World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Investigating the impact of cyber security risks and reliability scenarios under the influence of IoT on the Smart Grid environment

Asif Khan [1,*] and Saim Memon [2, 3, 4]

[1] *Division of Electrical and Electronic Engineering, School of Engineering, London South Bank University, London, SE1 0AA, UK*
[2] *Jiangsu Sanyou Dior Energy-Saving New Materials Co., Ltd (SANYOU DIOR), No.10 Guoxiang Road, West Tai Lake Science and Technology Industrial Park, Changzhou, 213149, Jiangsu, China.*
[3] *Department for Engineering, School of Engineering and the Built Environment, Birmingham City University, Millennium Point, Curzon Street, Birmingham, B4 7XG, England, UK*
[4] *Solar Thermal Vacuum Engineering Research Group, London Centre for Energy Engineering, School of Engineering, London South Bank University, 103 Borough Road, London, SE1 0AA, England, UK.*

World Journal of Advanced Research and Reviews, 2023, 18(02), 001–016

Publication history: Received on 23 March 2023; revised on 30 April 2023; accepted on 02 May 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.2.0783

Abstract

The modern infrastructure of the smart grid minimises the power losses and maintain the electric power flow closer to nominal values. It enables the bidirectional flow of energy between consumer end and generation end along with a communication flow. Due to increasing number of smart grid equipment, it is important to investigate security protection and appropriate recovery measures for the smart grid application. Cyber security measures are important to consider for improving the reliability and intelligence features of the smart grid. This paper investigated the security measurements and different standards to counter the future security threats to the smart grid power systems. False data injection and risk analysis is carried out along with an internet of thing (IoT) based security solution to increase the reliability of data flow and communication on the smart grid. The investigations are performed by creating a power system model on a MATALB/Simulink environment.

Keywords: Smart grid; Cyber security; Standards; Risk analysis; Stability issues

1. Introduction

Smart grid consists of three layers subject to power flow, communication flow and information technology-based computing layer. It maintains the balance between the energy consumption and the energy demand. This improves the overall efficiency of the energy systems. The bidirectional feature of the smart grid allows consumers to sell their electricity to power companies [1]. For this purpose, a dual way communication system monitors the power flow between consumer end and the grid. This allows the energy producer and consumer to monitor the power flow in both directions. The communication system of the smart grid will allow the energy producer to stop the power supply remotely by using internet facilities.

By the advance implementation of information and communication technologies there is need to improve the security measures of the smart grid. The failure of critical devices such as communication system on the smart grid can cause power blackout and economic damage to consumer electrical equipment [2-4]. Therefore, it is needed to investigate the factors that can impact the security of the smart grid. Particularly research is made on the equipment that is more vulnerable to cyber-attacks. This will assist to provide the direction of future challenges to meet the security demands

* Corresponding author: Asif Khan

of the smart grid. The control and management unit of the smart grid is responsible for reliable flow of electricity to consuming end in a protective and control way. The auto healing of the smart grid can be achieved by applying modern technologies such as high-speed microcontrollers, fastest communication system and advanced sensing techniques [5]. Smart grid should be able to resist any type of security challenges and disturbances of power flow at a fastest speed.

In this paper a MATLAB/SIMULINK based research is made on the smart grid systems to prevent the energy blackout during the faults/fluctuations. A smart sensing communication system is added that connects the Power converter stations and load side directly to the central control unit. The system continues monitor energy flow in the system that improves the efficiency of the smart microgrid. The sensing system monitors voltage, current and power on the microgrid and sent wirelessly signals to the control unit findings. It also identifies the faulty section of the microgrid and separates it from rest of the system. The applied system improves the energy management on the grid to protect the power equipment during the faults.

2. Methodology

Smart grid requires large scale of electronics and communication infrastructure to improve the reliability of power flow parameters. It enables two-way flow of electrical power along with dual communication systems. The communication network is linked with neighbour area network (NAN), wide area network (WAN) and home area network (HAN) as shown in Fig.1. The neighbour's area network fulfils the requirements of distribution power system, wide area network covers larger area of power network such as transmission lines and home area network cover the customer premises power applications. Home area network (HAN) is equipped with advanced metering infrastructure and transmits the data from thousands of homes local data centres (NAN) by means of multiple data aggregation units. Neighbour area network is one of the major parts of smart grid communication centres.

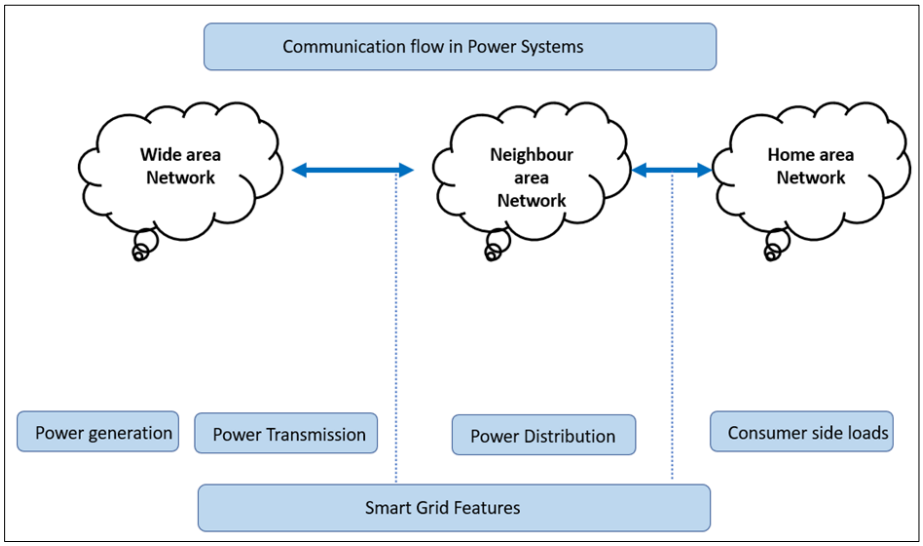

Figure 1 The three types of communication systems Home Area Network (HAN), Neighbour Area Network (NAN), and Wide Area Network (WAN)

The controlling and monitoring of power flow on the smart grid is achieved by installing sensors, smart meters, and smart measurement units. These units are connected to each other by wireless Simulink blocks. This benefits the smart grid is to securely operate if a fault happens at any unit. The communication between different units on the smart grid also allows to counter cyber-attacks, auto healing capabilities and supply the power to the consumer uninterruptedly. It will also provide awareness to consumer how much power they have utilised. The MATLAB simulation-based communication system are demonstrated in Fig.2. Reliability of neighbour area network is very important as it is a gateway of communication flow between centralised control unit and consumer side loads.

