 ISSN 2362-0412

Machine Learning and Data Mining Based Botnet Attack Detection Framework

O.A.S.P.O. Arachchi *, M.W.T.B. Aththanayake, L.L.G.M.P. Bandara
W.G.C.A. Sankalpa, K.L.K. Sudheera

[a]*Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle, Sri Lanka*

*Corresponding author: *eg162819@engug.ruh.ac.lk*

ABSTRACT

Internet of Things (IoT) provides an attractive surface for attackers to initiate large scale network attacks due to inherent vulnerabilities such as default usernames and passwords in the IoT devices. As can be seen by recent massive scale attacks such as Mirai, bots make use of this weakness to compromise vulnerable IoT devices and launch targeted attacks towards critical network infrastructure. Botnet attacks consist of multiple stages starting from scanning and progressing until specific attacks such as Distributed Denial of Service (DDoS). These individual stages leave traces in the underlying network traffic which can be extracted as patterns. To this end, we propose a framework that first extracts patterns from network traces using data mining and subsequently, trains a machine learning model to classify the extracted patterns to corresponding attack stages. The patterns are mined locally at gateways of each network and then, federated learning is used to train a global model at a centralized security manager by exchanging the weight parameters without violating the privacy concerns. We demonstrate the effectiveness of the proposed framework through multiple experiments using the OpenStack platform.

Keywords: *Association Rule, Botnet, Data Mining, Federated Learning, FIM*