Abstract

With the increase in devices that are connected to the Internet underpinning the Internet of Things (IoT) is growing rapidly, but many of these devices are basically insecure, free exposure on the Internet and allow for a variety of attacks. Lately, IoT has been influenced by a variety of botnets with different activities including Distributed Denial of Service (DDoS) attacks, spamming, phishing, until infect other systems. Because botnet with these attacks has been the cause of a fairly serious security risk to the Internet infrastructure for years, there is no Network Forensics technique that can identify and track the behavior of sophisticated botnets to date. In other literature there have been studies that have used Machine Learning (ML) to train and validate modeling to define these attacks, but still produce high enough errors in investigating botnet traces. This motivated the development of new techniques for Networking Technology based on the identification of network flows that could track the traces of suspected botnet activities. Based on experimental results obtained Machine Learning (ML) combined with the identification of network flows is quite effective and efficient in identifying and classifying attacks and traces of botnet activity on the suspected Internet of Things (IoT).

Keywords: internet of things, cyber attack, botnet, network forensics, machine learning.