Computers, Materials & Continua

Vol.73, No.2, 2022

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 Zeeshan[4], M. Muzaffar Hameed[1], Nauman Khan[1]

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

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, l open numerous security challenges. In traditional networks, intrusion detection and prevention systems (IDPS) have been the key player in the market f security. The challenges to the conventional IDPS are implementation cost, computing power, processing delay, and scalability. Further, online machine 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 sy secure the IoT devices such as centralized and distributed architecture-based detection systems. The centralized system has issues like a single point and load balancing while distributed system design has scalability and heterogeneity hassles. In this study, we design and develop an agent-base prevention system based on software-defined networking (SDN) technology. The system uses lite weight agents with the ability to scaleup for bigger netw is feasible for heterogeneous IoT devices. The baseline profile for the IoT devices has been developed by analyzing network flows from all the IoT devi profile helps in extracting IoT device features. These features help in the development of our dataset that we use for anomaly detection. For anomaly d support vector machine has been used to detect internet control message protocol (ICMP) flood and transmission control protocol synchronize (TCP S attacks. The proposed system based on machine learning model is fully capable of online and offline training. Other than detection accuracy, the system mitigate the attacks using the software-defined technology SDN technology. The major goal of the research is to analyze the accuracy of the hybrid age intrusion detection systems as compared to conventional centralized only solutions, especially under the flood attack conditions generated by the distribut of service (DDoS) attacks. The system shows 97% to 99% accuracy in simulated results with no false-positive alarm. Also, the system shows notable imp in terms of resource utilization and performance under attack scenarios. The R-IDPS is scalable, and the system is suitable for heterogeneous IoT dev networks.

Keywords

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

An Intrusion Detection System for SDN Using Machine Learning XIE Ying-ying et al., Computer Science, 2020
Logeswari G. et al., Intelligent Automation & Soft Computing, 2022