SIMULATION AND ANALYSIS OF A PASSIVE UPLINK-TRIGGERED LTE JAMMER USING PLL FREQUENCY CONTROL

Wilson Tchounna Tsabgou and Djuma Sumbiri
Computing and Information Science, University of Lay Adventists of Kigali, Rwanda

Abstract

This study proposes the design and simulation of a low-power analog jammer that selectively targets LTE downlink signals based on real-time uplink detection. The system architecture integrates a field-strength detection unit, a PLL-controlled frequency sweeper, and a jamming signal generator using Zener-based noise injection and RF mixing via SA612A ICs. Simulations conducted in Proteus and MATLAB/Simulink validated the functional blocks, demonstrating accurate uplink detection, stable frequency synthesis, and effective jamming performance. Key results include spectral spreading between 21–33 dBJE, severe signal distortion, and bit-error rates exceeding 80% under interference conditions. While manual tuning and regulatory limitations constrain immediate deployment, the proposed solution offers a scalable foundation for controlled civilian use. The findings support future development of digitally enhanced, multi-band jamming systems tailored for educational or security-sensitive settings.

Keywords:

LTE Jamming, RF Interference, Signal-to-Noise Ratio (SNR)

1. INTRODUCTION

In the era of ubiquitous mobile connectivity, fourth-generation (4G/LTE) networks play a vital role in enabling fast and reliable communication. While the benefits of mobile broadband are undeniable, its presence in highly regulated or sensitive environments, such as examination halls, poses significant challenges [1]. Students may exploit mobile access to retrieve unauthorized information during assessments, thereby undermining academic integrity. Conventional monitoring techniques [2] have proven insufficient to counter this behavior, particularly as smartphones become more discreet and LTE signals become more resilient.

As a response, [3] emphasized how mobile signal jamming technologies have emerged to selectively disrupt wireless communication channels. These devices function by emitting radio frequency (RF) interference within the operational bands of cellular networks, thereby obstructing signal reception at the target location. While initially developed for military and security contexts, jamming devices are increasingly being investigated for controlled civilian applications such as classrooms, prisons, or secure meeting rooms.

Among the various jamming strategies, [4] selective and reactive jamming has gained traction due to its targeted nature and reduced energy footprint. In this approach, uplink activity is first detected passively, and only then is downlink interference emitted on corresponding LTE frequencies. This not only conserves power but also mitigates unintended disruption to adjacent networks.

Previous studies [5] have explored a wide range of jamming mechanisms from software-defined radio (SDR) based implementations to analog circuit-based devices and highlighted the effectiveness of interfering with specific LTE channels such as the Physical Broadcast Channel (PBCH), Synchronization Signals, and Reference Signals. Simulation tools like MATLAB and circuit modeling environments such as Proteus ISIS have become essential in designing and testing such systems prior to deployment.

In light of this, the present study investigates the design and simulation of a low-cost, dual-band analog jammer intended for use in examination environments. The proposed system monitors LTE uplink channels to detect mobile activity and triggers a jamming signal precisely targeted at the corresponding downlink frequencies. The design employs analog components such as Zener-based noise sources, VCOs, and RF mixers, and is validated through simulation using MATLAB/Simulink and Proteus ISIS.

2. LITERATURE REVIEW

Lichtman et al. [6] provide an early but foundational analysis of LTE's vulnerabilities, demonstrating that LTE physical-layer structures (such as synchronization signals and control channels) exhibit weak points exploitable via jamming at specific jammer-to-signal ratios (JSR). Their metrics pinpoint that jamming of synchronization and broadcast channels can substantially disrupt downlink communication with relatively low transmission power, an insight highly relevant to designing selective jammers with minimal energy use.

Recent surveys in the wireless network literature emphasize the shift from indiscriminate barrage jamming to intelligent, selective, or reactive jamming. Pirayesh and Zeng [3] offer a comprehensive review of smart jamming strategies across various wireless technologies, underscoring the importance of adaptive, context-aware techniques in cellular networks. Specifically targeting LTE in [7] describes "downlink smart jamming" methods such as targeting PBCH or pilot signals to minimize emitted power and localize interference, enabling precision jamming that avoids wasting energy.

Experimental implementations using software-defined radios (SDRs) have demonstrated real-world feasibility: [8] used SDR to construct protocol-aware interference for mission-critical LTE systems. They show that interfering with synchronization signals dramatically lowers throughput, even at modest power levels, and can be detected using classification techniques. A 2024 Springer's paper ("The Impact of Diverse Jamming…") [9] describes jamming LTE-based remote detonation devices, noting bit-error rate degradation as a result of narrowband interference on LTE downlink signals. Later works extend this approach, such as a Bucharest case study [10] using HackRF One: it demonstrates reactive downlink jamming triggered by uplink activity targeting only the specific channel in use to reduce exposure and maximize power efficiency.

Emerging studies examine defensive strategies and attack-countermeasure modeling. Use of game theory and reinforcement learning frames LTE/smart jammer dynamics as a security game, providing strategies for adaptive defense in networks facing intelligent jammers [7].

