ABSTRACT

With the rapid development of the Internet of Things (IoT) devices, the cyber-attacks are mostly targeting these devices. Almost all of the attacks in IoT environments are botnet-based attacks. Many security weaknesses still exist on these devices because most of these devices have not enough memory and computational resources to adequate with the robust security mechanism. The complex cryptographic mechanisms are challenging to embed in almost IoT devices, especially in portable devices. Moreover, many existing rule-based detection systems can be circumvented by malware attackers. This study is to get an effective system for detecting the most challenging attacks, especially on botnet attacks. This study mainly explores the machine learning methodologies to investigate the suitable mechanism for securing the IoT environments.

Machine learning-based systems have high resources demand to perform their tasks. Thus, their processing cannot be performed on the IoT devices nor the resource constraint devices. Consequently, it is needed to find the possible way the lightweight mechanism, even if the machine learning-based methodologies are used in the detection system. We propose a novel feature selection method to select the corresponding features from each kind of attack category. The proposed approach could support a selection of the most important features and keep the admirable detection accuracy. This could support to reduce the high demand for the computation resources for the machine learning processes. Moreover, an attack detection system with sequential architecture is proposed for IoT environments. It can support the detection system to have better accuracy and be easily extensible for detecting future upcoming attacks. Finally, it approves that the proposed detection system can be implemented on the resource constraint device.