BOTNET DETECTION USING DEEP LEARNING APPROACHES

Master of Science

Cyber Security

UWE, Bristol, January 2022

Kiran Kumar Mohanraj

ABSTRACT

With the proliferation of the Internet of Things (IoT), computer networks have rapidly expanded in size. While Internet of Things Devices (IoTDs) benefit many aspects of life, these devices also introduce security risks in the form of vulnerabilities which give hackers billions of promising new targets. For example, botnets have exploited the security flaws common with IoTDs to gain unauthorized control of hundreds of thousands of hosts, which they then utilize to carry out massively disruptive distributed denial of service (DDoS) attacks. Traditional DDoS defense mechanisms rely on detecting attacks at their target and deploying mitigation strategies toward the attacker but differentiating between botnet attack traffic from normal traffic is extremely difficult, rendering mitigation strategies ineffective. An expanding body of work seeks to sidestep this difficulty by using sophisticated machine learning algorithms to detect botnet-basedattacks at their source; however, many of these algorithms are computationally demanding and require specialized hardware, which is expensive, rendering them impractical. In this study, Deep Residual Convolutional Neural Network (CNN) model, was proposed to detect botnet attacks, namely, BASHLITE and Mirai, on nine commercial IoT devices. Extensive empirical research was performed by employing a real N-BaIoT dataset extracted from a real system, including benign and malicious patterns. This study also implements Artificial Neural Network (ANN) Model and Convolutional Neural Network and Long Short-Term memory (CNN-LSTM) model to evaluate the proposed model. The experimental results exposed the superiority of the Deep Residual CNN model with accuracies of 87.27% in detecting botnet attacks from Provision PT-737E Security Camera, whereas the ANN and CNN-LSTM model showed 83.66% and 75.02% respectively. Overall, the Deep Residual CNN model was successful in detecting botnet attacks from various IoT devices with optimal accuracy.

KEYWORDS: convolutional neural networks, deep learning, distributed denial of service attacks, IoT security, long short-term memory, deep residual network.