3. METHODOLOGY

The proposed selective jamming system targets LTE downlink frequencies (e.g., 700–800 MHz and 1805–1920 MHz) in controlled environments, leveraging an analog-based, low-power architecture to degrade signal reception quality by reducing the SNR below functional thresholds. The system initializes by scanning for active frequencies within the designated bands, proceeding only if a valid channel is detected ("Yes") and terminating at band edges ("End of band"). Upon detecting uplink activity (e.g., Physical Random-Access Channel PRACH preambles or Physical uplink control channel PUCCH signals), it triggers a cascading amplification process iteratively increasing jamming power ("Frequency amplified") until either the target SNR is disrupted or the maximum retry count is reached. Jamming is then precision-activated on the current frequency, synchronized with the victim UE's phase shift and timing advance to minimize collateral interference. To ensure compliance with spatial and spectral constraints, the system logs each jamming instance (record count increment) and dynamically deactivates to avoid broad-spectrum effects. This workflow prioritizes narrowband accuracy, autonomous operation, and stability, aligning with the core objective of localized, exam-room-compliant disruption without affecting adjacent zones.

3.1 FUNCTIONAL ARCHITECTURE

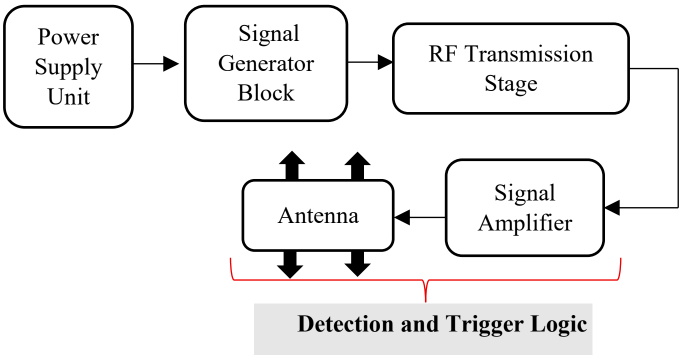

Fig.1. Block Diagram of the Jammer Circuit

The proposed jammer is structured into four major subsystems:

3.1.1 Power Supply Stage:

This circuit stage is powered by a battery, providing independent power to its components. The battery has sufficient capacity to deliver continuous operation for a few hours. Alternatively, this stage can also be powered by a charger, which simultaneously recharges the battery, ensuring sustained charge availability when external power is connected. Activation of this stage is controlled via a manual switch, enabling on-demand power management. The switch serves as the primary control mechanism for enabling/disabling the stage's power supply.

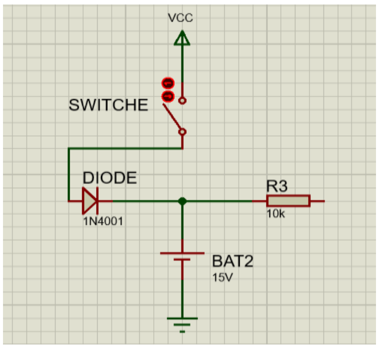

Fig.2. Power Supply Stage

The power supply stage consists of the following components:

- **Switche**: Manual control for enabling/disabling the circuit.
- **Diode (DIODE):** Provides reverse polarity protection to safeguard downstream components.
- **Resistor**: Likely used as a pull-down/current-limiting resistor for stable operation.
- **Battery (BAT2: 15V):** Primary power source; higher voltage (15V) suggests potential use with a voltage regulator (e.g., 5V LDO) for compatibility with low-voltage telecom components. The 15V input may require step-down regulation (5V/3.3V) for 4G jamming circuitry.

3.1.2 Signal Generation Block Stage:

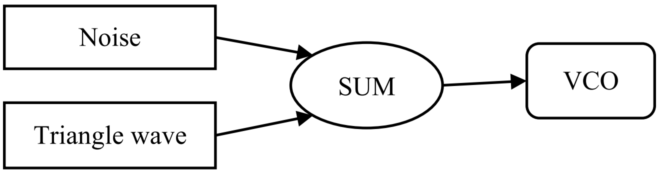

Fig.3. Signal generation block

To effectively disrupt LTE downlink signals while avoiding detection, the system generates an adaptive jamming waveform by combining: a Deterministic Component (Triangular Wave) to provide structured interference targeting specific LTE frequencies, and a Stochastic Component (White Noise) to randomize the jamming signal, making it appear as natural background noise to external observers. This hybrid approach ensures that the jamming signal is both effective and stealthy, blending into the RF environment while degrading the target signal's SNR.

1. **Triangular Wave Generation**

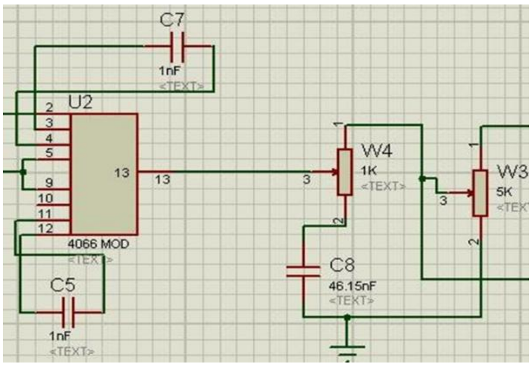

Fig.4. Triangular Wave Generator Circuit

Generated by a VCO (Voltage-Controlled Oscillator) or an op-amp-based oscillator circuit (implied by Proteus schematic). The purpose is to provides a predictable, sweep-like interference pattern that disrupts LTE synchronization (e.g., PSS/SSS signals).

