ABSTRACT

Wireless Sensor Networks (WSNs) are increasingly used in critical communication systems but remain vulnerable to various cyber-attacks, particularly virtual jamming. Unlike traditional jamming, virtual jamming targets the Medium Access Control (MAC) layer by exploiting the RTS/CTS mechanism to create silent denial-of-service attacks without emitting detectable interference. This study presents a hybrid deep learning approach using Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) networks to detect such attacks based on sequential traffic behavior.

Simulated traffic data was generated using NS2, capturing both normal and jamming behaviors. Temporal features were extracted and segmented using various sliding window sizes to train and evaluate the model. The proposed GRU-LSTM architecture was compared against traditional classifiers, particularly Support Vector Machines (SVM), and evaluated using accuracy, precision, recall, and F1-score.

Results show that the GRU-LSTM model achieved a peak accuracy of 99.00%, significantly outperforming the SVM baseline. The findings confirm the model's capability to capture subtle sequential patterns in network traffic and distinguish malicious behavior from legitimate activity. This research highlights the potential of deep sequential learning for robust, real-time intrusion detection in WSNs.

Keywords: Virtual jamming, wireless sensor networks, GRU-LSTM, deep learning, intrusion detection, RTS/CTS, sequential classification.