang, Y. Liu, X. Liu, and M. Wang, "A new improved multi-sequence frequency-hopping communication anti-jamming system," *Electronics*, vol. 14, no. 3, p. 523, 2025, [Online]. Available: https://doi.org/10.3390/electronics14030523.

[30] L. H. Newman, "GPS Jamming Is Screwing With Norwegian Planes," *Wired* , Jun. 27, 2023. [Online]. Available: https://www.wired.com/story/gps-jamming-is-screwing-with-norwegian-planes . [Accessed: Oct. 24, 2023].

[31] Nairametrics, "Aircraft Navigation System Disruptions Surge by 175% in 2024 – IATA," *Nairametrics* , Feb. 26, 2025. [Online]. Available: https://nairametrics.com/2025/02/26/aircraft-navigation-system-disruptions-surge-by-175-in-2024-iata/ . [Accessed: Oct. 24, 2023].

[32] AINonline, "Mitigating the Effects of GNSS Jamming and Spoofing," *AINonline* , Jan. 3, 2025. [Online]. Available: https://www.ainonline.com/aviation-news/air-transport/2025-01-03/mitigating-effects-gnss-jamming-and-spoofing . [Accessed: Oct. 24, 2023].

[33] Atlassian, "The Cost of Downtime," *Atlassian* . [Online]. Available: https://www.atlassian.com/incident-management/kpis/cost-of-downtime . [Accessed: Oct. 24, 2023].

[34] GDPR Info, "Fines & Penalties under GDPR," *GDPR Info* . [Online]. Available: https://gdpr-info.eu/issues/fines-penalties/ . [Accessed: Oct. 24, 2023].