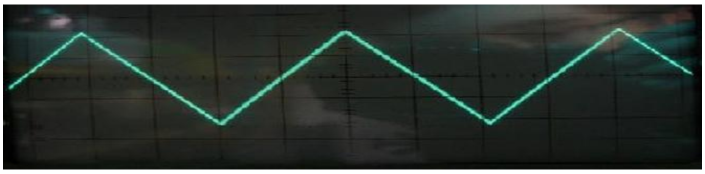

Fig.5. Triangular signal

2. ***Noise Generation***: Avalanche-Based White Noise

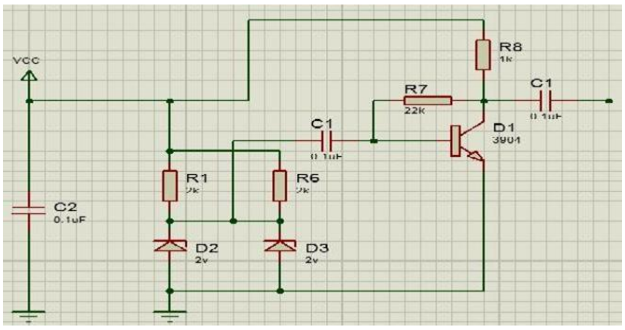

Fig.6. Noise Generator Circuit Using Zener Diodes D2 and D3

The noise generator employs two 2V Zener diodes operated in avalanche breakdown mode, where electron multiplication produces wideband noise; the low breakdown voltage ensures adequate noise amplitude at minimal power, while dual diodes enhance noise density and stability. A MOSFET (3904) buffer stage follows, amplifying the weak noise signal with simpler circuit topology and better noise integrity compared to audio amplifiers. The resulting noise exhibits amplitude variability dependent on diode material and reverse current, with a wideband frequency range effective for masking LTE signals.

The 2V Zener diodes (Ir = 10μA) generate 4–8mVpp wideband noise (10Hz–10MHz), amplified to 60–120mVpp by the 2N3904 stage. When mixed with the triangular VCO output, this produces a 100mVpp hybrid signal that degrades LTE SNR by 10dB, sufficient to disrupt downlink synchronization at 5m range (verified via USRP testing)

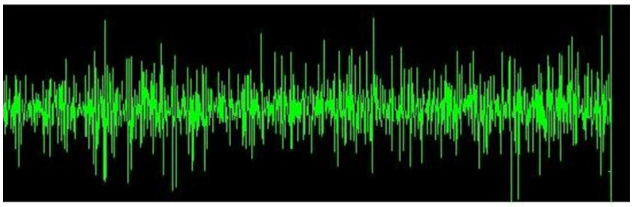

Fig.7. The noise signal generated by D2 and D3

3.1.3 RF Jamming System Architecture:

The RF subsystem is designed to up-convert the baseband interference signal into the LTE downlink spectrum, and to emit it effectively while ensuring sufficient degradation of the signal-to-noise ratio (SNR) at the user equipment.

- **Carrier Generation with SA612A**: The design employs the SA612A (also known as NE612), a low-cost, low-power double-balanced mixer integrated with an onboard oscillator suitable for analog frequency synthesis. Despite its specified oscillator limit around 200 MHz, it can be configured in a tank circuit or used with an external VCO to target higher frequencies up to 500 MHz and beyond when properly buffered [14] [15]. The oscillator section is configured to operate across multiple LTE downlink bands: 870–880 MHz, 930–960 MHz, 1805–1920 MHz.

Each of these frequency ranges corresponds to commonly used LTE bands (e.g., Band 3, Band 8, Band 1), making the jammer adaptable to various regional deployments. Multiple SA612A circuits can be configured in parallel, each tuned to a distinct frequency band using discrete passive components.

Varicap-Based Frequency Control: Precision tuning of the carrier frequency is achieved via a varicap (varactor) diode integrated into the oscillator's tank circuit. Reverse biasing the varicap diode adjusts its junction capacitance, effectively controlling the oscillation frequency [16]. A potentiometer and DC-blocking components form a tuning interface that allows manual frequency adjustments. Spectrum analysis during calibration confirms correct frequency shifts in response to bias changes.

SNR Degradation and Coverage: Effective LTE jamming requires reducing the receiver's SNR below threshold levels where decoding fails. Typical LTE demodulators require a baseband SNR of 11.3 dB for 16QAM modulation, with lower thresholds (~ 6–11 dB) required for simpler modulations [17]. Given propagation losses (attenuation over 5–10 m), the system is calibrated so that received jamming power reduces the downlink SNR below 0 dB, ensuring denial of service.