Cyber-attacks and malfunctions are one of the biggest threats to reliability of smart grid communication systems [6]. Power flow analysis is performed on a smart grid system from generation unit to household consumption along with data flow communication and monitoring systems as illustrated in Fig.3. The major parameters that are related to the reliability of the power systems are quality power flow without disruption in voltage, frequency, or outages of the power supplies. These power flow features are analysed by simulating a model of 210MVAr.

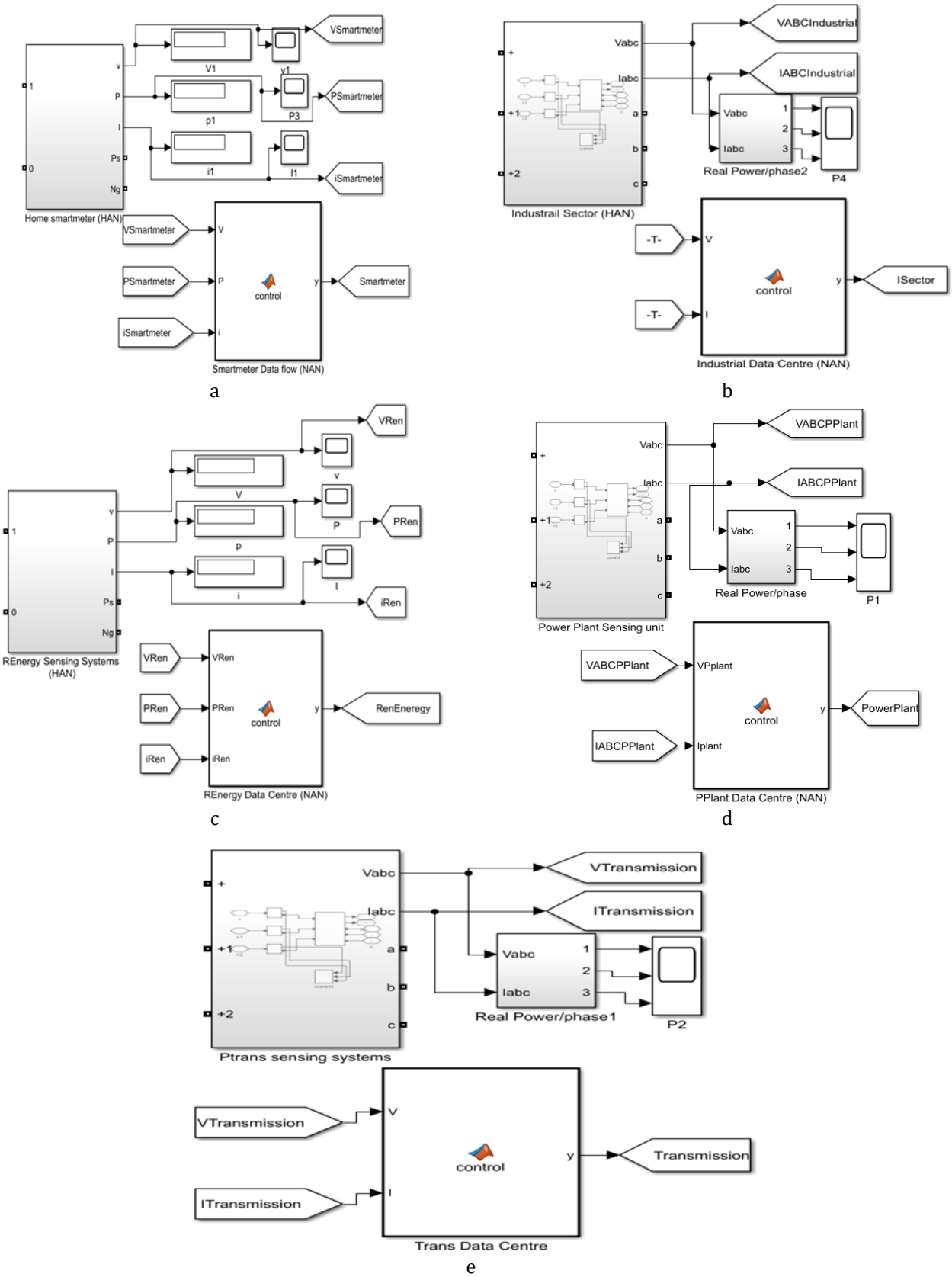

Figure 2 (a) Home area network and Neighbour area network system. (b) Industrial data flow systems on the smart grid. (c) Renewable energy connection by means of internet of things. (d) utility data flow system (e) Power variable data communication on the transmission network.

There are three power generation units installed to investigate the impact of cyber physical attack on the power flow parameter. The nominal value of the Simulated model is shown in Tab.1.

Table 1 Specifications of the simulated model used to analyse the cyber physical attack

Generated Voltage	23kV
Nominal Power G1	100MVA
Nominal Power G2	100MVA
Mixed energy sources	10MVA
Consumer Load	Variable
Armature inductance	0.000835Ω
Output voltage	415V/230V
Transmission Voltage	400kV/132kV

The aim of research is to identify the power system features that cannot perform according to reliabilities theories. SIMULINK provides all the components that can be used to simulate the smart grid system to analyse power flow. To achieve the accurate reliability, it is required that all components should be tested regularly and performed according to design specifications. If any of the device fail than it should be removed from the systems.

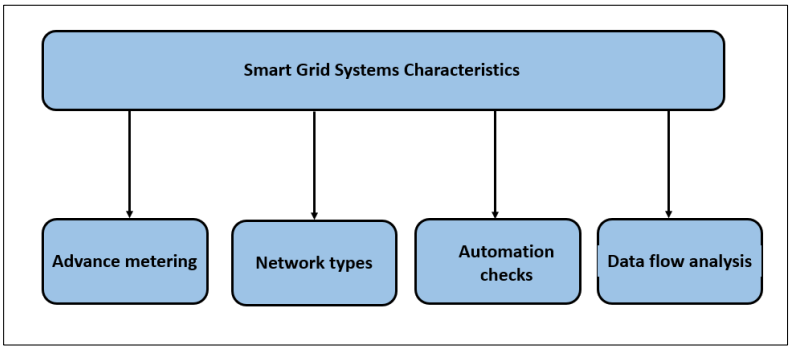

Figure 1 The hierarchy of Power systems and communication flow.

