Chapter 16
Network-Based Detection of Mirai Botnet Using Machine Learning and Feature Selection Methods

Ahmad Al-Qerem
Zarqa University, Jordan

Bushra Mohammed Abutahoun
Princess Sumaya University for Technology, Jordan

Shadi Ismail Nashwan
https://orcid.org/0000-0002-1476-4162
Computer Science Department, Jouf University, Saudi Arabia

Shatha Shakhatreh
Princess Sumaya University for Technology, Jordan

Mohammad Alauthman
https://orcid.org/0000-0003-0319-1968
Zarqa University, Jordan

Ammar Almomani
https://orcid.org/0000-0002-8808-6114
Department of Information Technology, Al-Huson University College, Al-Balqa Applied University, Jordan

ABSTRACT

The spread of IoT devices is significantly increasing worldwide with a low design security that makes it more easily compromised than desktop computers. This gives rise to the phenomenon of IoT-based botnet attacks such as Mirai botnet, which have recently emerged as a high-profile threat that contin-

DOI: 10.4018/978-1-7998-2701-6.ch016

ues. Accurate and timely detection methods are required to identify these attacks and mitigate these new threats. To do so, this chapter will implement a network-based anomaly detection approach for the Mirai botnet using various machine learning and feature selection algorithms. Authors use Multiphase Genetic Algorithm section methods and PSO to select the best subfield of features capable of producing good overall classification results, and with this Feature Selection Algorithm, Random forest algorithm can detect all anomaly behavior with 100% accuracy.

INTRODUCTION

Internet of things (IoT)' is a platform where everyday devices become smarter, every day processing becomes intelligent, and every day communication becomes informative'(Ray, 2018). As the IoT devices contribute to everything and its number increasing very fast with the lake of security, which creates disaster attacks, the need for timely detection methods of IoT attacks becomes very important to promote IoT network security and prevent attacks from spreading. IoT is a new paradigm that looks forward to linking all the components of the physical world within the digital world under the idea of merging the 'things' that represent the world into software applications and the internet, making them communicating and benefit from the world's context information(Alauthman et al., 2019; Alauthman et al., 2020; Atzori et al., 2010; Gonzalez et al., 2008; Sterling, 2005). IoT technology is developing rapidly, it becomes the focus of the modern cities, and huge enterprises, and many applications have been built recently. As a new technology, it is facing a lot of challenges, and one of them is very important and crucial, which is security (Alauthaman et al., 2018; Xia et al., 2012).

IoT devices and systems are suffering from security and privacy issues that are the heart of everything (Lee & Kim, 2017) and have very high-risk vulnerabilities. They are spreading in the market with little consideration of basic security and privacy protections 'Insecurity by design'. Therefore, the proliferation and increasing popularity of the internet of things with its insecure large number of devices with high computational power and resources make them an easy, attractive, and powerful target for attackers seeking to compromise these devices and use them to make large-scale botnets. Botnets are robot networks of compromised or infected machines of malicious software that become controlled by a third party (Attacker); it uses the command-control infrastructure to accomplish different bad attacks like email spam delivery, identity theft and distributed denial of service attack (DDOS).DDOS attack crowd a huge number of machines (bots) to overwhelming the target website with many requests. Therefore, the target website will not be able to serve requests by actual and legitimate users. The weakness of security in IoT devices promotes such attacks and support them to be larger and more dangerous (Bertino & Islam, 2017).

Figure 1 shows the DDOS attack. In 2016, a website of computer security consultant Brian Krebs was hit with 620 Gbps of traffic; another attack happened after it attacks hundreds of websites including Twitter, Netflix, Reddit, and GitHub; In February 2017, DDOS attack happened against a US college and stayed 54 hours long and other dangerous attacks. Analyzing these massive DDOS attacks considered that IoT devices are contributing to these attacks, and that is the reason why it is so huge. They called this type of DDOS attack (Mirai) stands for the future(Shoemaker, 2017). This attack showed the importance of security, which has been missed in the IoT devices and causes disaster attacks. Mirai attack is taking the place of the hugest most dangerous effectively DDOS attacks which reaches an unprecedented level(Kolias et al., 2017).