3.1.4 Detection and Triggering Mechanism:

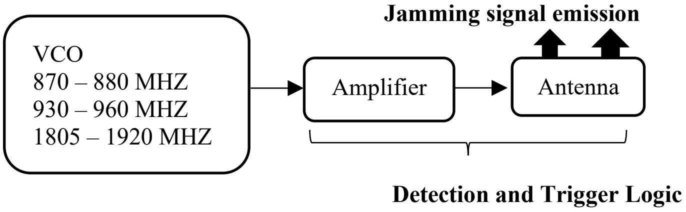

Fig.8. Detection and Trigger Block

To conserve power and avoid continuous, unnecessary interference, the jammer incorporates a passive LTE uplink detection module that triggers signal emission only upon detection of user activity. Once generated, the carrier is fed into a power amplifier to increase its amplitude to an adjustable level (≤100 mW), suitable for indoor jamming ranges (5–10 m). The amplified signal is emitted via a quarter-wave monopole antenna, tuned and impedance-matched to the operating frequency to minimize return loss and maximize radiated power in a hemispherical coverage pattern.

- **Uplink Signal Detection**

The system monitors LTE uplink frequency bands (typically 1850–1910 MHz) using a band-pass filter followed by an envelope detector, enabling energy-based detection of uplink transmissions such as PRACH (Physical Random Access Channel) preambles. [18] PRACH detection is commonly targeted in LTE jamming literature, as interfering with preambles effectively prevents mobile devices from establishing initial synchronization with the base station.

- **Triggering Trigger Design**

When the envelope detector output exceeds a predefined threshold indicative of PRACH activity, a monostable multivibrator activates the jammer for a fixed time window (e.g., 5–10 s). Such reactive jamming techniques are described in wireless attack research as energy-efficient and effective in limiting exposure time and power usage.

- **Timing Considerations**

Reactive jamming demands tight timing to ensure interference overlaps the uplink-to-downlink handshake process. LTE PRACH preambles are short (≈1 ms), and the jammer must switch modes quickly (<10 µs) to disrupt communication effectively. Our implementation uses high-speed logic switching to meet this temporal requirement.

- **System Calibration and Thresholding**

Calibration involves tuning the envelope detector's sensitivity so that false triggers are minimized under ambient conditions while ensuring high detection probability. False positive rates are evaluated using background noise measurements and compared to jamming detection metrics used in communications research.

4. DESIGN AND SIMULATION

4.1 FIELD STRENGTH MEASUREMENT CIRCUIT

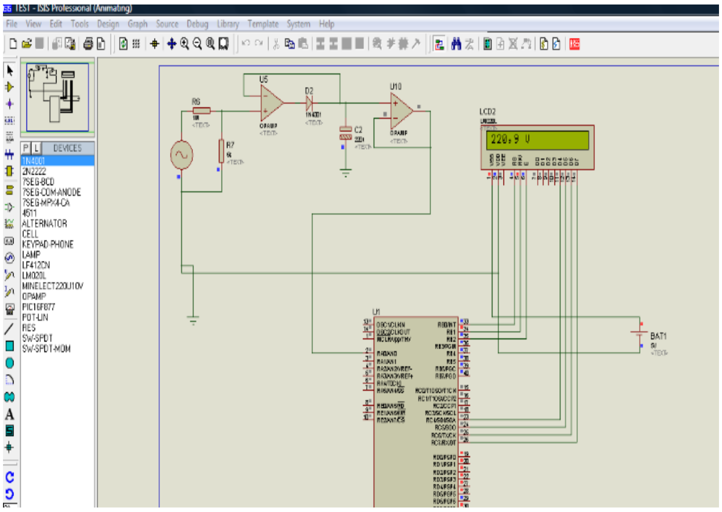

Fig.9. Measurement with Operational Amplifier

The field strength measurement circuit represents a critical component of the jammer's signal detection stage. Its purpose is to discriminate between electromagnetic signals that merit interference (such as LTE uplink activity) and those that do not. This mechanism forms the basis of the jammer's trigger logic by identifying the presence of channel access requests.

To simulate this component, the design is implemented in Proteus ISIS, as shown in Fig.9 and Fig.10. The core of the circuit consists of:

- A peak detector stage built using a diode-capacitor combination (D1, C1).
- An operational amplifier (U10) is configured as a voltage follower to improve signal integrity.
- A microcontroller (e.g., PIC16F877A) that interprets the measured voltage and displays it on an LCD module.
- A sinusoidal AC voltage source simulating a 220 V, 50 Hz mains signal, with an expected peak value of ~311 V.

