

Lujain Alsweed, Fatima Aldhowayan, Layan Alhmari, Rawan Aljuwayid, Aryam Alotibi, Asrar Alenezi, Batool Aljaiussy
Eng. Malak Neyazi Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, P.O. Box ⁸⁴⁴²⁸, Riyadh 11671, Saudi Arabia

Abstract

Wireless communication systems are more vulnerable to jamming and interference attacks that disrupt signal transmission and degrade reliability. This project proposes an intelligent Software Defined Radio (SDR) system with Artificial Intelligence for secure and reliable wireless communication. The proposed system continuously analyses the conditions of the signals detects the interference in real time and adaptively responds to maintain the communication performance. In addition the encryption module is designed to improve data confidentiality and reduce unauthorised interception. The system was simulated and tested in different jamming conditions using GNU Radio and Python. The results showed improved signal stability, lower BER, and more reliable communication compared to conventional systems.

Introduction / Background

Wireless communication systems are challenged by interference and intentional jamming, which reduce signal quality and data accuracy. This study presents an AI-driven adaptive Software-Defined Radio (SDR) system that uses cognitive radio techniques for real-time jamming detection and mitigation. The system combines BPSK modulation, XOR-based Physical Layer Security (PLS), and FFT-based spectrum analysis to provide secure and reliable communication. Performance was assessed in three jamming scenarios using Bit Error Rate (BER), Signal-to-Noise Ratio (SNR), and Jamming-to-Signal Ratio (JSR) metrics. Results show that the proposed system increases spectrum efficiency, improves communication reliability, and strengthens physical-layer security compared to conventional methods.

System Model / Methodology

- GNU Radio and SDR Simulation:**
The GNU Radio platform is used to simulate the SDR transmitter and receiver, support real-time digital signal processing and communication link modeling.
- Python-Driven AI Engine:**
An AI engine developed using Python automates system decision-making and implements autonomous frequency hopping by interacting with the flowgraph through XMLRPC.
- Spectrum Sensing:**
A dedicated module continuously monitors the spectral activity to identify jamming interference and to measure channel quality metrics.
- Encryption Module:**
Data confidentiality is maintained using XOR based physical layer encryption to prevent any unauthorized interception of the transmitted bit stream.
- Performance Analytics and Visualization:**
Real time analysis is performed using QT GUI sinks and the Error Rate block, enabling precise measurement of Bit Error Rate (BER) and signal constellations under simulated AWGN and jamming channel conditions.

Frequency	Jammer	BER(No AI)	BER(With AI)
15kHz	0.0	0.000	0.000
15kHz	0.5	0.020	0.002
15kHz	0.7	0.030	0.004
15kHz	1.5	0.270	0.005
15kHz	2.0	0.330	0.003

Table 1. Sample BER comparison at 15 kHz as a representative frequency under varying jammer levels.

Proposed Solution / Main Idea

When a jamming attack occurs, a fixed-frequency communication system continues transmitting on the same vulnerable channel, which makes the link easier to disrupt. Our solution is a simulated AI-based SDR system that senses interference and reacts adaptively, making the communication link more flexible and resilient under jamming conditions.

The system combines an SDR transmitter and receiver with spectrum sensing and a lightweight AI decision engine. It monitors communication quality using BER, SNR, and JSR to identify jamming conditions and support adaptive frequency selection, helping maintain more reliable signal performance in a simulated environment.

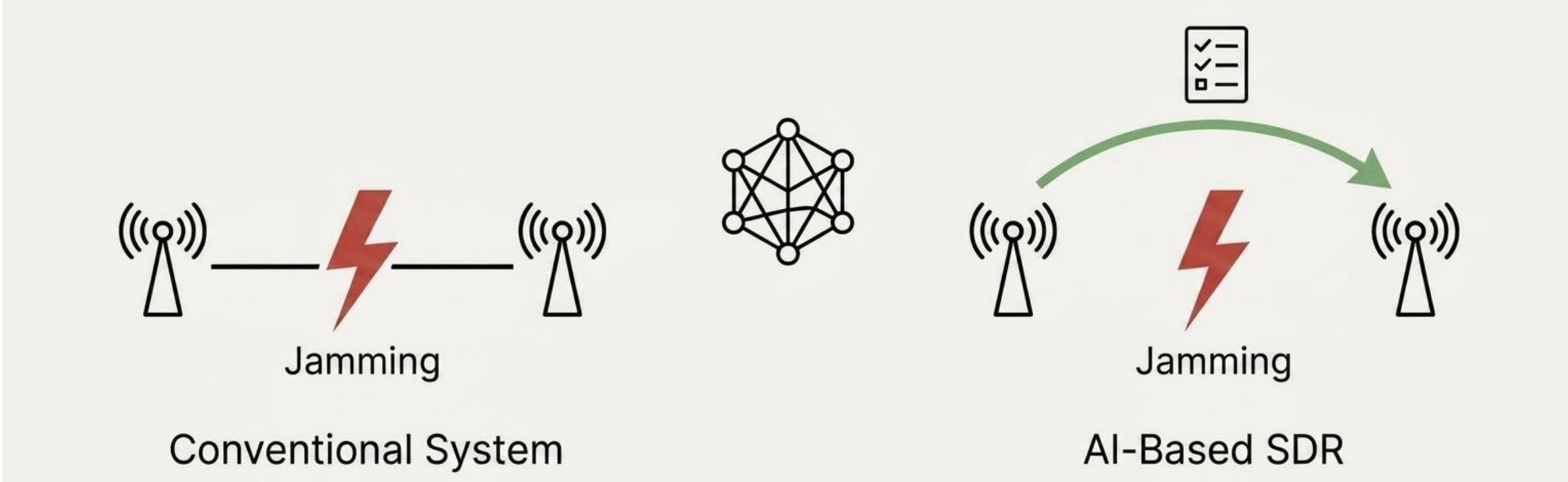


Figure 1. Comparison between Conventional and AI-Based SDR Systems

Results / Simulation / Discussion

The proposed AI-assisted SDR system was tested under different jammer strengths and operating frequencies. The conventional system showed severe BER degradation as interference increased, reaching approximately 0.35 under strong jamming, indicating system failure.

