iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VI Month of publication: June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72461

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Hacker 5GHz Jammer: Mechanism, Simulation, Impact, and Countermeasures

Angshuman Ghosh[1], Tushar Basak[2], Vinayak Raj Gupta[3], Koushik Pal[4], Surajit Basak[5], Kaushik Roy[6]
Department of Electronics and Communication Engineering, Guru Nanak Institute of Technology

Abstract: The rapid proliferation of 5 GHz wireless communication technologies has made them essential for high-speed connectivity in modern applications. However, this increased dependence also brings a heightened risk of cyber threats such as jamming attacks. This report investigates the mechanism of 5 GHz jamming attacks launched by malicious hackers, simulates their effects on wireless networks, and proposes robust countermeasures. Through code-based simulations in Python and Bash, this study models the relationship between jammer power and network degradation. We conclude by recommending techniques for mitigating these threats and ensuring secure wireless communication.

Keywords: 5 GHz jamming, wireless security, denial of service, Wi-Fi interference, countermeasures, simulation

I. INTRODUCTION

The 5 GHz band is widely adopted in modern wireless communications due to its higher data rates, reduced congestion, and increased number of non-overlapping channels. Despite these advantages, wireless systems remain vulnerable to jamming attacks. A jamming attack disrupts communication by introducing intentional interference into the wireless medium, causing denial-of-service (DoS) to legitimate users. This report explores how such attacks are carried out, simulates their impact, and discusses practical defensive strategies.

II. BACKGROUND AND RELATED WORK

Jamming attacks are a class of Denial-of-Service (DoS) attacks that target the physical layer of wireless communication. These attacks aim to disrupt the availability of wireless channels by introducing intentional interference that overwhelms legitimate signals, effectively blocking communication between devices. Types of jammers include:

A. Constant Jammer

A Constant Jammer is the most basic and aggressive form of jamming device used in wireless communication environments.

It operates by continuously transmitting high-power radio frequency (RF) signals over a particular wireless channel, with the sole objective of disrupting or completely blocking legitimate wireless communications.

B. Random Jammer

A Random Jammer is a more energy-efficient variant of the constant jammer. It operates by transmitting interference signals intermittently—that is, alternating between jamming and sleeping periods. This makes it both less detectable and more power-efficient, while still disrupting legitimate wireless communication.

C. Reactive Jammer

A Reactive Jammer is an intelligent and highly efficient jamming device that monitors the wireless medium and activates only when it detects legitimate communication. This makes it particularly stealthy, energy-efficient, and hard to detect. It is considered one of the most dangerous forms of jamming because it can target specific packets or transmissions in real-time.

While extensive research exists on jamming in general, relatively few studies focus specifically on 5 GHz networks. This report seeks to fill that gap.

III.MECHANISM OF 5GHZ JAMMING

A. Techniques

1) *Hackers employ several techniques to jam 5 GHz networks:* Tone Jamming: Tone Jamming is a type of narrowband jamming technique that works by emitting a strong, continuous sine wave (tone) on a specific frequency or channel used for legitimate wireless communication. It is a precise and targeted attack designed to interfere with signal decoding by reducing the Signal-to-Noise Ratio (SNR) at the receiver.

2) *Sweep Jamming:* Sweep Jamming (or Swept-Tone Jamming) is a type of frequency-agile interference in which a jamming signal rapidly shifts its frequency across a wide band, often in a periodic or pseudo-random pattern. This technique disrupts communication systems that use fixed frequencies or even some spread-spectrum systems, by intermittently introducing interference across the communication band.
3) *Packet Injection:* Packet Injection is a network attack technique where an attacker inserts forged or deceptive data packets into a communication stream. These packets are crafted to appear as though they are part of the normal communication but are used to confuse, disrupt, or manipulate network behavior and device responses.

Unlike jamming, which disrupts communication via interference, packet injection manipulates the protocol logic, making it especially dangerous in wireless and IoT networks.

Fig.1 ESP8266 NodeMCU Wi-Fi Development Board for IoT

B. *Hardware Tools*Common hardware used includes:

1) HackRF One: HackRF One is a low-cost, open-source Software-Defined Radio (SDR) platform developed by Great Scott Gadgets. It can transmit and receive radio signals from 1 MHz to 6 GHz, making it extremely versatile for studying and attacking a wide range of wireless protocols—including 5 GHz Wi-Fi.
2) USRP B200/B210: The USRP B200 and B210 are high-performance SDR platforms developed by Ettus Research (now part of NI – National Instruments). They are widely used in academic research, defense, wireless security, and telecom prototyping due to their robust architecture and precision control.
3) Wi-Fi Deauthentication tools with custom firmware: These tools use low-cost microcontrollers—such as the ESP8266 or ESP32—flashed with specialized firmware to send malicious packets (especially deauth frames) to disconnect clients from Wi-Fi networks. They are mainly used for educational penetration testing, not full-spectrum jamming.