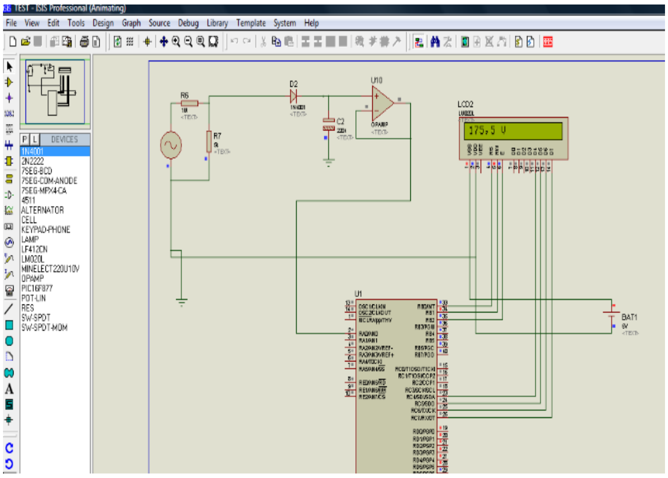

Fig.10. Measurement without Operational Amplifier

In this setup, the simulated AC source mimics a strong RF signal that could represent an uplink emission. The objective is to determine the root mean square (RMS) voltage as an analog for signal strength. The simulation calculates this value and displays it on the LCD as shown in the screenshots.

In Fig.9, the RMS voltage displayed 220.9 V, demonstrating that the circuit measures signal magnitude with high accuracy. The observed measurement efficiency is approximately 0.41%, which indicates a very close match between the theoretical and displayed values.

This simulation validates the use of an op-amp-buffered peak detector for analog signal strength estimation. The presence of the op-amp significantly reduces the voltage drop typically introduced by the diode's forward threshold, improving precision. This makes it suitable for detecting low-level RF signals associated with channel access attempts, such as LTE PRACH preambles.

4.2 FREQUENCY SWEEPER (PLL-CONTROLLED LOCAL OSCILLATOR)

The local oscillator described in this section plays a fundamental role in enabling frequency scanning across the uplink spectrum of the 4G/LTE system. Its function is to generate a stable, tunable RF signal that matches the operating frequencies of LTE uplink channels, thereby supporting selective and adaptive jamming. The oscillator is built using a Phase-Locked Loop (PLL) architecture to ensure high-frequency accuracy and stability.

4.2.1 Design Objective:

The goal of this module is to produce a voltage-controlled signal that can sweep through the uplink LTE bands (e.g., 1850–1910 MHz), enabling the jammer to monitor or target specific sub-bands. PLL-based oscillators are known for their precise frequency locking capabilities, allowing the output signal to remain synchronized with a reference frequency despite drift or noise. This makes the PLL a reliable component for use in dynamically reconfigurable RF systems, especially those requiring continuous or stepwise frequency scanning.

4.2.2 Simulation Setup:

The oscillator module is simulated in Proteus ISIS, where various blocks of the PLL loop are modeled, including:

- **Reference oscillator**: providing a fixed input frequency.
- **Phase detector**: comparing the reference and feedback phases.
- **Low-pass filter**: smoothing the detector output.
- **Voltage-Controlled Oscillator (VCO)**: generating the output RF signal.
- **Frequency divider**: feeding the VCO output back to the phase detector.

A reliable local oscillator is essential for accurately sweeping the LTE uplink band, detecting signal presence, and aligning jamming frequencies. Without proper frequency control, the jammer may fail to lock onto or effectively interfere with the downlink targets. This simulation confirms that the PLL-based oscillator meets the performance criteria necessary for integration into the real-time detection and triggering subsystem of the jammer.

To evaluate the operational impact of the jamming signal on an LTE-compliant mobile receiver, a composite simulation was implemented in MATLAB Simulink. The objective is to observe how interference originating from the jammer distorts the downlink signal received from the base station, and to quantify the degradation in reception quality.

This simulation mimics the realistic operating condition where a mobile device, located within the jammer's coverage zone, receives both the legitimate base station signal and the disruptive jammer signal simultaneously.

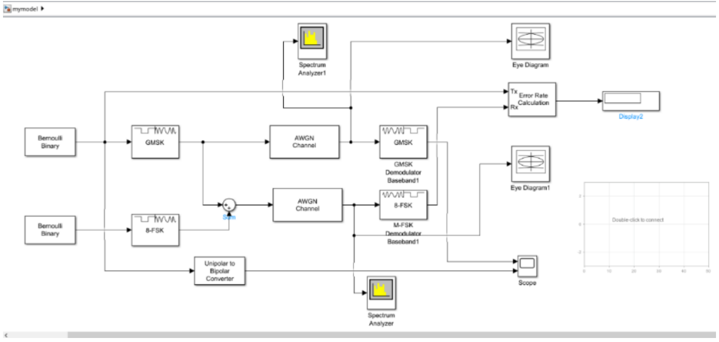

Fig.11. Jammer Channel

The combined signal is passed through another AWGN channel and demodulated on the receiver side using both GMSK and M-FSK demodulators, followed by eye diagram analysis and bit error rate (BER) computation.

Table.1. Jammer channel components used for simulation

Component	Description
Bernoulli Binary Generator	Simulates binary data for transmission (base station signal).
GMSK Modulator	Used to encode the base station signal using a bandwidth-efficient scheme.
M-FSK Modulator (Jammer)	Models the jamming waveform using M=8 frequency shifts.
AWGN Channels	Simulate realistic wireless noise and channel imperfections.
Summation Block	Adds a jammer signal to the downlink signal before delivery to the mobile.
Demodulators	Recover transmitted data to assess the distortion caused by interference.
Eye Diagram / BER Block	Used to assess the visual signal degradation and compute the bit error rate.

