JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH
E-ISSN: 2980-9231
https://jce.bushehr.iau.ir
https://doi.org/...

Vol. 14/ No. 53/Autumn 2024

Research Article

Detection of DDoS Attacks in SDN Switches with Deep Learning and Swarm Intelligence Approach

Mohsen Eghbali, PhD Student[1] | Mohammad Reza Mollakhalili Meybodi, Assistant Professor[2*]

[1]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, m.eghbali@maybofiau.ac.ir

[2]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, mr.mollahoseini@iau.ac.ir

Correspondence
Mohammad Reza Mollakhalili Meybodi, Associate Professor of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, mollakhalili@maybodiau.ac.ir

Received: 16 October 2023
Revised: 2 December 2023
Accepted: 17 December 2023

Abstract

Internet of Things nodes infected with various types of malware and any smart device can appear as a botnet attacking node. The challenge of most intrusion detection systems in the Internet of Things is the need for intelligent feature selection and the imbalance of the training data set and centralization. In this article, an efficient intrusion detection system for the Internet of Things based on the distributed architecture of the SDN network is presented. In the proposed method, the data set is balanced using the SMOTE method in the first stage. Then in the second stage, the essential features are selected using the African vulture optimization algorithm. In the third step, the LSTM deep learning method is trained in the SDN controller so that the switches of the SDN network use this trained model to detect attacks. In the proposed method, the addresses of attacking nodes are shared between SDN switches so that the attacking node is recognized as an attacking node in all switches and DDoS attacks are stopped. Experiments running in the MATLAB environment and the NSL-KDD dataset and the results of the experiments show that the proposed method in detecting attacks has accuracy, sensitivity, and precision of 99.34%, 99.16%, and 98.93%. The proposed method is more accurate in detecting DDoS attacks than the feature selection methods based on WOA, HHO, and AO algorithms. The proposed method for detecting DDoS attacks is more accurate than deep learning methods such as LSTM, RNN, and CNN.

Keywords: Internet of Things, Intrusion detection system, DDoS attacks, SDN network, Deep learning.

Highlights

- Providing a distributed intrusion detection system based on SDN architecture.
- Data set balancing using SMOTE method in SDN controller.
- Presenting a feature selection and binary version of the African vulture algorithm in detecting attacks.
- Combining group intelligence and LSTM deep learning in SDN network to detect attacks in Internet of Things.

Citation: (in Persian).