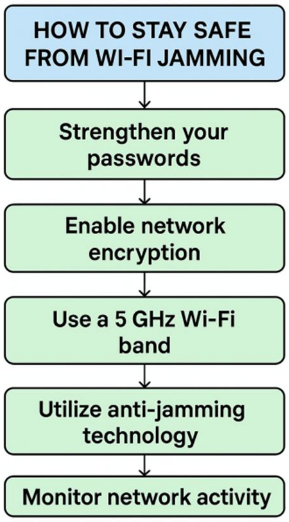

HOW TO STAY SAFE FROM WI-FI JAMMING
Strengthen your passwords
Enable network encryption
Use a 5 GHz Wi-Fi band
Utilize anti-jamming technology
Monitor network activity

Fig.2 Preventive actions against jamming attacks

IV. SIMULATION ENVIRONMENT

To analyze the impact of jamming on 5 GHz wireless networks, we implemented two separate simulations—one in Python for analytical modeling and visualization, and another in Bash to emulate packet-based interference in a simplified manner. These simulations aim to capture the degradation of network performance in the presence of varying jammer power levels.

A. Python-Based Simulation

The Python-based simulation focuses on modeling the Signal-to-Interference-plus-Noise Ratio (SINR) and its relationship with packet transmission success rates. This environment simulates the behavior of a wireless system under increasing levels of jamming power and tracks how signal quality and data integrity are affected.

1) Key Features

Packet Transmission Model: The system simulates the transmission of 1000 data packets for each jammer power level ranging from 0 dBm to 30 dBm in 5 dBm increments.

SINR Calculation: For each packet, the SINR is computed using the formula:

$$\mathrm{SINR} = P_{\mathrm{signal}} / (P_{\mathrm{jammer}} + P_{\mathrm{noise}})$$

where:
P_{signal} = 20 dBm
P_{jammer} = varies from 0 to 30 dBm,
$P_{\mathrm{noise}} = -90$ dBm

Packet Success Probability: A logistic function is applied to the SINR to model the probability of successful packet delivery. This reflects real-world wireless channel behavior where higher SINR correlates with greater reliability.

Visualization: The results are plotted to show the relationship between jammer power and packet delivery ratio (PDR), highlighting the critical thresholds where communication begins to fail.

B. Bash-Based Simulation

To simulate jamming effects in a more practical and command-line friendly environment, a lightweight Bash script is developed. This script models packet drops based on jammer power levels without involving detailed radio layer parameters.

1) Simulation Logic:

i. For each jammer power level, the script simulates 1000 packet transmissions.
ii. The jammer power is mapped to a drop probability, increasing linearly.
iii. If a randomly generated number exceeds the drop threshold, the packet is marked successful; otherwise, it is dropped.

2) Advantages:

i. Useful for quick emulation of jamming conditions.
ii. Requires minimal system resources.
iii. Ideal for integration into automated testing pipelines for DoS vulnerability testing.

C. Parameters

The following parameters were standardized across both simulations to ensure consistency and replicability:

TABLE I
PAREMETERS FOR SIMULATION

Parameter	Value
Transmit Power	20 dBm
Jammer Power	0 to 30 dBm
Noise Floor	-90 dBm
Number of Packets	1000 per run

These values approximate realistic wireless communication settings and allow the simulation to capture the impact of progressively stronger jamming signals on network reliability.

V. RESULTS AND ANALYSIS

This section presents the results obtained from the Python and Bash-based simulations, offering insights into how 5 GHz jamming affects wireless communication in terms of throughput, packet loss, and SINR degradation.

A. Throughput and Packet Loss

The most direct consequence of increasing jammer power is a decline in throughput and a rise in packet loss. As the jammer emits stronger signals, it increasingly interferes with legitimate communication between Wi-Fi transmitters and receivers.

1) *Linear Drop in Success Rate:* The simulation clearly demonstrates a near-linear decline in packet success rate wit increasing jammer power.
2) *Critical Power Threshold:* At a jammer power of 20 dBm, over 80% of packets are dropped or fail to reach the receive successfully.
3) *Network Disruption:* When jammer power exceeds 25 dBm, the network experiences near-complete disruption, making reliable communication virtually impossible.

This behavior aligns with real-world observations where jammers operating at similar power levels can effectively neutralize nearby 5 GHz communications within range.

B. SNR Impact

Signal-to-Interference-plus-Noise Ratio (SINR) is a key metric in determining the quality and reliability of a wireless link. As jammer power increases, the SINR drops sharply, leading to increased bit error rates and failed transmissions.

