Temasek Defence Systems Institute

Temasek Defence Systems Institute

Using A K-Nearest Neighbours Machine Learning Approach to Detect Cyberattacks on the Navy Smart Grid

LTC Vincent Chan Chi Meng, Republic of Singapore Navy
Prof. Preetha Thulasiraman, ECE Dept., Naval Postgraduate School

Introduction

In 2013, the U.S. Naval Facilities Engineering Command (NAVFAC) formulated its plan for the Navy's own smart grid [1]. However, in placing the Navy's critical infrastructure on a network, both state and non-state actors will be particularly interested in what information they can learn, and what damage they can cause through these means. Different cyberattacks warrant different responses to maintain grid availability; the grid cannot be taken offline every time there is an attack.

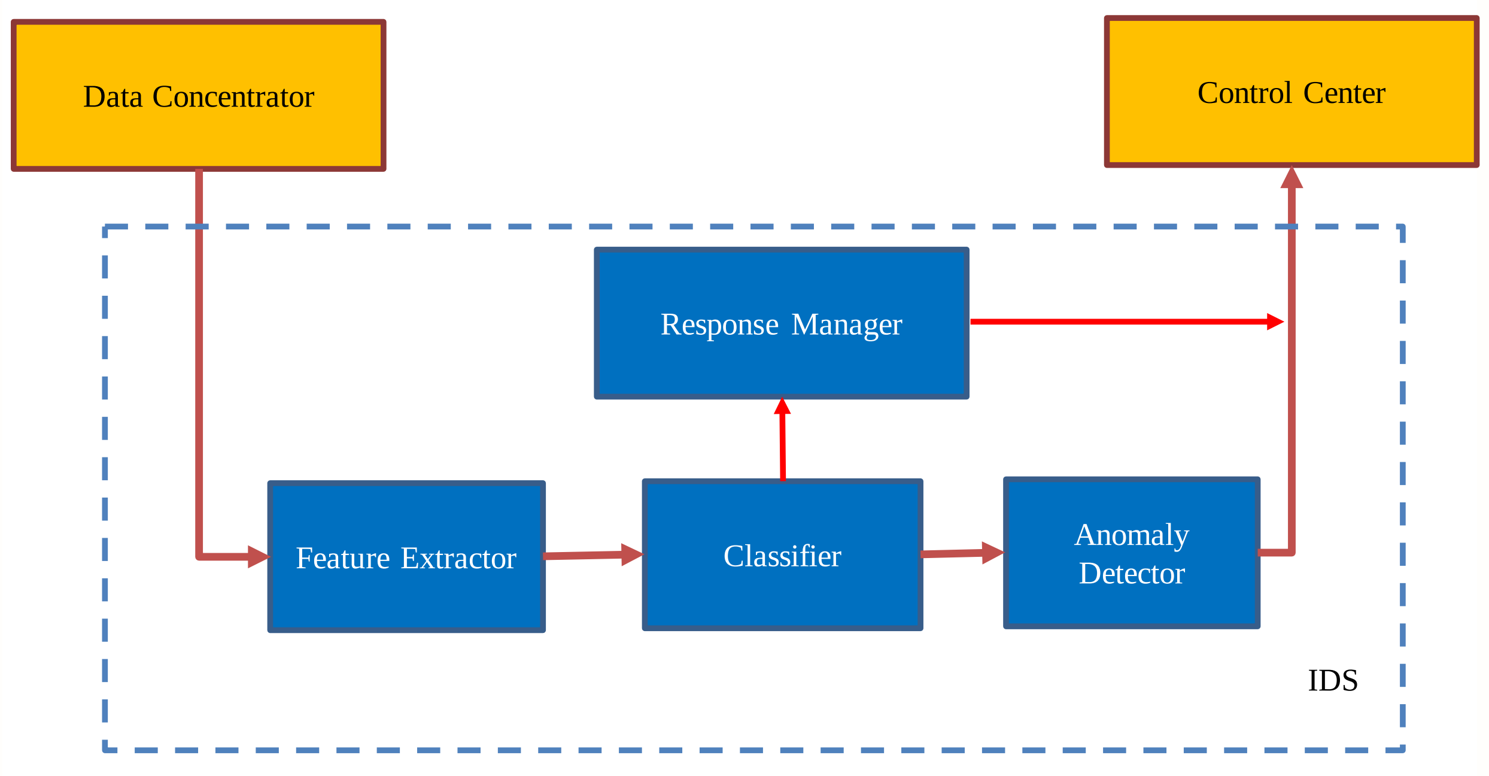
Objectives

Our objective is to provide a starting point to using machine learning applications for the Navy smart grid. The contributions of this thesis are as follows:

- Propose an Intrusion Detection System (IDS) for the NAVFAC grid.
- Introduce the CICIDS2017 data set and the use of the open source CICFlowMeter for feature extraction.
- Prove that different attacks can be grouped together based on objectives, and that machine learning using the K-nearest neighbours (KNN) algorithm can be used to segregate the various classes of attack traffic from benign traffic.