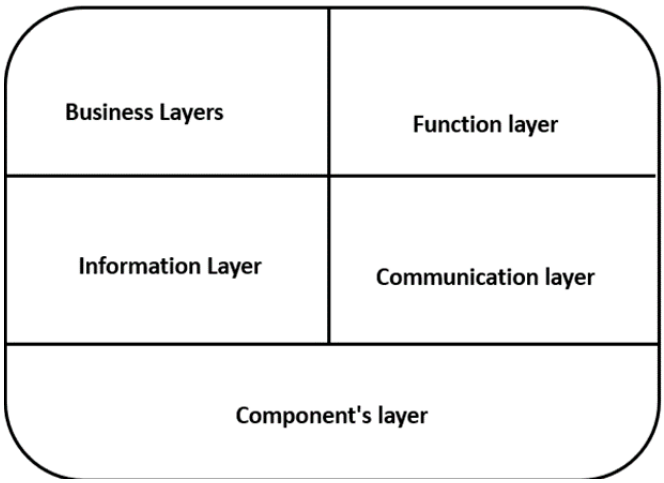

Figure 2 The architecture model of the smart grid. It displays the five complete layers that relate to smart power systems along with zones, domains, and interoperability dimensions

The major issues associated with reliability are networking and communication systems. Any issues constrained with networking or communication compromise the reliability of the power systems such as network failure or malfunction

attacks will have severed power flow impacts on the grid network that will cause power blackout and leakage of grid information. The applied components ensure the reliability and resilience of data transmission. The complete layering features of the smart grid is demonstrated in Fig.4.

The smart grid also provides the predictable information to energy suppliers and consumer about the power disruptions or fluctuations [8]. This will improve the overall energy efficiency and reduce the carbon emission for a clean environment. The major components of the smart grid are information and communication technology, measurement units, Remote control systems, smart meters, log servers, protection appliances and protocol gateways [9]. Smart grid systems should be design in a way to meet security challenges. The security devices should have the features to counter cyber-attacks or tackle any types of communication failures. Smart grid receives the energy from different sources such as from fossil fuels, nuclear, renewable, or hydro. The structure of the smart grid is presented in Fig.5. Therefore, it is also important to stabilise and monitor energy from these sources accurately. Failure of any energy supply sources can result in reduction of power flow on the grid and imbalances in voltage or frequency components.

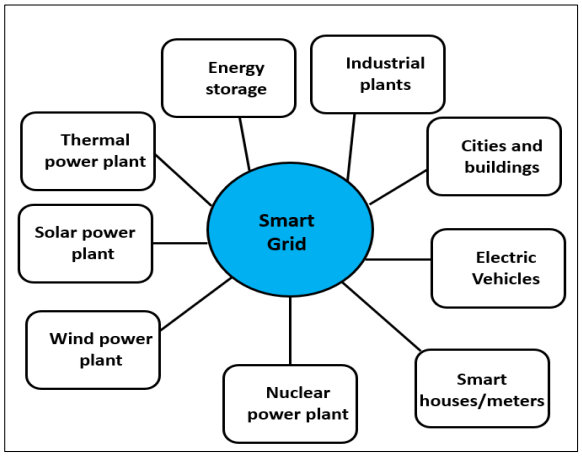

Figure 3 Illustrate the structure of the smart grid

2.1. Framework to identification of false data injection:

A state estimator can be applied to calculate the power at different sections of the smart grid if the voltage magnitude, current and phase angel is given in that point. Once these parameters are given real power and reactive power can be determined on the transmission grid. These measurements on the smart grid are usually relates to system state function. Reactive and real power flow on the smart grid can be expressed as [10-11]:

$$P_k = \sum_{J=1}^{N} V_k V_j Y_{kj} cos(\theta_k - \theta_j - \psi_{kj}) \;\; k = 1, \ldots . N \qquad \text{Eq.1}$$

$$Q_k = \sum_{J=1}^{N} V_k V_j Y_{kj} sin(\theta_k - \theta_j - \psi_{kj}) \;\; k = 1, \ldots . N \qquad \text{Eq.2}$$

P_k is the active power injection on the smart grid.

Q_k is the reactive power injection on the smart grid.

Y_{kj} is magnitude of admittance from k to j.

ψ_{kj} is the phase angle from k to j.

$$P_{kj} = \sum_{J=1}^{N} V_k V_j Y_{kj} cos(\theta_k - \theta_j - \psi_{kj}) - V_k^2 Y_{kj} cos\psi_{kj} \qquad \text{Eq.3}$$

$$Q_{kj} = \sum_{J=1}^{N} V_k V_j Y_{kj} sin(\theta_k - \theta_j - \psi_{kj}) - V_k^2 Y_{kj} sin\psi_{kj} \qquad \text{Eq.4}$$

P_{kj} is the real power from k to j on the smart grid.

Q_{kj} is the reactive power from k to j on the smart grid.

The voltage angle θ_j, θ_k cannot be measured direclty so to extract the values a nonlinear state estimator has to be applied. The measurements are completed by at different section by means of communication channel. Therefore, the values can be corrupted and amend if there is a attack or any sort of error happen due to failure of communication components. False data can also be injected to create error in the true measurements which can corrupt the entire system. False data can be inserted as a targeted unconstrained and targeted constrained to mislead the estimation process.

3. Results and Discussion

The communication system of smart grid comprises of subnetworks along with different communication technologies. Smart grid applications define the communication systems that is used to control and monitor the information from different sections of the network. It is required to choose the best technology for the smart grid communication system to meet the current needs and fill the gaps that create security challenges. Internet of things (IoT) connect different devices such as machine to machine communication by using internet [12-13]. A device can be any component such as sensing system, control units, measuring system or protection system of the smart grid. IoT connect these devices by IP-based systems where a device can communicate directly to the other device by using internet protocol (IP) address. Smart grid is one of the major applications of internet of things that will have a power flow on the grid along with communication flow as shown in Fig.6. The communication signals are very important to consider because that control and monitor the power flow on the grid. Smart grid uses sensors, measuring units, actuators and smart meter to provide the data with accuracy.

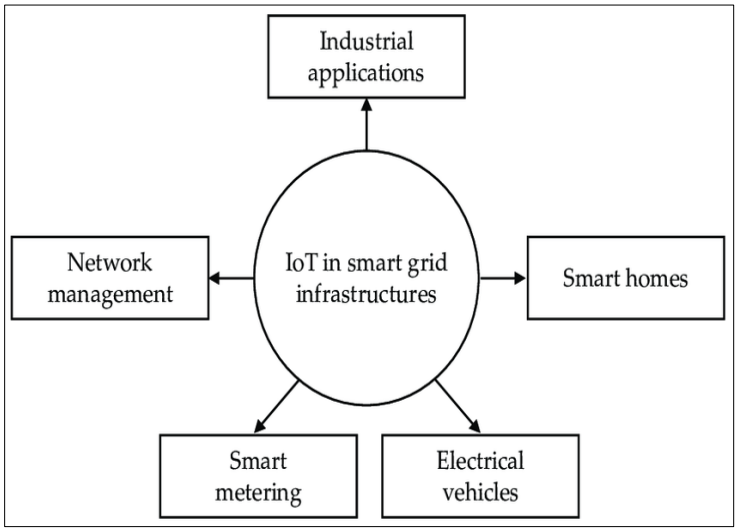

Figure 4 Importance of Internet of Things for smart grid applications.

There are different security standards that can applied to meet security demands of the smart grid communication systems such as NISTIR 7628 [14]. The other latest standard for smart grid security and reliability are GB/T 22239 and NIST 800-124. ISO/IEC 27000 is the cyber security for SCADA [15]. These standards relate to network security, security standards, integrity, data security, availability and confidentially parameters of the smart grid as shown in Fig.7.

3. 1. NISTIR 7628

This standard defines the categories of the security related logical interface and security properties of the smart grid. Key management framework is one the important section of communication systems that provides the ways to protect the communication channels by auto update, generate and deletion of keys that are used to exchange information over the channel.

3.2. GB/T 22239

GB/T 22239 is a standard published in 2008 that relates to system security and protect communication system and information security systems. This standard describes the security systems by detecting security events against threats

from cyber-attacks. If the damage is happening than this technique will restore the system to previous state. This technique can be implemented to all equipment of the smart grid and security assessment can be done by periodical network with no extra guidance and requirement of this standard can be split between managerial and technical parameters.

3.3. NIST 800-124

This standard is published by National institute of standards and technology (NIST). It defines all the components that are connected to the smart grid such as Bulk power generation, substations, renewable energy, distribution systems and utilisation. These standard analyses the security assessment of the components and ensures the control is applied precisely to achieve desire outcomes with respect to security management of the smart grid network.

3.4. ISO/IEC 27000

This standard covers every layer of smart grid. This is the most important standard of information security management that the describes the different stages such as system planning, analysis, implementation stage and design process [16]. This standard is applied worldwide by different organisation to meet the security demand. Regular security checks are performed in this standard to ensure the security demands are fulfilling according to registered standards.

3.5. IEC 62351

This standard can be applied to protect many smart grid components except physical cable layer. It provides communication and data security related to power system management and information exchange on the network. It asses the risk of attacks to apply security measurement. The information from these techniques can be used to make security policies and procedures to protect the power system network.

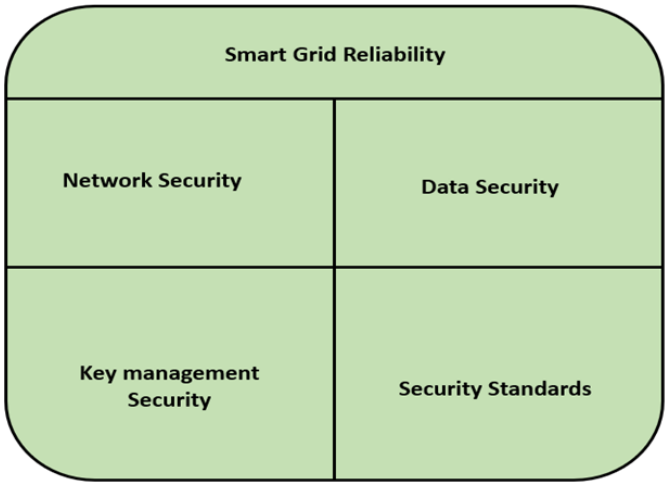

Figure 5 Demonstrates the reliability properties of the smart grid

There are many ways to insert false data into the system as follows [17].

3.5.1. Line Attack

In this technique, attackers attack the power system measurement system and circuit breakers that is connected between two points/buses on the smart grid as shown in Fig.8. The purpose is to change the actual values on the measurement and create disruption in power flow. This type of attack is also called random attack. Fig.9. shows the line attack on the power protection system that isolated G1 power plant from the system.

3.5.2. Bus attack

In this technique, attackers access the meters and create attack vectors based on matrix knowledge to amend information. This type of attack is also called targeted attack. This is also defined to targeted constrained attack and targeted unconstrained attack. In targeted constrained attack, attacker create mislead state variables by inserting specific errors in those variables. This type of attack usually happens if the conditions are met by the attacker's data. Targeted unconstrained attack is like targeted constrained attack except in this state other variables in the system are also get corrupted [18].

3.6. Random false data injection method

In this method attackers inject random number of errors into the state variable to corrupt the data in the communication channel. It will affect the power flow control and transmit information's wrongly cause of malfunction. This type is attack is very complicated and difficult to detect.

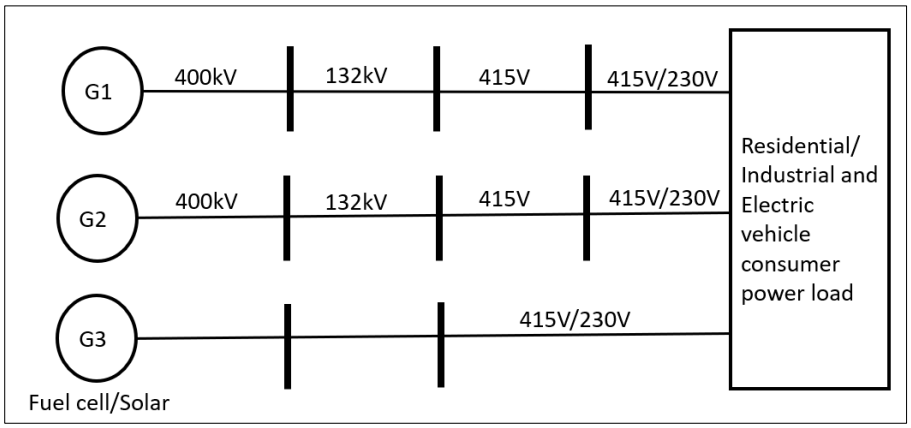

Figure 6 Demonstrate the single line schematic of the system

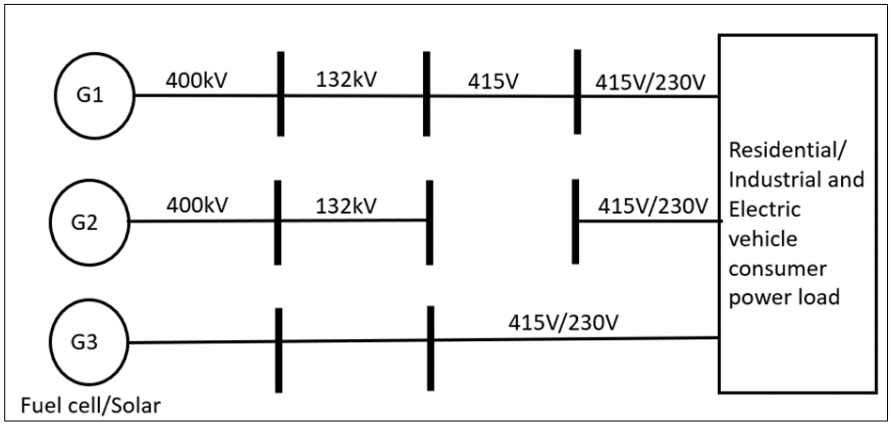

Figure 7 The power network isolation after the cyber attack at 132kV substation protection system.

