Vidyavardhini's College of Engineering and Technology

Android Botnet Detection using Machine Learning

Chetan Sapkal, Yash Patil , Shubhamkar Patra

Department of Artificial Intelligence and Data Science. Vartak Engineering College, Vasai, Maharashtra, India.

A B S T R A C T

A botnet is a widely spreading malware among mobile applications which is dangerous to mobile apps. Nowadays developers are widely using malicious software for fast development and good results, this leads to the spreading of botnet malware. A botnet mainly aims to hack the entire system and abduct the details of the user. By applying the proposed methodology and algorithms for the detection of botnets. By applying the Machine learning algorithm to the predefined datasets and got the conclusion of successfully testing against the dataset, and detecting some botnet-infected apps.

In machine learning-based botnet detection, various features are extracted from network traffic, such as packet size, protocol, and port number. These features are then used to train a machine learning model, such as a decision tree, support vector machine (SVM), or neural network, to classify network traffic as either botnet or legitimate.

One of the challenges in machine learning-based botnet detection is the imbalance between botnet and legitimate traffic data. Botnet traffic is relatively rare and difficult to obtain, while legitimate traffic data is abundant. To overcome this challenge, various techniques, such as oversampling and undersampling, are used to balance the dataset.

Smart technologies are used by developers and smartphone users rapidly in use these days. by using this technology, the threat is getting infected with malicious viruses like botnets. these viruses mainly attack android apps. some of the types of the famous types of attacks on the android app are increasing these days. the flow of this malware is to command and control the app's server. This mobile botnet runs automatically when it gets installed in the system without the antivirus. Mobile botnet obtains overall access to device change himself continuously. the overall methodology for the detection and prevention of mobile botnets is proposed in this paper. For testing against the apps, the ISCX dataset is used to detect the botnet-infected apps.

The overall system is built using python and Machine Learning models like SVM. Some python libraries are used in this system like Pandas, NumPy, Sci-Kit, Seaborn, etc.