



Make Submissions

Propose a Special Issue

Vol.73, No.2, 2022

Views 116
PDF Downloads 78

Download & Citation

- Full-Text PDF
- Full-Text HTML
- Full-Text XML
- Full-Text Epub

Citation Tools

- BibTex
- EndNote
- RIS

Vol.73, No.2, 2022, pp.3099-3118, doi:10.32604/cmc.2022.028285 OPEN ACCESS ARTICLE

R-IDPS: Real Time SDN-Based IDPS System for IoT Security

Noman Mazhar^{1,2}, Rosli Saleh^{1,*}, Reza Zaba^{1,3}, Muhammad Zeeshan⁴, M. Muzaffar Hameed¹, Nauman Khan¹

1 Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, 50603, Malaysia

2 Centre for Research in Industry 4.0, University of Malaya, Kuala Lumpur, 50603, Malaysia

3 MIMOS Berhad, National Applied R&D Centre, Kuala Lumpur, 57000, Malaysia

4 School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, 44000, Pakistan

* Corresponding Author: Rosli Saleh. Email: rosli_salleh@um.edu.my

Received 06 February 2022; Accepted 07 April 2022; Issue published 16 June 2022

[Download PDF](#) [View HTML](#)

Abstract

The advent of the latest technologies like the Internet of things (IoT) transforms the world from a manual to an automated way of lifestyle. Meanwhile, it opens numerous security challenges. In traditional networks, intrusion detection and prevention systems (IDPS) have been the key player in the market for IoT security. The challenges to the conventional IDPS are implementation cost, computing power, processing delay, and scalability. Further, online machine learning model training has been an issue. All these challenges still question the IoT network security. There has been a lot of research for IoT based detection systems to secure the IoT devices such as centralized and distributed architecture-based detection systems. The centralized system has issues like a single point of failure and load balancing while distributed system design has scalability and heterogeneity hassles. In this study, we design and develop an agent-based intrusion prevention system based on software-defined networking (SDN) technology. The system uses lightweight agents with the ability to scale up for bigger networks and is feasible for heterogeneous IoT devices. The baseline profile for the IoT devices has been developed by analyzing network flows from all the IoT device profiles helps in extracting IoT device features. These features help in the development of our dataset that we use for anomaly detection. For anomaly detection, support vector machine has been used to detect internet control message protocol (ICMP) flood and transmission control protocol synchronize (TCP SYN) attacks. The proposed system based on machine learning model is fully capable of online and offline training. Other than detection accuracy, the system mitigates the attacks using the software-defined technology SDN technology. The major goal of the research is to analyze the accuracy of the hybrid agent-based intrusion detection systems as compared to conventional centralized only solutions, especially under the flood attack conditions generated by the distributed denial of service (DDoS) attacks. The system shows 97% to 99% accuracy in simulated results with no false-positive alarm. Also, the system shows notable improvement in terms of resource utilization and performance under attack scenarios. The R-IDPS is scalable, and the system is suitable for heterogeneous IoT device networks.

Keywords

Machine learning; Internet of things; software defined networking; distributed denial of service attacks

Cite This Article

[BibTex](#) [EndNote](#) [RIS](#)

N. Mazhar, R. Saleh, R. Zaba, M. Zeeshan, M. Muzaffar Hameed *et al.*, "R-idps: real time sdn-based idps system for iot security," *Computers, Materials & Continua*, vol. 73, no.2, pp. 3099–3118, 2022.



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We recommend

Hybrid Deep Learning Based Attack Detection for Imbalanced Data Classification

Almarshdi Rasha *et al.*, *Intelligent Automation & Soft Computing*, 2022

Detecting Man-in-the-Middle Attack in Fog Computing for Social Media

Farouq Aliyu *et al.*, *CMC-Computers, Materials & Continua*, 2021

Towards Machine Learning Based Intrusion Detection in IoT Networks

Nahida Islam *et al.*, *CMC-Computers, Materials & Continua*, 2021

An Efficient Internet Traffic Classification System Using Deep Learning for IoT

Muhammad Basit Umair *et al.*, *CMC-Computers, Materials & Continua*, 2021

SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)

Azka Wani *et al.*, *CAAI Transactions on Intelligence Technology*, 2021

A blockchain future for internet of things security: a position paper

Mandrita Banerjee *et al.*, *Digital Communications and Networks*, 2018

A model to classify cyberattacks using swarm intelligence

Ingrid Fadelli *et al.*, *TechXplore.com*, 2019

Challenge-based collaborative intrusion detection in software-defined networking: an evaluation

Wenjuan Li *et al.*, *Digital Communications and Networks*, 2021

Survey on Internet of Things Based on Named Data Networking Facing 5G

Powered by **TREND MD**

Further Information

[About Tech Science Press](#)
[Open Access Policy](#)
[Article Processing Charges](#)
[Terms and Conditions](#)
[Privacy Policy](#)
[Advertising Policy](#)
[Contact TSP](#)

Guidelines

[For Editors](#)
[For Reviewers](#)
[For Authors](#)
[For Conference Organizers](#)
[For Subscribers](#)

Contact Us

871 Coronado Center Drive, Suite 200, Henderson,
Nevada, 89052, USA
[General Contact](#)
Email: office@techscience.com
[Office Locations](#)

Copyright© 2020 Tech Science Press

© 1997-2020 TSP (Henderson, USA) unless otherwise stated

