Tekleselassie H, J Comput Eng Inf Technol
2020, 9:6 DOI: 10.37532/jceit.2020.9(6).242

Journal of Computer Engineering & Information Technology

Short communication

A SciTechnol Journal

DDoS attacks detection on internet of things using unsupervised machine learning algorithms

Hailyie Tekleselassie*

The increase in the deployment of IoT networks has improved productivity of humans and organisations. However, IoT networks are increasingly becoming platforms for launching DDoS attacks due to inherent weaker security and resource-constrained nature of IoT devices. This paper focusses on detecting DDoS attack in IoT networks by classifying incoming network packets on the transport layer as either "Suspicious" or "Benign" using unsupervised machine learning algorithms. In this work, two deep learning algorithms and two clustering algorithms were independently trained for mitigating DDoS attacks. We lay emphasis on exploitation based DDOS attacks which include TCP SYN-Flood attacks and UDP-Lag attacks. We use Mirai, BASHLITE and CICDDoS2019 dataset in training the algorithms during the experimentation phase. The accuracy score and normalized-mutual-information score are used to quantify the classification performance of the four algorithms. Our results show that the autoencoder performed overall best with the highest accuracy across all the datasets.

The increment of sensors and computing devices have made life easy and convenient for us due to the fast and accurate computation of our information. However, increased integration and deployment of connected devices also exposes essential resources to DDoS threats. In 2016, the Mirai attack that destroyed many popular websites really exposed the weakness of IoT devices.

Over 100,000 inadequately secured player, cameras, digital video recording and other IoT devices were turned into botnets for starting an extraordinary Terabytes per seconds (Tbps). DDoS attack through the Mirai. The Mirai source code that was further released resulted in frequent additional IoT attacks. With the magnitude of attacks that have been launched, securing IoT devices is a problem as host-centric IT security solutions cannot be totally relied upon because most manufacturer's appliances place more priority on functionality and cost over security. Besides, unlike servers that can undergo software update, IoT software is hardly or never updated, hence making them more vulnerable to attackers. In view of these security problems and resource-constrained nature of IoT devices, greater focus should be placed on packet security within the IoT network.

Traditional network-centred security has relied on predefined signature or system models for known threats. Recently, there has been a rising awareness in machine learning (ML) to network security. However, many ML solutions use supervised learning i.e. they build attack classifiers by training on known anomalies, which makes them ineffective against new threats. The main aim of this work to determine the performance of unsupervised learning algorithms in accurately classifying network packets as either benign or malicious. We achieve this by training the algorithms on modern DDOS datasets and performing rigorous testing while benchmarking the performance of the algorithms using standard performance metrics.

Citation: Tekleselassie H (2020) DDoS attacks detection on internet of things using unsupervised machine learning algorithms J Comput Eng Inf Technol 9:6 .DOI: 10.37532/jceit.2020.9(6).242

***Corresponding author:** Hailyie Tekleselassie, Department of Information Systems, School of Informatics, Wolaita Sodo University, Ethiopia Tel: + 0923700484; E-mail: hailye.tekleselase@gmail.com

Received: November 30, 2020 **Accepted:** December 16, 2020 **Published:** December 23, 2020

Author Affiliation Top

Department of Information Systems, School of Informatics, Wolaita Sodo