Contribution ID: **143**   Type: **Poster**

JAMMING RESPONSE SYSTEM (THEORETICAL)

Jamming is a deliberate attempt to disrupt wireless communication by transmitting interfering signals on specific frequencies. With the growing reliance on wireless systems in critical infrastructures, the threat of malicious signal interference has become a major concern for security and defense. Traditional jamming devices block communication across wide frequency ranges, but this often results in excessive collateral disruption. This paper focuses on the design of a Jamming Response System (JRS) using microcontroller-based architectures that introduces an adaptive and directional approach to signal jamming. The system analyses the frequency spectrum, detects suspicious activity, and activates targeted jamming only upon confirmation of a threat. This paper covers techniques such as frequency monitoring, dynamic frequency locking, adaptive filtering, power modulation, and directional antenna control for precision jamming. Recent advancements such as machine learning-based anomaly detection are also discussed to enable the system to differentiate between benign and malicious transmissions. The goal of this paper is to provide a theoretical design and simulation framework for intelligent and responsible jamming systems, highlighting their applications in cybersecurity, military defense, and critical infrastructure protection. Comparative discussion of adaptive jamming with conventional jamming methods is also included.

Authors: Mr B, Adhiyaman (M.Sc.DFIS); Ms REBECCA, Carol (M.Sc. DFIS); .O, Suvetha (M.Sc. DFIS)

Co-author: Mr VENKATESH, Vishnu (Assistant Professor)

Presenter: .O, Suvetha (M.Sc. DFIS)

Track Classification: Forensic Sciences