Paper ID: MISS21_06

# Botnet Attack Detection in Iot Networking Environment Using Machine Learning Approach

D.V.Jeyanthi[1*], B.Indrani [2]

[1]Sourashtra College, Madurai, Tamil Nadu, India

[2]Madurai Kamaraj University, Madurai, Tamil Nadu, India

*Corresponding author

## Abstract

**Background:** Botnets have become one of the most significant dangers to cyber security since they are the main vehicle for most organized cybercrime. Cyber criminals now have a strong motivation to participate in harmful, profit driven unlawful behaviours on the internet. Botnets are a common technique used by cyber criminals nowadays. This has resulted in an increase in the number of new botnet threats, as well as many significant cyber security problems. Botnet has infected both desktop and mobile machines. Microsoft Windows is the most commonly used consumer operating system in the world, with desktop computers accounting for the majority of its use.

**Objective:** To identify IoT botnets at the network level, utilized a Feed Forward Neural Network training model that employs the Bold Driver Back propagation learning method. During the weight update process, the method has the benefit of dynamically adjusting the learning rate parameter.

**Methodology**: Machine learning techniques are used to evaluate IoT botnets and develop a detection system. The Apriori association rule mining algorithm is used to generate unique patterns (i.e. combinations of requested permissions and used features) based on malicious botnet activities, and the information gain method is used to select the most significant patterns in order to provide a better detection. The machine learning framework uses the chosen unique patterns to categorize the apps as benign or malicious. We utilized Android botnet data sets from a variety of sources, including the Android Malware Gnome project, Drebin, Droid Analytics, ISCX Android Botnet dataset, and a dataset from Beijing Jiao-tong University in China.

**Result and discussion:** As a result, a research and analysis of botnets impacting the above mentioned operating systems is conducted in the research in order to provide a better solution for detecting botnets and mitigating assaults. Experiments results shown on real world benchmark datasets indicate that the chosen patterns have high detection accuracy.

**Conclusion and Future work:** In future studies attempted to provide a logical answer to the crucial issue of IoT botnet identification. Machine Learning methods were employed to detect botnets after an analysis of numerous actual bots.


DOI: 10.21467/abstracts.120

ISBN: 978-81-954993-2-8