

Deteksi Serangan DoS Pada Jaringan SDN Berbasis P4 Programmable Dataplane menggunakan Machine Learning

Sya Raihan Heggi¹, Parman Sukarno², Satria Akbar Mugitama

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

¹heggiraihan@students.telkomuniversity.ac.id, ²psukarno@telkomuniversity.ac.id,

³satriamugitama@telkomuniversity.ac.id

Abstract

This thesis proposes LSTM-NB, a combination of Long Short-Term Memory (LSTM) and Naive Bayes (NB) algorithms to tackle Denial of Service (DoS) attacks on Programming Protocol-independent Packet Processors (P4) language-based Software Defined Network (SDN). The implementation of SDN is becoming more popular. However, there are critical aspects of the SDN architecture, one of which is that it is vulnerable to DoS attacks that can cause the network to lose the availability principle of the CIA Triangle. There are a number of works have been proposed to overcome this vulnerability, however, the threat is still exist. The proposed technique achieves an accuracy of 88% on SDN-DL Dataset, 98% on NSL-KDD, and 96% on CICIDS2017 with FNR score between 1-2%. In addition, we compare our proposed technique with other machine-learning and deep-learning methods. Through extensive experimental evaluation, we conclude that our proposed approach exhibits a strong potential for DoS detection in the SDN environments.

Keywords: Computer Network Security, Intrusion Detection System (IDS), Machine Learning, Deep Learning, Denial of Service (DoS)