Proposed Cybersecurity System

In a typical smart grid, nodes which serve buildings or units are connected to a data concentrator by wireless means. We propose a system where the IDS is placed at the data concentrators which receive the data from the wireless networks before pushing it to the local control center. These concentrators are assumed to be physically secure and computationally more capable than the nodes they serve.

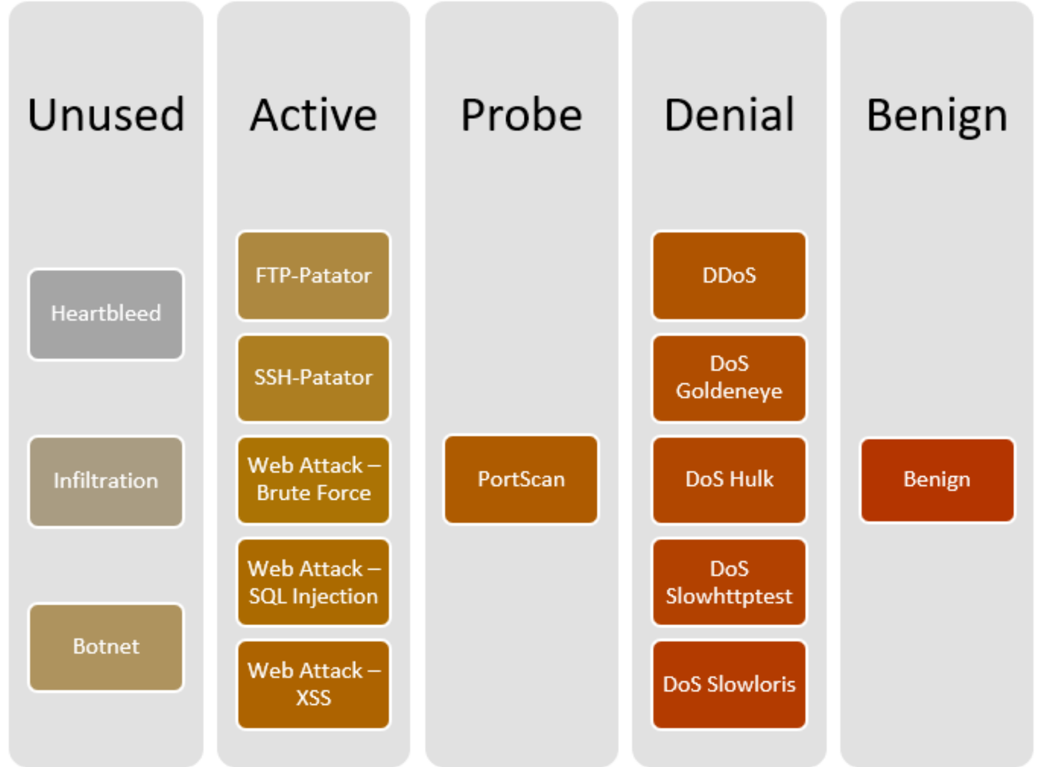


The proposed system is a combination of a classifier to quickly detect known attacks, and an anomaly detector to detect new threats. This system should be able to trigger specific responses to protect the integrity of the grid and isolate the areas under attack. Not every base has a SOC, the classifier needs to be highly accurate in order to alleviate the workload of cybersecurity personnel and allow them to direct their efforts to investigate the anomalies.

If an attack is detected by the classifier, the system will trigger the response manager. The response manager is responsible for a set of pre-planned responses to allow the system to quickly isolate the problem and ensure availability of the rest of the network.

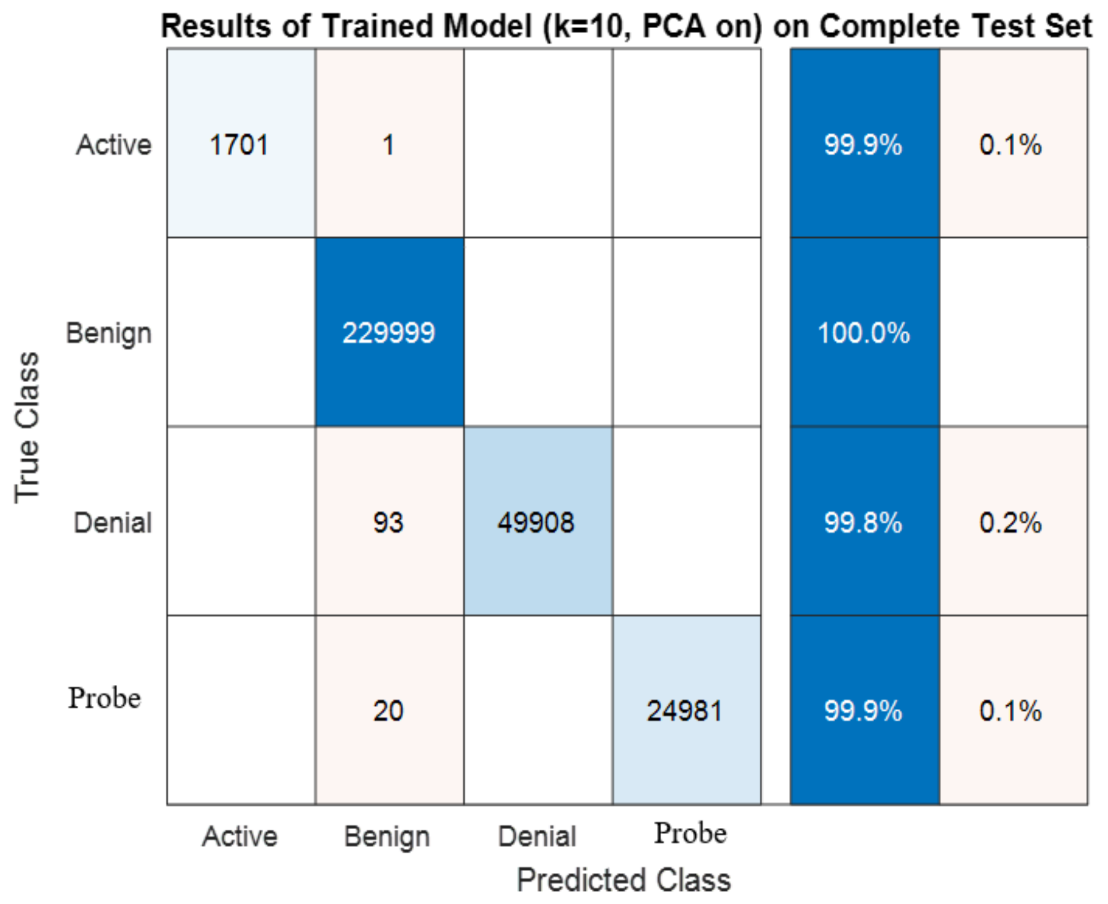
Grouping Attacks by Objectives

Sharafaldin, Lashkari and Ghorbani generated the CICIDS2017 data set [2] by setting up a comprehensive testbed and running a variety of attack types to satisfy a framework set by the Canadian Institute of Cybersecurity used to benchmark datasets [3]. Traffic from this test bed was put through an open source program called CICFlowMeter to extract up to 80 features from each "flow" which can be defined based on when a connection is terminated in a TCP exchange, or by time. The data set contains eight files of different attacks which were grouped into attack types as shown in the image below.



Results

We grouped different attacks based on the perceived objectives. Using MATLAB's machine learning toolbox, we demonstrated that a classifier using the KNN technique is able to segregate the various classes of attack traffic from benign traffic even though different attacks were combined. This implementation will enable the automated response and the results are shown in the confusion matrix below.



We recommended two methods by which to increase the accuracy of the classifier in order to minimize false positives, and therefore, an unnecessary interruption to the smart grid. These methods are to increase k (specific to KNN) and use the full suite of features provided by the feature extractor instead of feature reduction through methods such as Principal Component Analysis. The trade off, however, is time.

Future Work

We conducted our simulations based on a publicly available dataset, generated by an experimental setup. The next step will be to show that similar techniques can be applied specifically to the Navy smart grid. To that end, the following steps are recommended:

1. Build a smart grid test bed.
2. Manual feature selection.
3. Investigate methods to reduce the false positive rate.

References:
[1] Navy and Marine Corps Smart Grid CDD Industry Version. Commander, NAVFAC, Washington, DC, USA, 2014.
[2] I. Sharafaldin, A. Habibi Lashkari, and A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." *Proceedings of ICISSP 2018*, pp. 108-116, 2018.
[3] I. Sharafaldin, A. Gharib, A. Habibi Lashkari, and A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset," *Software Networking*, vol. 2017, pp. 177-200, 2017.

NUS
National University of Singapore