CSE438
Task1
Paper Report

Name: Md Minhazul Islam Rimon
ID: 20101078
Section: 1

Paper Title

IoT Botnet Detection Based on Anomalies of Multiscale Time Series Dynamics

Paper Link

IoT Botnet Detection Based on Anomalies of Multiscale Time Series Dynamics | IEEE Journals & Magazine | IEEE Xplore

1 Summary

1.1 Motivation

The paper aims to detect anomalies created by different IoT devices when they are attacked by botnets. As we use different IoT devices around the house such as: doorbell, security camera, monitors etc, these devices are connected to the internet so that we may see the result on our devices such as computers or mobiles. Now, our personal devices are quite secure due to their complex architecture but the IoT devices are quite simple so they are prone to the botnet attack.

Due to the botnet attack on these devices, the devices act a bit differently then they used to. Even though they can perform their day to day tasks to some extent. In some cases, there are many unnecessary actions that they take. The goal of this paper is to identify those unnecessary tasks or anomalies and experiment if we can detect botnet attacks using this behavior pattern.

1.2 Contribution

The paper identifies the anomaly on IoT devices and proposes a model which can predict the anomaly behaviors which are caused by botnets with great accuracy as the time series increases. The model proposed is also efficient and requires less training time and allows plug and play.

1.3 Methodology

After acquiring an appropriate amount of dataset of IoT device behavior, the data is processed with ordinal pattern transformation and then with derived transformation. And then some numerical analysis is done on the data to get insight of the data and maintain a balanced data. Then kitsune unsupervised machine learning was used to the data set in 2 ways: one is one model for all category and other is one model for one category.

1.4 Conclusion

The paper establishes that it can detect botnet attacks based on the affected IoT device behaviors. The theory was already there but this paper used an efficient model and established the fact on few most used IoT devices we use at home.

2 Limitation

2.1 First Limitation

The scenario of the IoT device is too generalized. There might be different behavior in different situations and the author did not take that into consideration.

2.2 Second Limitation

The devices used to collect data are almost too similar and there is less difference between them. So we can say that the detection was done case specific and as there are many variations of modern devices, it fails to reflect that aspect.

Synthesis

Everyone in the current timeline is dependent on IoT devices. We are using them everyday to make our lives easier. Thus the tool to detect if the IoT devices were affected by any botnet attacks or not is really crucial as it will help them to realize when to maintain the crucial devices and ensure security and safety.