Lightweight Internet of Things Botnet Detection Using One-Class Classification

ABSTRACT

Like smart phones, the recent years have seen an increased usage of internet of things (IoT) technology. IoT devices, being resource constrained due to smaller size, are vulnerable to various security threats. Recently, many distributed denial of service (DDoS) attacks generated with the help of IoT botnets affected the services of many websites. The destructive botnets need to be detected at the early stage of infection. Machine-learning models can be utilized for early detection of botnets. This paper proposes one-class classifier-based machine-learning solution for the detection of IoT botnets in a heterogeneous environment. The proposed one-class classifier, which is based on one-class KNN, can detect the IoT botnets at the early stage with high accuracy. The proposed machine-learning-based model is a lightweight solution that works by selecting the best features leveraging well-known filter and wrapper methods for feature selection. The proposed strategy is evaluated over different datasets collected from varying network scenarios. The experimental results reveal that the proposed technique shows improved performance, consistent across three different datasets used for evaluation.