1) *SINR Degradation Curve:* With jammer power starting at 0 dBm, SINR remains high (>30 dB), indicating a clean channel. However, as jammer power reaches 20 dBm, SINR drops below 0 dB, making successful decoding of signals nearly impossible.
2) *Error Propagation:* Low SINR values increase the likelihood of frame errors, which in turn cause retransmissions, congestion, and further throughput degradation.
3) *Impact on Latency:* Due to retransmission and error correction mechanisms kicking in, network latency also increases significantly under high jamming conditions.

C. Visual Trends

1) *Jam Power vs Packet Success Rate:* A line graph showing packet success percentage against jammer power in dBm.
2) *Jam Power vs SINR:* A graph demonstrating how SINR declines as jammer power increases.
3) *Histogram of Packet Drops:* A frequency plot to visualize how often packets are lost at each power level.

D. Cross-Validation Between Simulations

The results from the Python simulation, which uses a probabilistic SINR model, are consistent with the Bash-based simulation that operates via randomized packet success/failure events. This cross-validation strengthens the reliability of the outcomes and suggests that both simulation approaches effectively model the effects of 5 GHz jamming.

VI. COUNTERMEASURES

To combat the growing threat of 5 GHz jamming attacks, various countermeasures have been proposed and implemented. These techniques range from physical-layer adaptations to protocol-level modifications and intelligent detection mechanisms. The following subsections detail the most promising strategies.

A. Frequency Hopping

Frequency Hopping Spread Spectrum (FHSS) is one of the oldest and most effective anti-jamming techniques.

1) *Working Principle:* Transmitters and receivers hop across a wide range of frequencies in a synchronized manner, making it difficult for a jammer to consistently interfere unless it can jam the entire band (which is energy-inefficient).
2) *Advantage Against Constant Jammers:* Constant jammers target fixed frequencies. FHSS evades these attacks by never staying on one frequency for long.
3) *Regulatory and Hardware Considerations:* Implementing FHSS in Wi-Fi systems, especially those based on IEEE 802.11ac or 802.11ax, may require significant firmware and hardware upgrades.

B. Adaptive Power Control

Adaptive Power Control (APC) is used to dynamically adjust the transmission power based on real-time channel conditions.

1) *Jammer Mitigation:* Increasing signal strength temporarily can help maintain communication even in the presence of moderate jamming.

2) *Trade-offs:* While higher power improves Signal-to-Noise Ratio (SNR), it can cause:
   i. Battery Drain in mobile devices.
   ii. Regulatory Violations due to power limits on unlicensed spectrum bands.
3) *Smart Implementation:* APC is most effective when implemented with contextual awareness and only activated during detected jamming incidents.

C. Detection Mechanisms

Detecting the presence of a jammer is critical for activating protective measures and tracing attack origins.

1) *Signal Anomaly Detection:* Monitoring metrics like sudden drops in throughput, spikes in packet loss, or unusual signal strength can indicate jamming.
2) *Machine Learning Models:*
   i. Supervised learning can classify traffic patterns as normal or jammed.
   ii. Unsupervised learning can flag deviations without prior labels.
3) *Localization Techniques:* Directional antennas and triangulation help pinpoint jammer location, especially useful in securing sensitive environments like hospitals or military networks.

D. Protocol Enhancements

Modifications at the protocol level offer another layer of defense.

1) *RTS/CTS Mechanism (Request to Send / Clear to Send):*
   i. Helps mitigate hidden node and collision issues.
   ii. Can be adapted to delay communication during suspected jamming windows.
   iii. Acts as a handshake to ensure the channel is clear before data is sent.

