ABSTRACT

With the advanced trends in pervasive computing, the data users face different kinds of attacks. Several algorithms for attack detection are performed with minimal accuracy in prediction and consideration of performance metrics was not effective. Hence effective and prompt detection of malicious attacks must be optimized in terms of confidentiality, privacy, availability and integrity. Accordingly, the proposed research provides an effective mechanism for detecting and classifying DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slow Loris Slow Post and Brute Force attack, by utilizing machine learning methods within the UNSW-NB15 dataset and NSL-KDD dataset. Significantly, Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging (GRU-BWFA) classifier is utilized as a proposed classifier approach for high detection rate and accuracy in distinguishing the mentioned DDoS attacks. Feature selection is performed using the Enhanced Salp Swarm Optimization technique to select the optimal features for identifying the attacks. The proposed classifier evaluates the other different classifiers which provide a detailed study in detecting DDoS attacks using the UNSW-NB15 dataset and NSL-KDD dataset. The proposed model results 0.9936 accuracy for UNSW-NB 15 dataset and 0.9918 accuracy for NSL-KDD dataset. Empirical findings indicate that the machine learning methods are highly effective at detecting and classifying attacks with a higher accuracy rate.

With the advancing trends in the field of information technology, the data users are subjected to face different attacks. Hence effective and prompt detection of malicious attacks must be optimized in terms of confidentiality, privacy, availability and integrity. Accordingly, this work provides an effective mechanism for detecting and classifying DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris Slow Post and Brute Force attack, by

utilizing machine learning methods within SNMP-MIB dataset. MIB (Management Information Base) is meant for attack classification database linked to the SNMP (Simple Network Management protocol). Three classifiers are considered such as MLP, Random Forest, Ada boost to construct the detection model. Significantly, Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging (GRU-BWFA) classifier is utilized as a proposed classifier for high detection rate and accuracy in distinguishing the mentioned DDoS attacks. Feature selection is performed using the Enhanced Salp Swarm Optimization technique to select the optimal features for identifying the attacks. The application of various classifier provides a detailed study on the effectiveness of SNMP-MIB dataset in detecting DDoS attacks. Empirical findings indicate that the machine learning methods are highly effective at detecting and classifying the attacks with a higher accuracy rate.