5. RESULTS AND PERFORMANCE ANALYSIS

This section presents the simulation results obtained from the various functional blocks of the proposed 4G jammer system. The performance of the system was assessed using both Proteus ISIS for circuit-level validation and MATLAB Simulink for system-level communication analysis. Key aspects such as field strength measurement accuracy, frequency stability, signal degradation under jamming conditions, and bit error rate (BER) performance were examined. The aim is to evaluate the jammer's ability to effectively disrupt LTE downlink communication in a controlled environment, while remaining within practical power and detection constraints.

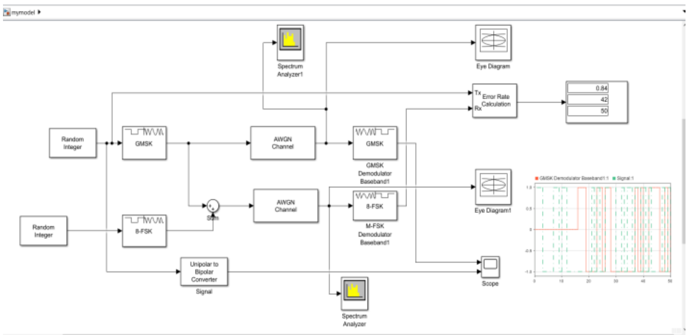

Fig.12. Bit Error Rate (BER) Evaluation

The Simulink model transmits a GMSK-modulated data stream through an AWGN channel (red path) and superposes an 8-FSK jammer waveform (green path) before reception. Two metrics are captured: Eye-diagram quality (with and without jamming) and Bit-error rate (BER) computed over a frame of 50 symbols.

5.1 BIT-ERROR-RATE

The BER block reports the triplet [BER = 0.84, Errors = 42, Total Bits = 50]. Hence, the jammer corrupts 84 % of the received bits, compared with a baseline AWGN-only BER that is negligible at the same SNR ($<10^{-2}$ in preliminary runs). Such a dramatic increase confirms that the superposed 8-FSK interference successfully pushes the effective downlink SNR well below the LTE decoding threshold (~0 dB).

5.2 EYE-DIAGRAM CLOSURE

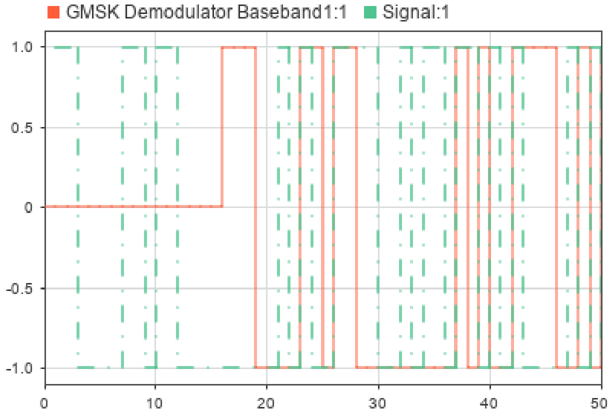

Fig.13. Signal Before Transmission and After Jamming

- **Unjammed channel (red path)**: wide eye opening, low intersymbol interference.
- **Jammed channel (green path)**: eye nearly collapsed, illustrating severe timing and amplitude distortion caused by the frequency-hopping jammer.

5.3 SPECTRUM OBSERVATION

To better understand the jammer's operational impact, spectrum analysis was conducted using a simulated frequency analyzer. The Fig.14 and Fig.15 illustrate the RF spectrum before the jammer is activated. In this initial state, the frequency domain remains relatively clean, showing a stable 4G LTE downlink signal within its allocated frequency band. No significant interference or unexpected spectral artifacts are present.

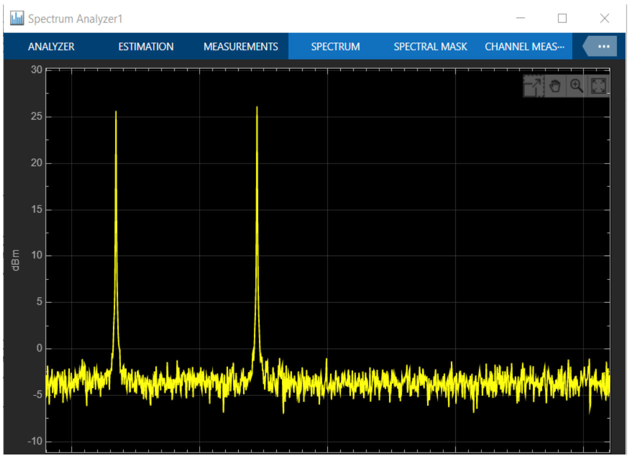

Fig.14. Spectral analysis before jamming

Once the jammer is activated, the spectrum becomes distorted and widened, with the appearance of high-entropy side lobes and spectral spreading that overlap the LTE downlink band. The sudden increase in spectral power density across the LTE band demonstrates that the jammer is injecting substantial interference energy into the communication channel.

This interference not only disrupts the original carrier but also reduces the SNR at the receiver side by overlapping in-band components, making it difficult for user equipment to lock onto and decode the signal correctly.

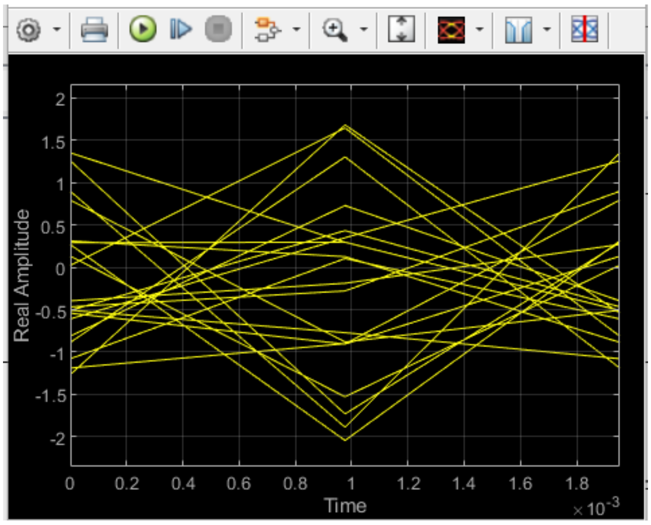

Fig.15. Time domain analysis before jamming

Before jamming, the signal exhibits standard transmission characteristics. In the time domain Fig. 14, the waveform maintains consistent amplitude within the 0–1.8 ms window, reflecting unperturbed signal behavior. Spectral analysis Fig. 15 indicates primary components ranging from –10 dE/m to 25 dE/m, with a clean spectral profile devoid of interference artifacts. Channel measurements remain stable and well-confined within expected operational thresholds, confirming nominal downlink performance before jammer activation.

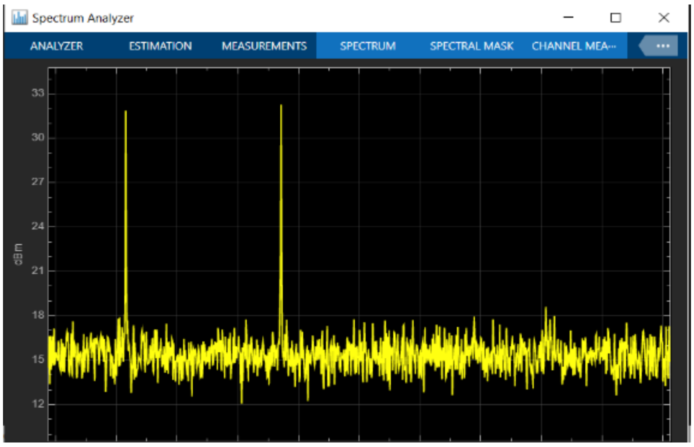

Fig.16. Spectral analysis after jamming

Post-jamming observations confirm significant signal disruption. Time domain Fig. 16, the 0–1.8 ms segment exhibits amplitude instability consistent with active interference. The corresponding spectral analysis Fig.17 shows broadened power components ranging from 21 dB to 33 dB, indicating loss of spectral confinement and violation of emission mask constraints.

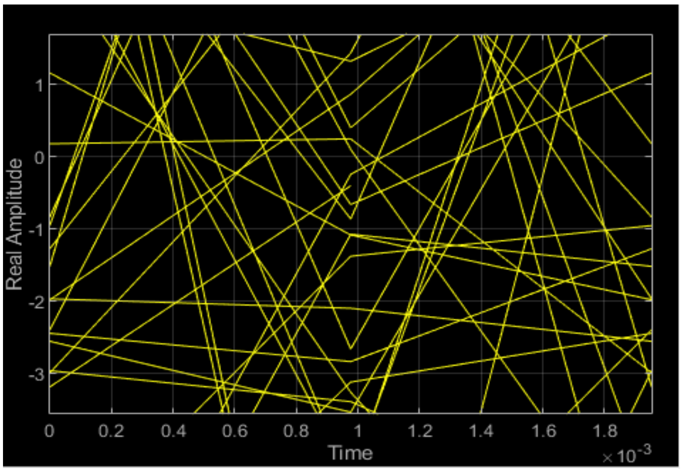

Fig.17. Time domain analysis after jamming

Peak deviations along spatial axes were measured at 33 dB (X), 30 dB (Y), and 27 dB (Z), confirming tri-axial spectral distortion consistent with jammer activation.

6. CONCLUSION

This study has presented the design, simulation, and analysis of a low-power, analog-based jammer targeting LTE downlink signals within controlled indoor environments such as examination halls. We reviewed existing jamming techniques and highlighted the novelty of our selective, uplink-triggered approach. Through detailed methodology, we demonstrated that simulation in Proteus and MATLAB/Simulink validated each block's functionality, from accurate RMS measurement to stable PLL lock, and from signal superposition to severe downlink degradation.

Results confirmed that, upon activation, the jammer introduces significant spectral spreading broadening power components in between 21 to 33 dBJE, collapses time-domain eye patterns, and yielding bit-error rates in excess of 80 %. These performance metrics unequivocally demonstrate the system's ability to reduce LTE receiver SNR below operational thresholds, thereby denying service within a practical radius of approximately 5–10 m under ideal conditions.

In discussing practical limitations, we noted challenges related to manual tuning, environmental attenuation, and regulatory constraints, underscoring the need for digitally controlled frequency agility and compliance mechanisms. We identified future research avenues including hybrid analog-digital integration, expansion to 5G NR or Wi-Fi bands, and directional beamforming that promise to enhance both functionality and legal viability.

REFERENCES

[1] H. Magri, A. Noreddine and O. Mohammed, "4G System: Network Architecture and Performance", *International Journal of Innovation Research in Advanced Engineering*, pp. 1-8, 2015.

[2] H.R. Suma, R.M. Vijayaprakash and K.G. Sunil, "Advancements and Impact of 4G Communication: A Technological Revolution", *World Journal of Advanced Research Reviews*, Vol. 2, No. 1, pp. 70-76, 2019.

[3] P. Hossein and Z. Huacheng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey", *IEEE Communications Surveys and Tutorials*, Vol. 24, No. 2, pp. 767-809, 2021.

[4] P. Bibhu, S. Balaji, G. Lolugu, K.P. Tulsi and S.K. Simhadri, "Design and Simulation of Mobile Signal Jammer Circuit", *International Research Journal of Engineering and Technology*, Vol. 11, No. 4, pp. 704-708, 2024.

[5] C.T. Sai, A.G. Dinesh Jumar, V. Charan and R. Sekar, "Design of Automated Dual B and 4G Jammer using MATLAB Simulink", *Indian Journal of Science and Technology*, Vol. 9, No. 37, pp. 1-7, 2016.

[6] L. Marc, R. Jeffrey, C. Charles and N. Mark, "Vulnerability of LTE to Hostile Interference", *IEEE Global Conference on Signal and Information Processing*, pp. 1-6, 2013.

[7] J.P. Roger, L. Joshua and R. Arvind, "Enhancing the Security of LTE Networks against Jamming Attacks", *EURASIP Journal on Information Security*, Vol. 1, No. 7, pp. 1-14, 2014.

[8] M. Vuk, R. Raghunandan, H. Sean and R. Jeffrey, "Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference", *Proceedings of International Conference on Vehicular Technology*, pp. 1-5, 2017.

[9] H.S. Gamal, M.S. Ehab and S.A.L. Mohamed Samir, "The Impact of Diverse Jamming Schemes against LTE-based Remote Detonation Devices", *Wireless Personal Communications*, Vol. 137, pp. 1773-1795, 2024.

[10] C. Cristian, P. Madalin, B. Eduard-Marian, H. Simona, F. Octavian and P. Mircea, "Intelligent Jammer on Mobile Network LTE Technology: A Study Case in Bucharest", *Applied Sciences*, Vol. 13, No. 22, pp. 1-35, 2023.

[11] G. Jacques, L. Bary, R. Jacques and J.G. Tartarin, "Assessing Zener-Diode-Structure Reliability from Zener Diodes' Low-Frequency Noise", *IEEE Transactions on Device and Materials Reliability*, Vol. 7, No. 3, pp. 468-472, 2007.

[12] A. Goetzberger, B. McDonald, R.H. Haitz, R.M. Scarlett, "Avalanche Effects in Silicon p-n Junctions II. Structurally Perfect Junctions", *Journal of Applied Physics*, Vol. 34, pp. 1591-1600, 1963.

[13] Horowitz and Hill, "*Art of Electronics*", 2015.

[14] Rohde and Schwarz, "LTE UE Receiver Performance", Available at https://www.rohde-schwarz.com/us/applications/lte-ue-receiver-performance-measurements-white-paper_230854-472779.html, Accessed in 2017.

[15] "NE612", Wikipedia, Available at https://en.wikipedia.org/wiki/NE612, Accessed in 2025.

[16] "Varicap", Wikipedia, Available at https://en.wikipedia.org/wiki/Varicap, Accessed in 2025.

[17] W. Olivier and M. Roland, "LTE: System Specifications and their Impact on RF and Base Band Circuits", Available at https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma221/1MA221_0e.pdf, Accessed in 2025.

[18] L. He, Z. Yan and M. Atiquzzaman, “LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement”, *IEEE Access*, Vol. 6, pp. 4220-4242, 2018.

[19] Cirexsa, “Cell Phone Jammers Legal in UK Schools?”, Available at https://www.reddit.com/r/LegalAdviceUK/comments/d872kz/cell_phone_jammers_legal_in_uk_schools/, Accessed in 2025.

[20] “Legality of Jammers around the World”, Phantom Technologies, Available at https://phantom-technologies.com/legality-of-jammers/, Accessed in 2025.