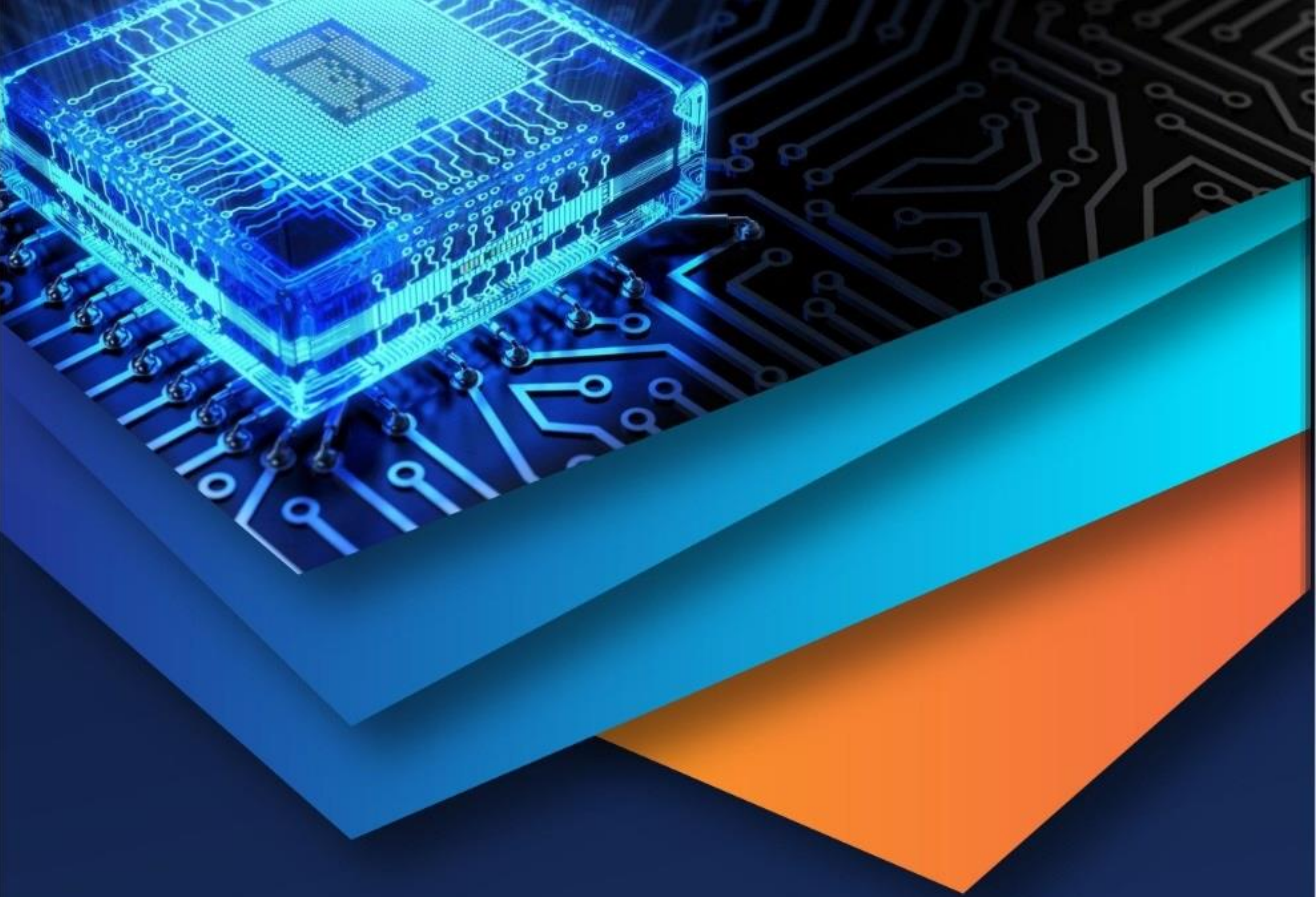
2) *MIMO Beamforming:*
   i. Multi-Input Multi-Output (MIMO) systems use multiple antennas to focus signal energy in a particular direction.
   ii. Benefit: Reduces signal leakage and interference from jammers not aligned with the beam.
   iii. Challenge: Requires sophisticated hardware and algorithms for real-time spatial filtering.

VII. CONCLUSIONS

The increasing dependence on 5 GHz wireless communication in modern applications—ranging from enterprise Wi-Fi to smart home networks—makes it a critical target for jamming-based denial-of-service attacks. This paper has explored the inner workings of 5 GHz jamming techniques used by hackers, developed simulation environments in both Python and Bash to model the degradation of packet success rates under varying jamming conditions, and analyzed the results. Our simulations confirm a direct, inverse correlation between jammer power and communication reliability. Even moderate levels of jamming significantly reduced packet delivery rates and overall network efficiency. These findings emphasize the real threat posed by physical-layer attacks on high-frequency wireless networks. To mitigate such threats, we recommend a layered defense strategy comprising frequency hopping, adaptive transmission protocols, power control, and machine learning-based jammer detection. As the reliance on wireless technologies continues to grow, the proactive implementation of such countermeasures will be essential to safeguard communication integrity and availability. Future research should focus on integrating software-defined radios for real-time detection and response, experimenting with AI-based anomaly detection models, and validating these simulations in real-world testbeds.

REFERENCES

[1] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. ACM MobiHoc.
[2] Wood, A., & Stankovic, J. (2002). Denial of service in sensor networks. IEEE Computer.
[3] IEEE Std 802.11ac-2013 - Wireless LAN MAC and PHY Specifications.
[4] NS-3 Network Simulator: https://www.nsnam.org
[5] HackRF One SDR: https://greatscottgadgets.com/hackrf/
[6] GNU Radio Toolkit: https://www.gnuradio.org
[7] Python: https://www.python.org
[8] bc Calculator: https://www.gnu.org/software/bc/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY