Chapter 8
A Machine Learning Approach for Anomaly Detection to Secure Smart Grid Systems

Richa Singh
Pranveer Singh Institute of Technology, India

Arunendra Singh
https://orcid.org/0000-0003-2897-1573
Pranveer Singh Institute of Technology, India

Pronaya Bhattacharya
Institute of Technology, Nirma University, India

ABSTRACT

The rapid industrial growth in cyber-physical systems has led to upgradation of the traditional power grid into a network communication infrastructure. The benefits of integrating smart components have brought about security issues as attack perimeter has increased. In this chapter, firstly, the authors train the network on the results generated by the uncompromised grid network result dataset and then extract valuable features by the various system calls made by the kernel on the grid and after that internal operations being performed. Analyzing the metrics and predicting how the call lists are differing in call types, parameters being passed to the OS, the size of the system calls, and return values of the calls of both the systems and identifying benign devices from the compromised ones in the test bed are done. Predictions can be accurately made on the device behavior in the smart grid and calculating the efficiency of correct detection vs. false detection according to the confusion matrix, and finally, accuracy and F-score will be computed against successful anomaly detection behavior.

DOI: 10.4018/978-1-7998-2795-5.ch008

INTRODUCTION

Traditional electricity systems support various operations in which the four basic operations are: generate electricity, transmission of electricity, distribution of electricity and electricity control. The term grid is basically used for this electricity system which supports all these basic operations which is discussed by (Fang et al., 2011).

The power grid systems generate power with the help of some central generator and provide it to the customers. As the time changes the revolution comes in every field. The power industry also comes in this revolution and made various changes and introduce the new innovative way in large scale which is beneficial for the customers as well as the power industry also. Smart devices and systems play a vital role in power industry. It creates a distributed network with the help of two-way communication for the flow of information and electricity. It has capability to control the electricity safely and in efficient manner with the help of grid parameter. Ability to sense and react on the behalf of what is happening by the smart devices in power grid has comes the power industry in the picture of revolution.

Fang et al., 2011) discuss with the help of modern techniques that the smart grid has the capability of power generation, power transmission, power distribution and control in effective manner. It can sense about the event and react accordingly.

Comparing the traditional power grid with new one, it has been found that the smart devices play a vital role for the modernization of the traditional grid, but it has certain limitations or challenges also. The major challenge is to handle the security problem that are very serious issue nowadays. Compromised smart devices in power industry leads a security issue. The sensors that measure and the controllers that directly or indirectly controlled behavior of grid have terrible consequences. Sometimes a sensor may supply a false information as a result the voltage are increased and overloading occur on grid or a malicious activity performed and this make electricity unavailable. To overcome this problem, time to time it must be ensure that the smart devices perform the healthy operations on grid and behave as expected.

(Farhangi, H. et al., 2009) gives a brief comparison between the existing grid and the smart grid are as follows:

Existing grid has one-way communication whereas smart grid has two-way communication.
Existing grid has centralized concept whereas smart grid has distributed concept.
Existing grid has few sensors whereas smart grid has sensors throughout.
Manual monitoring and manual restoration are done in existing grid whereas self-monitoring and self-healing is done in smart grid.