3.7. Cyber physical and communication security measures

The channel of communication flow is very becoming very large due to growing numbers of control and electronics components on the smart grid. A two-way communication system for the smart grid is shown in Fig.10. Power flow properties are also becoming very complex such as non linear correlation between voltage and current and non-functional depenedency. Due to complex features it is difficult to capture non linearity in power flow parameters before the attack and after the cyber attack. Such as voltage, frequency and phase can show the similar fluctations and it can be difficult to detect the threat of cyber attacks.

It is important to receive the values of voltage phase, current phase and other power system parameters closer to nominal values to save the system from cyber attacks. Phasor measurement is one of the technique that can be used to provide these values close enough [19]. Cyber physical data can be fomred from physical data of the phasors system measuremens and the overall communiction flow, network log as shown in Fig.11**.**

The type of attack can be detected if there are amendment happens in the cyber physical data from the attackers that can inject false data into the system. If the attack happens in the cyber pysical data, firstly identify the nature of attack and then collect the attacking data samples, and extract data peaces that contains the information behaviour of attack. Then remove the attacker useless inofmations and redundent data and perform self learning and reset procoess. By comparing the results before and after attack this model can be used to adjust the modelling parameters. Fig.12 shows

the voltage flow on the network before the cyber attack on the substation. Two power plants of 100MW each and a mixed energy sources of (Fuel cell/solar) 10MW are connected to feed of variable megawatts load at the residential/industrial sector. The grid is equipped with sensing units and circuit breaker. A cyber-attack is happened on the circuit breaker of one power 132kV substation that stopped power flow from one of power plant. At this point one power plant is disconnected from the system. Voltage is reduced to 380V, and frequency is noticed lower to 47HZ as shown in Fig.13.

