International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 09 | Sep 2022 www.irjet.net p-ISSN: 2395-0072

Fault Prediction and Interdependencies Identification in Smart Grids Using Deep Learning

D.Ajay Sai Reddy[1], Chiripalli Neha[2], Anjuri Bhanusree[3]

[1,2,3] *Students, B.Tech Electrical and Electronics Engineering , Anurag Group of Institutions , Telangana , India*

Abstract - *Smart Grid is an modernisation of current Electrical Grid which uses both communication and Information Technology to make electricity transfer more efficient. The smart grid is an interconnection of many communication devices and electrical components hence it makes an interdependent network . As the smart grid is interconnected, small changes or attacks on the network can lead to a cascade of failures across the networks which can lead to grid failures or power blockouts. Hence it is necessary to identify the faults and interdependencies among communication systems and electrical networks. This type of networks can be referred to as cyber-physical systems. This paper proposes an Artificial Neural Network based model that can detect the grid failures and interdependencies of grid components. This predictive model can help systems operators in Smart grid to make necessary preventive actions and mitigate the attacks or failures from time to time. As a case study to perform analysis we have used IEEE power bus system, namely IEEE-57 which represents American Power system. And the model achieves an accuracy of 99.92% on simple data and also 99.19% on complex data in predicting grid failure sequences.*

***Key Words*: failure prediction, Artificial Neural Network, deep learning, Multi-class classification, Smart grid, Interdependencies Issues.**

1.INTRODUCTION

Smart grids are cyber-physical systems which means that it consists of sensors, actuators, communication networks and protocols. The smart grids are different from conventional grid due to its two way communication and it is a resilient system that can heal itself during any failures in the network. The communication systems are responsible for this. The communication networks connect each component to achieve communication between various physical systems of the grid.[1] The cyber-physical systems are found everywhere like Industrial control process, Power systems, etc. The communication systems in the smart grid have enabled high dependability standards to achieve high accuracy. Nowadays, due to population growth, the electricity demand is also increased, hence it is extremely vulnerable to any attacks and can cause cascading failure attacks [1], [2], [3].Cascade failures is the failure of one or more components which in turn can cause failure to all other components in network. This vulnerability can result in devastating consequences if any initial component failures are critical ones.

Considering the smart grid as graphical representation. In smart grid, each component (node) has load and capacity [3], [5] . Due to cascading failure in smart grid, even single failure at single node [6] can lead to failure of its neighbor components (nodes) due to change in balance power flow .This can lead to global redistribution of loads in entire system components causing overloads and power shutdown of grids.

There are few large scale networks that are affected due to damaged components in the network or due to connected systems. In 2011 Arizona-southern blackout is an example for cascaded failures which caused an 11 minutes power outage in transformer causing 2.7 million people to be left out with power outage nearly up to 12 hours [7]. Italy blackout in 2003 due to connection issues with the internal architectures of the network [8].There is an most recent cyber attacks on power systems is, attack on the Ukraine power grid in December 2015, which is a synchronized and coordinated cyberattack, causing a 6-h blackout and affecting hundreds of thousands of customers[9].So, it is evident that these are very dangerous issues that can affect the economy and also causes physical damage to the systems. So, it is necessary to detect the failures and issues due to interdependency.

Smart Grids bring better capabilities and improvements to the present Power system. This makes systems more complex and vulnerable to different types of attacks and even unintentional failures due to increased complexity of systems and levels of cyber fragility. Hence, there are more security issues that need to be addressed. In smart grid these happen because of communication networks.

This paper provides a better understanding of interdependencies of network components and also fault detection in smart grids. To illustrate this work we used the IEEE-57 bus system and it is simulated on various faults. The data is collected for various components of the grid. The data collection and description will be explained in detail below. To predict the faults and identify interdependencies we used the Artificial Neural Network

to observe the underlying pattern of the data and analyze interdependencies so that it can be used to find the cascading components and also detect the failures in the grid due to communication networks . The dependency can be found with the help of correlation factors. There are various correlation methods that can help to find relations between the components in the grid. And also this predictive tool can be used by smart grid operators, Smart grid security tools provider, Smart grid manufacturers and vendors to analyze the attacks and provide counter measures from time to time. The Experiments and results shows that this method can effectively detect failure sequences in grid.

2.EFFECT OF CYBER ATTACKS ON SMART GRID

Due to advancements in smart grid technology there is a chance for cyber attacks, which deeply affect power industries. However the security in industries is a new topic and still experts are learning and trying to make security tools and find the vulnerabilities.

Vulnerabilities occur when hackers try to change the original values of devices in grids .There are many vulnerabilities which can affect the configuration of smart grids.[ ] There are few vulnerabilities that possess a serious threat to smart grids.

1. Smart grid has many communication devices that can help in controlling and monitoring the smart grid remotely. And Intelligent Electronic devices (IEDs) which handle many devices to manage both electricity supply and demand of load. So, a small update or modification of configuration can lead to great economic losses and also the operators need to travel to remote locations to identify the cause of the problem.

2. IEDs in smart grids process large amounts of data and hence preserving the information is one of the important tasks. Disclosure or unauthorized access to data or information can lead to major problems that can't be controlled after their occurrence.

3. As we use communication networks, small outages in the network can lead to power blockout and cause many economical issues.

4. FDI attacks can be possible due to vulnerable users at the customers end who intend to steal or enter the network to access back-doors and hack information and also modify the devices configuration which in turn can cause a cascade of failures in Smart grid.

Hence we need to provide more security measures compared to conventional power systems. In this paper we will use a computational method to resolve this problem.

3.INTERDEPENDENCIES IN SMART GRID

This section deals with the interdependencies analysis of components in cyber-physical systems. We have various communication protocols in smart grid to interconnect various physical devices like substations, distribution grids and transmission grids. And some of these communications like Local Area Network (LAN), Home Area Network (HAN),etc are provided by Internet service providers (ISP's) and these service providers might be shared with multiple companies which can lead to unethical information access, as this data will be shared across multiple communication devices which makes accessing of this data feasible and hence any cyber attacks can take place. Where, a simple attack on transmission lines or false data injection or failure of a smart meter ,etc can affect entire load stability of grid, and resulting a grid failure. As the smart grid is an interdependent network failure of one component in grid results in cascading failures. Hence proper security measures must be taken.

Interdependence of components is the Influence of one state component on the other state components and vice versa. The identification of interdependencies depends on systems behavior during failure of system. The disruption in system during failure can cause failure sequences in the grid from which we can find the dependencies between components. As, the interdependency of the communication network and power network shows the linkage of these two infrastructures. Figure 1 shows the power and information flow between the Power system network and communication network. The interdependencies in any cyber-physical systems can be classified into mainly four types : logical, Physical, cyber, geographic [10]. As, we are discussing about the interdependency relationship between Power system network and communication network they can described as below,

I. Communication networks have physical dependence on power system networks as it needs power supply to perform its data transmission functionalities.

II. The power system has cyber dependency on communication because, as a type of cyber-physical system (CPS), control of the power grid relies on the latter to deliver the monitoring data and control messages between the control entity and the field devices.

III. Geographical interdependence between the two infrastructures, since the transmission line and optical fiber are usually located close to each other in the power transmission network, while

the utility poles often carry both distribution lines and communication equipment on them.

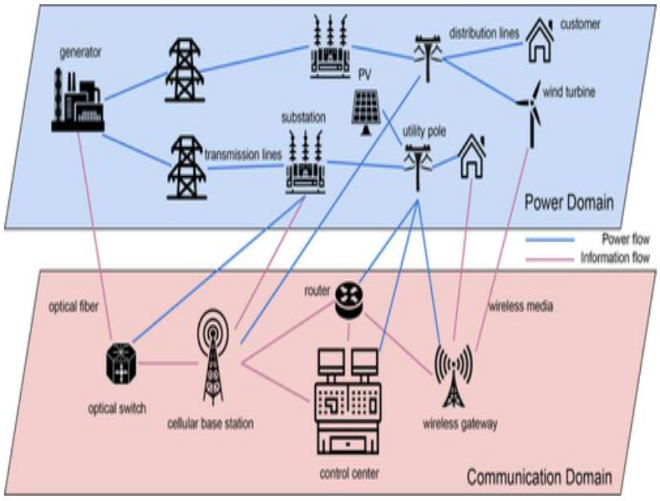

Figure 1 Interconnection of Communication Network and Power system Network

4.RELATED WORK

Anomaly Detection in Smart Grids using Machine Learning Techniques

The study paper authors Manikant Patni examined how the anomalies occur in smart grids. He discussed the detection of faults, cyber-attacks , etc. His work aims to detect cyber attacks in smart grid using Machine Learning techniques and for evaluating and experimenting he used IEEE-3 bus system.

Evaluating Anomaly Detection Algorithms through different Grid scenarios using k-Nearest Neighbor, iforest and Local Outlier Factor

The study paper authors Nils Jakob Johannesen; Mohan Lal Kolhe; Morten Goodwin used K-Nearest Neighbors to study the anomalies in smart grid and predict the cyber-attacks on grid.

A Systematic Literature Review of Machine Learning Approaches for Detecting Events and Disturbances in Smart Grid Systems

The study paper authors Ricardo Buettner; Johannes Breitenbach; Jan Gross; Isabell Krueger; Hari Gouromichos; Marvin Listl; Louis Leich;Thorsten Klier proposed an literature of different Machine Learning algorithms to detect abnormal events occurring in grid and also anomalies like cyber-threats and FDI attacks.

Identification of Interdependencies and Prediction of Fault Propagation for Cyber-Physical Systems

The study authors Koosha Marashia , Sahra Sedigh Sarvestanib , Ali R. Hursonb used deep learning to predict the failure of components of a grid using an Artificial Neural Network and also their work provided an analysis of interdependencies in smart grid that causes a cascade of failures .

5.PROPOSED WORK

In this section we will discuss the proposed work to identify faults and detect interdependencies in smart grid.

5.1 Simulations to collect data

To demonstrate the proposed work we used the IEEE-57 Bus system. Figure shows the single line diagram of the IEEE-57 bus system. As we know that classic IEEE bus system don't use any communication network but consists of generators, Transformers, etc. But our study is on cyber-physical infrastructure hence, we add communication network to the classic IEEE system to make an equivalent smart grid. This communication network consists of SCADA, PMU's , FACTS devices. FACTS devices help in power flow in transmission lines and we used methods [11] to find the location of PMU's and FACTS devices in grid.

We have designed the IEEE bus system test case as per our needs , now we need to perform the required simulation for failure cases of the grid. As we are learning the interdependencies of components it is important to find the number of failure sequences/cases needed to obtain all dependencies. In the case of predictive models, a large amount of data can give accurate results. Studies present in [12] describe a method to select required failure cases providing maximum accuracy. [10] described the following scenarios,

1. two simultaneous transmission line outages .
2. at most one FACTS device failed.
3. at most one PMU failed, failure of decision system.

The selection of failure cases are taken based on the real world failure rate of components in the grid.FACTS, PMU's failure cases are considered because they are prone to cyber attacks so a small attack on these can cause failures in cascaded systems. And transmission lines are also considered as they are a major part in power systems in which faults are usual .

5.2 Identification of Interdependencies and analysis

Interdependency is the state of an entity that influences or is correlated with the state of another, and vice versa[10

[10] Koosha Marashi, Sahra Sedigh Sarvestani, Ali R. Hurson, "Identification of interdependencies and prediction of fault propagation for cyber–physical systems ",Reliability Engineering & System Safety,Volume 215,2021,107787.

[11] M. Asprou, E. Kyriakides, Optimal PMU placement for improving hybrid state estimator accuracy, in: IEEE Trondheim PowerTech, 2011, pp. 1–7. doi:10.1109/PTC.2011.6019247.

[12] J. Qi, K. Sun, S. Mei, An interaction model for simulation and mitigation of cascading failures, IEEE Trans. Power Syst. 30 (2) (2015) 804–819. doi:10.1109/TPWRS.2014.2337284.