ABSTRAK

Jaringan Sensor Nirkabel (Wireless Sensor Networks/WSNs) banyak digunakan dalam sistem komunikasi kritis, namun tetap rentan terhadap berbagai serangan siber, khususnya serangan jamming virtual. Berbeda dengan jamming konvensional, jamming virtual menyerang lapisan Medium Access Control (MAC) dengan mengeksploitasi mekanisme RTS/CTS untuk menciptakan gangguan komunikasi tanpa menghasilkan interferensi fisik yang terdeteksi. Penelitian ini mengusulkan pendekatan pembelajaran mendalam hibrida menggunakan jaringan Gated Recurrent Unit (GRU) dan Long Short-Term Memory (LSTM) untuk mendeteksi serangan tersebut berdasarkan perilaku lalu lintas jaringan secara berurutan.

Data simulasi lalu lintas jaringan dihasilkan menggunakan NS2, mencakup aktivitas normal dan jamming. Fitur temporal diekstraksi dan disegmentasi menggunakan berbagai ukuran jendela geser (sliding window) untuk melatih dan mengevaluasi model. Arsitektur GRU-LSTM yang diusulkan dibandingkan dengan metode klasifikasi tradisional seperti Support Vector Machine (SVM), dan dievaluasi berdasarkan metrik akurasi, presisi, recall, dan F1-score.

Hasil menunjukkan bahwa model GRU-LSTM mencapai akurasi puncak sebesar 99.00% dan secara signifikan mengungguli model SVM. Temuan ini membuktikan kemampuan model dalam mengenali pola temporal halus pada lalu lintas jaringan dan membedakan perilaku jahat dari aktivitas normal. Penelitian ini menunjukkan potensi kuat pembelajaran sekuensial dalam mendeteksi intrusi secara real-time pada jaringan sensor nirkabel.

Kata kunci: Jamming virtual, jaringan sensor nirkabel, GRU-LSTM, pembelajaran mendalam, deteksi intrusi, RTS/CTS, klasifikasi sekuensial.