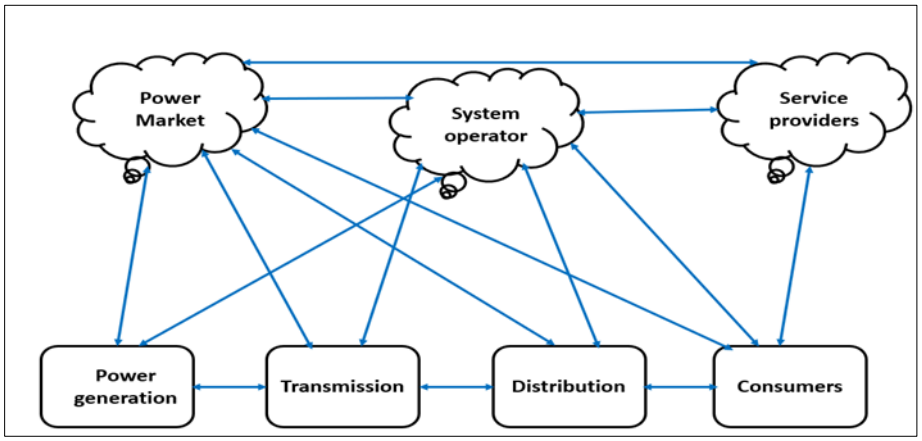

Figure 8 *T*he two way communication flow for the smart grid systems

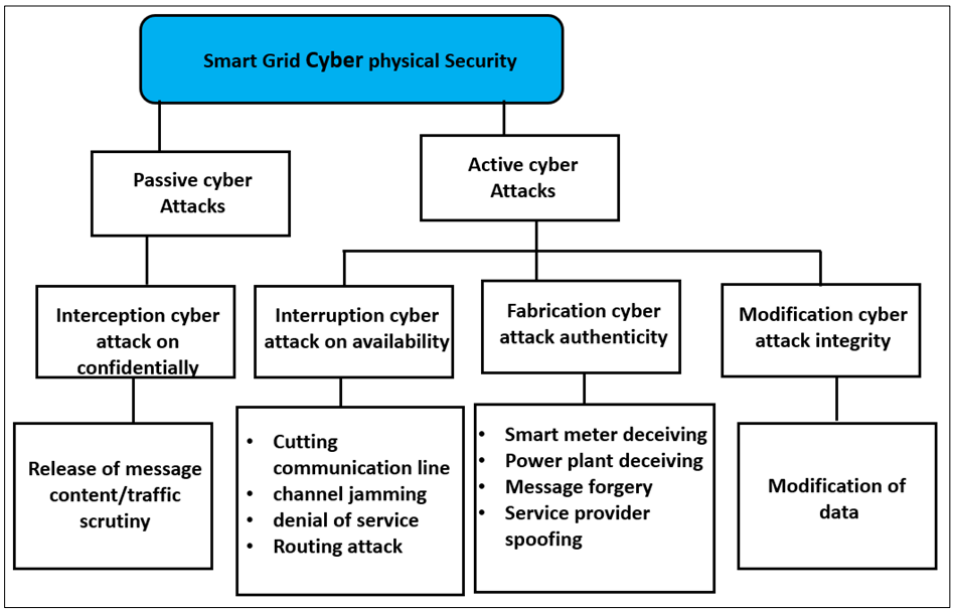

Figure 9 Cyber physical security of the smart grid

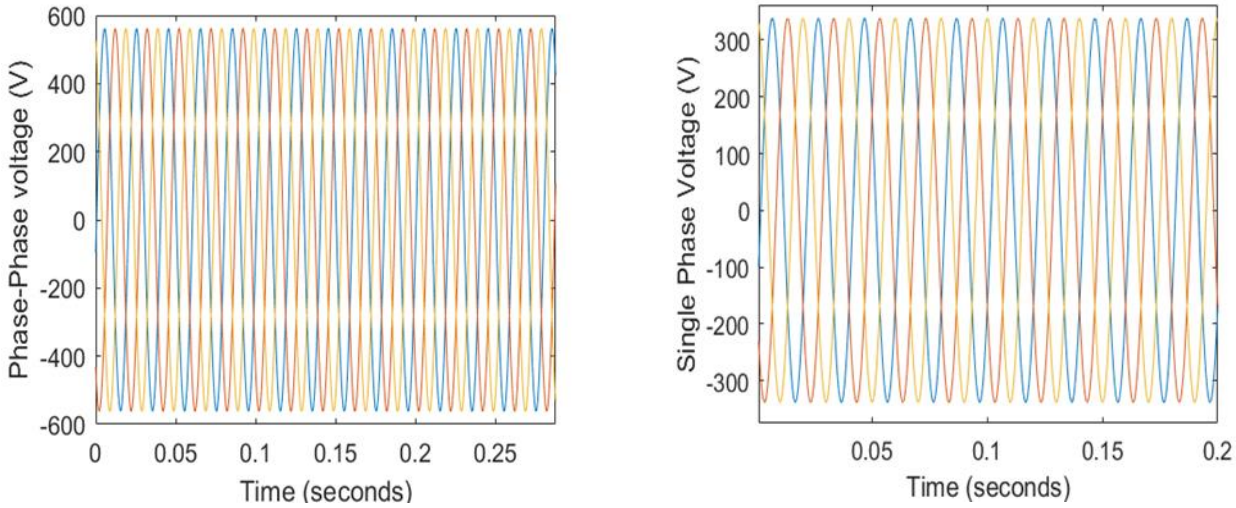

Figure 12 Illustrates the voltage flow on the distribution network before the cyber physical attack

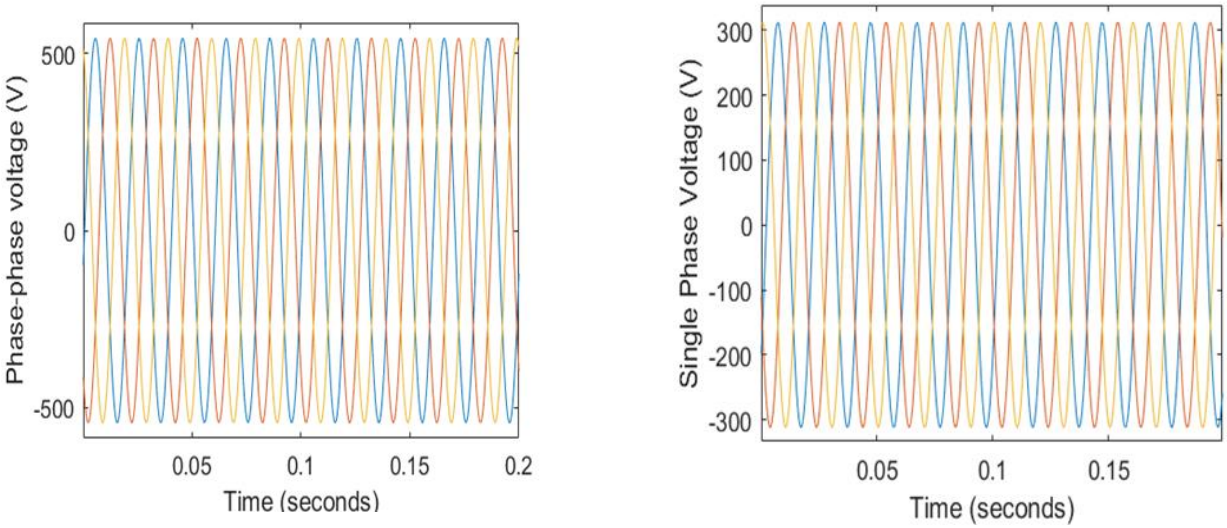

Figure 13 The voltage reduction on the distribution network after the cyber physical attack on one power substation

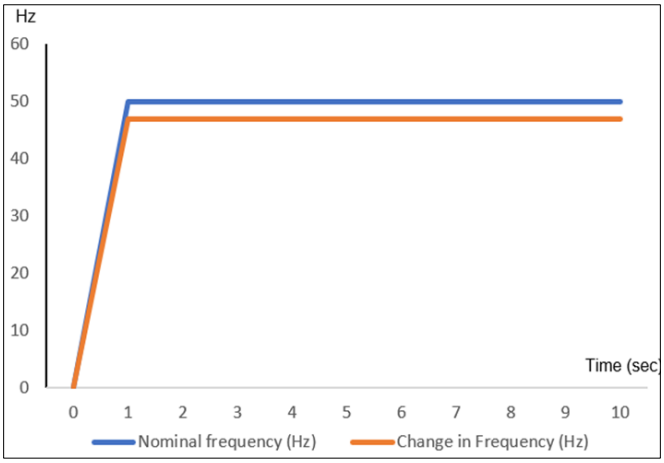

Figure 14 Illustrates the differences in frequency before and after cyber attack on the power substation.

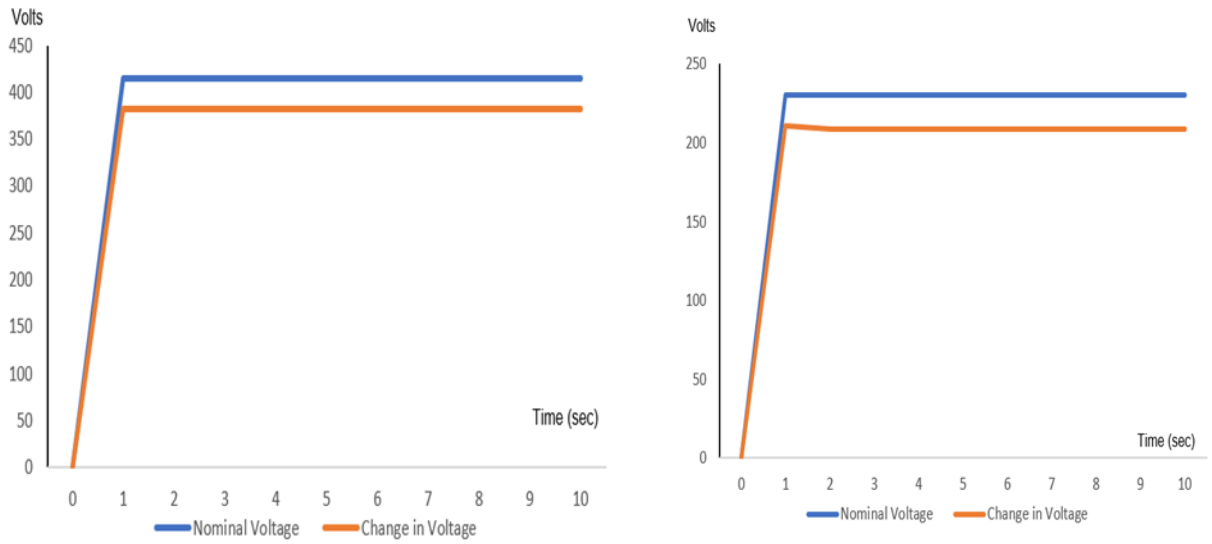

Figure 15 The differences in voltage before and after cyber physical attacks.

