ABSTRACT

The advancement of modern network architecture encourages the adoption of Software Defined Networking (SDN) as a flexible and adaptive solution to dynamic changes and cybersecurity threats. One prominent challenge is the Denial of Service (DoS) attack, particularly the Ping of Death (PoD) type, which can disrupt network systems by continuously sending oversized Internet Control Message Protocol (ICMP) packets. This research aims to implement a dynamic SDN-based Firewall integrated with a Support Vector Machine (SVM) algorithm to detect and mitigate PoD using Firewall automatically within 15 seconds. Experiments were conducted using the Mininet emulator on Ubuntu Linux within a VMware virtual environment. The Ryu Controller was utilized to manage decision-making processes and enforce Firewall rules based on traffic classification. ICMP traffic was captured and analyzed to train the SVM model, which was then used for real-time detection. Upon identifying an attack pattern, the system automatically blocked the attacker's IP address using the Blacklisting method. The system was tested under normal conditions and during simulated attacks by evaluating performance parameters such as Round-Trip Time (RTT). The results of the study show that the integration of SDN Firewall and SVM classification through accuracy calculations on the confusion matrix shows that the evaluation accuracy value reaching more than 97% have positive effectiveness in detecting and minimizing the impact of PoD attacks. The system successfully maintains overall network performance without significantly affecting normal traffic. This research contributes to the development of adaptive and automated network security systems based on SDN and machine learning.

Keywords: ***SDN, DoS, Ping of Death, Firewall, SVM, Blacklisting, Ryu Controller***