ABSTRACT

The rapid growth of Internet of Things (IoT) ecosystems has introduced significant cybersecurity challenges, particularly regarding Distributed Denial of Service (DDoS) and other network intrusion attacks. This study proposes an anomaly-based intrusion detection system (AIDS) integrating Analysis of Variance (ANOVA) F-test feature selection with a Multilayer Perceptron (MLP) deep learning architecture with scenario multiclass attack classification on the Bot-IoT dataset. From total of 42 feature available, ANOVA selected the 10 most important features, reducing dimensionality by 71.4% while achieving a Macro F1-Score of 86.07%, which surpassing the full-feature model's 83.90%. The proposed model with 46,085 parameters demonstrated competitive performance against other feature selection methods, while requiring only 1.4 seconds for feature computation compared to 772.9 seconds for wrapper-based approaches. These results suggest that ANOVA-based feature selection offers a favorable balance between classification performance and computational efficiency for resource-constrained IoT environments.

Keywords: Internet of Things, Intrusion Detection System, ANOVA Feature Selection, Multilayer Perceptron, Bot-IoT Dataset, Network Security.