3.8. Supervised Fine-Tuning Classifier

This SoftMax is built to detect the attack where output layer are set to neuron (N). The type of attack is represented by each neuron in the system. It completes detection process by setting the values to neuron such as output layer neuron given a value of 1 and all other neurons N-1 are equal to zero. The neuron with value of 1 represent the detected attack. The equation defines the Supervised Fine Tuning Classifer is shown [20]:

$$Y_i = \frac{e^{xi}}{\sum_{i=1}^{N} e^{xi}} \qquad Eq.5$$

Here i is the category index, Y_i is the probability of the detection results in ith classification, N is the total number of categories, X_i is the softmax classifier input value.

It is also necessary to regularly check the performance of the security model. The performance test can be performed by testing time, training time, accuracy and precision that were set to achieve the desires outcomes [21]. The accuracy and precision of the model can be evaluated to:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad Eq.6$$

$$Precision = \frac{TP}{TP+FP} \qquad Eq.7$$

TP is the true positive case that can used to recognise the normal conditions of the communication flow, TN is the true negative case that is applied to identify the attacks on the data systems, FP is the false positive that wrongly categorise the true situations, FN is the false negative that can wrongly identify the attacks [22].

The analysis on the future security trends on the smart grid is performed on smart grid applications and communication flow systems. The internet of thing (IoT) is analysed with solutions to improve the security of network. Particularly communication and information system of the smart grid are described. The information is analysed to meet the security demands of the smart grid and different types of security standards are investigated to achieve the cyber security standards. The main sections of the smart grid are shown in Fig.16. It is concluded that the internet of thing and wireless communication flow are very good strategies that can be applied on the smart grid to solve the security problems. Cloud computing is also one of the major technologies to reduce security risks for the increasingly number of control devices and growing smart meter devices.

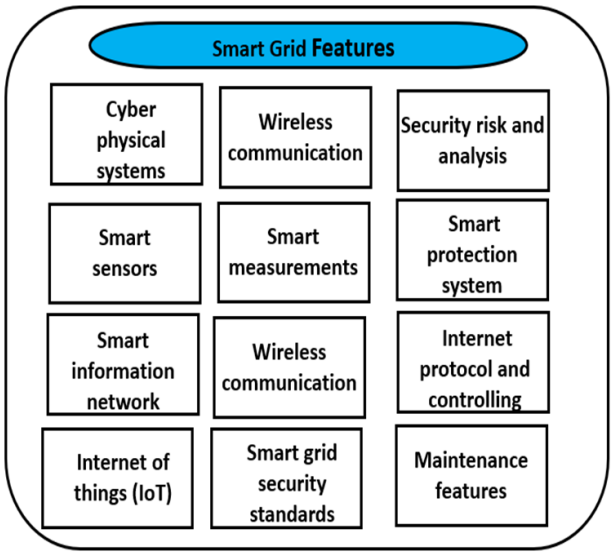

Figure 10 Major control and management functions of the smart grid

3.9. Smart grid simulation environment

The simulation of the smart grid is performed on MATLAB/Simulink. A smart sensing system and monitoring units (sub-control) is applied at different parts of the network. These units sense and measure the power flow on the grid. A smart meter is installed at the consumer side that describes the energy consumption at the load section known as Home area Network (HAN). This type of network is installed in the smart metering infrastructure in the electrical appliances at homes and in buildings. It also supports the dual way of energy flow between utility and local energy generation. The advance meters show the consumption of electricity. The advance metering unit is responsible for managing power management at the public utility. It buys electric energy from the generation plants through distributed transmission lines. The advance meter is a part of smart grid infrastructure that send and receive the data by wireless network communication systems. Home area network (HAN) is always connected with neighbour area network (NAN). This network collects the nearby data between consumers side metering substations. There are networking devices installed for transmitting and collecting data in a reliable way such as intelligent electronic devices (IEDs). It is bridge of dual way of communication system for power deliver between advance digital meters and substation control centre. Data flow is not high as wide area network due to shorter transmission network compered to wide area network. The data transmission is mainly adopted by wireless communication system with low bandwidth channels. The applied components ensure the reliability and resilience of data transmission.

A centralised control unit is established that is major control system of the smart grid as shown on Fig.17. The centralised control unit monitor the power flow in real time scenarios and compare with the predicted reference values of the voltage, current and power and is known as Wide area Network (WAN). This category maintains the flow of communication between substations and utility centres. It consists of control and measuring data centres at power generation units and substations to provide wider information. It covers a longer distances data flow where communication flow needs reliability because of requirement of high bandwidth-based communication network. This system are always equipped with modern control and sensing applications.

The applied protection is also interconnected with centralised control unit by wireless communication channel to protect the grid in case of false data injection into the network. Fig.18 demonstrates the variations in power flow parameters if the cyber-attack happens after 10 sec. This will protect the smart grid equipment and components on the consumer side. The wide area network (WAN) mainly depends on the data receive from the neighbour area network (NAN) units which collect the data at different point on the grid using measurement tools such voltage measurements and current measurements. The sensing system send the other variables such voltage angles and magnitudes along with the frequency. The control system then asses the stability of voltage and frequency control. In the case of cyber-attack, several protection techniques can be applied as mentioned above to protect the smart grid. Each sensing system should be equipped with high-speed internet local area network (LAN).