In contrast, the rule-based adaptive engine detected interference and automatically switched to cleaner channels using adaptive frequency hopping, maintaining BER below 0.01 across all conditions. XOR encryption further enhanced communication security without affecting performance.

Overall, the AI-assisted SDR significantly improved reliability and resistance against jamming compared to the conventional system.

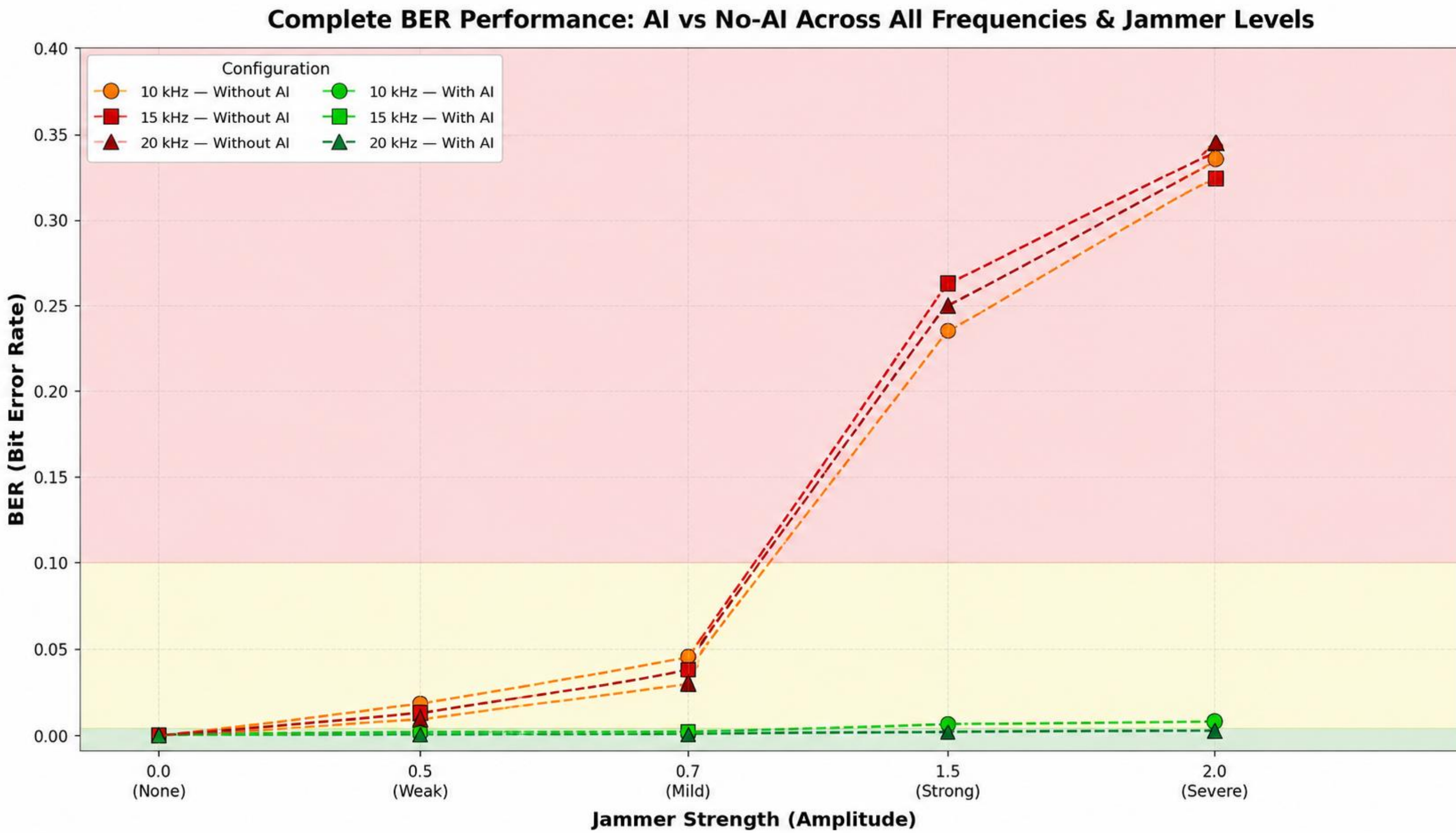


Figure 2. BER performance between AI vs. non-AI under different jammer levels and frequencies.

Conclusions

In this project, we proposed an AI-assisted SDR system designed to combat jamming attacks through adaptive frequency hopping and spectrum sensing.

The system integrates GNU Radio simulation, a Python-driven AI engine, spectrum sensing, XOR encryption, and real-time performance analytics to create a resilient communication link. Results demonstrated that the conventional system suffered severe BER degradation up to 0.35 under strong jamming, while the AI-based system maintained BER below 0.01 across all jammer strengths and across different operating frequencies.

The AI engine successfully detected interference and autonomously switched to cleaner channels without compromising security or performance.

Future work includes deploying the system on physical SDR hardware and testing under real-world jamming environments to further validate its robustness.