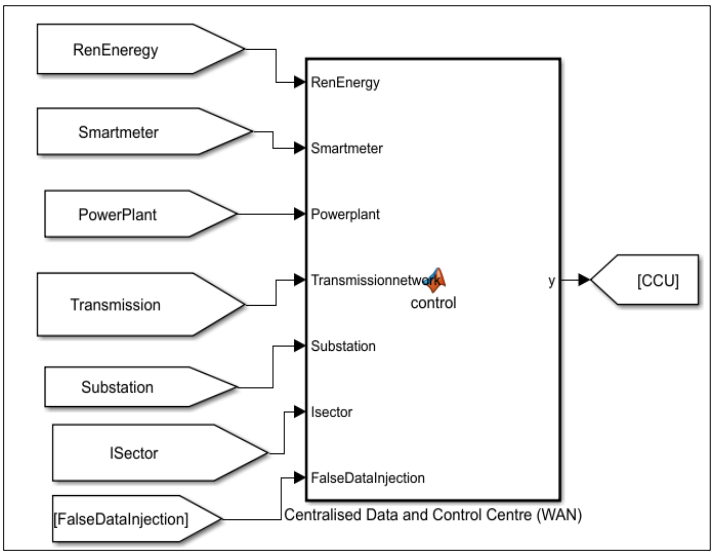

Figure 11 Wider data analysis system on the smart grid

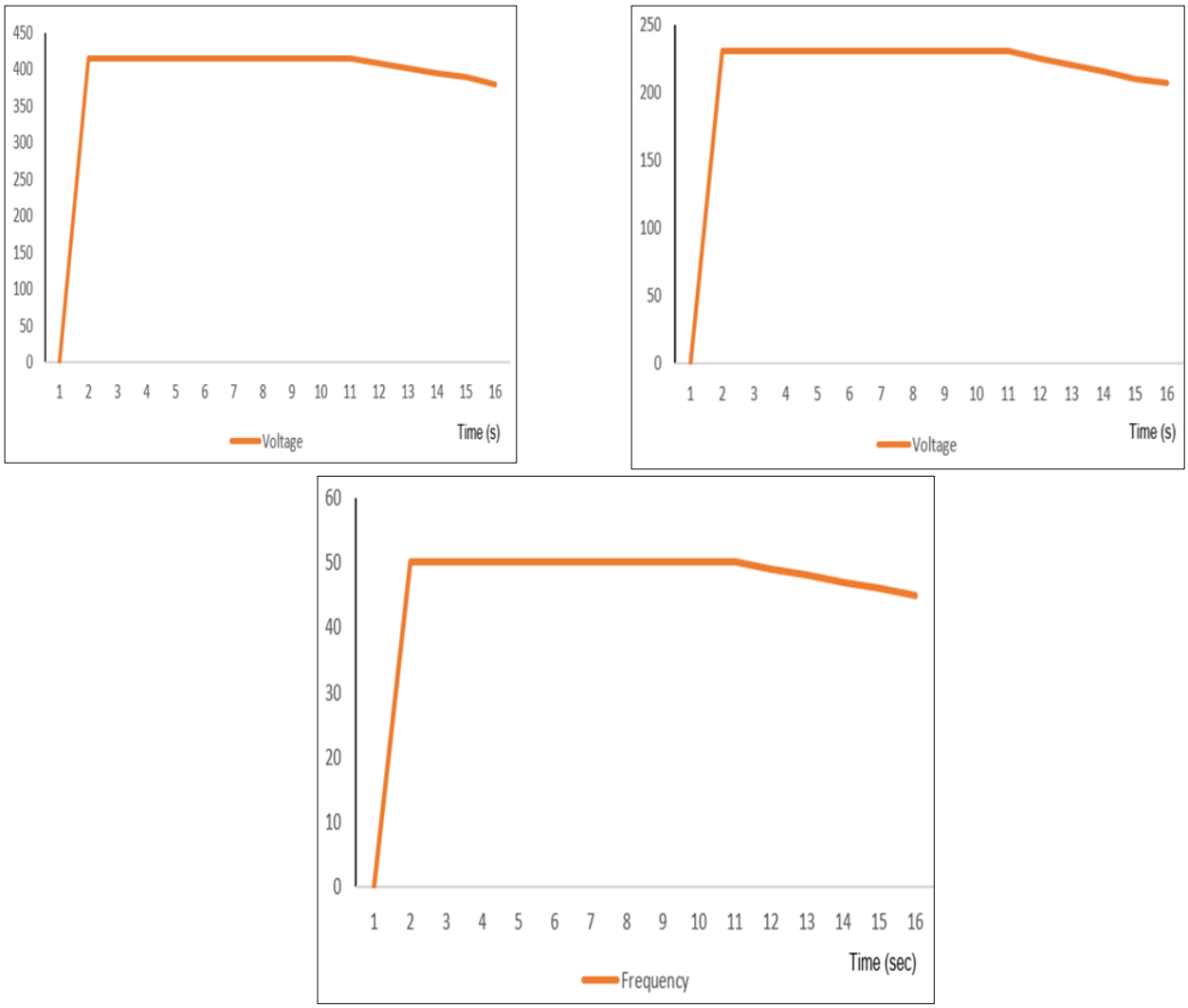

Figure 18 (a). Variations in voltage after the cyber-attack. (b) Shows the single-phase voltage after the cyber-attack. (c) demonstrates the frequency analysis

The algorthim is defined as

- Findout the features of origional attack.
- The optimal properties of the attack that made changes in the system.
- Collect the maximum information at all section and features of each catergory.
- Remove the irrelavent parameters and weakly related properties on the system.
- Delete the remaining features in the network
- Observe the auto learning properties of the system before and after attack.
- Obtain the data and analyse it
- Reset the system
- Repeat the above procedure incase of another attack.

Nomenclature		Abbreviations	
$R_s(f)$	Risk of failure	IoT	Internet of Thing
P_k	Real power injection	IP	Internet protocol
Q_k	Reactive power injection	LAN	Local area network
Y_i	Probability of attack detection	ICT	Information and communication technology
X_i	Softmax classifier	NS	National standards
θ_j	Voltage angle	FDA	False data attacks
Y	Magnitude of Admittance	TN	True negative
t_d	Detection time	TP	True positive
H_dc	Combined attacks	FN	False negative
Z_a	Tempered data	FP	False positive
T_a	Terminal layer	SFTC	Supervised fine tuning classifier

4. Conclusion

Cyber security is one of the key factors to consider for smart grid applications. Smart grid consists of data centres and control system that needs to protect from different types of attacks that can inject false data into the system. In this paper different types of control techniques and risk analysis is performed to secure the smart grid from such attacks. It is noticed that the false data creates disruption in the power flow and cause power blackout. By applying the proposed methods and algorithm future attacks on the smart grid applications can be prevented. The research presents the understanding and needs of the cyber security requirements of the smart grid. Different types of cyber security attacks and defensive system is also proposed in this paper. It is concluded smart grid requires different types of security management such as data security, network security, communication flow security, data recovery systems, application security and host security systems. Wireless communication security and terminal security are also important parts of the smart grid applications. Different types of standards can be applied to provide security to these systems. The probability analysis is also performed that can be used to auto detect the security threats for reliable systems operations. State estimators are also discussed to relate the corrupted data during the attacks and how to recover the missing data and to reset the systems. Future work is to create mobile based private applications that should be capable of stopping the cyber-attacks on the data centres. Because of security risks in information technology of the systems, deeper research needs to be performed to counter potential vulnerabilities and cyber-attacks.

Compliance with ethical standards

Acknowledgment

Authors would like to thank the research facilities support provided by the Solar Thermal Vacuum Engineering Research Group at London Centre for Energy Engineering at London South Bank University. This research is self-funded and did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclosure of conflict of interest

All authors declare that they have no conflicts of interest.

References

[1] Mathias Uslar, etal, “Applying the Smart Grid Architecture Model for Designing and Validating System-of-Systems in thePower and Energy Domain: A European Perspective”, MPDI Energies, 2019, 12(2), 258, doi:10.3390/en12020258, https://doi.org/10.3390/en12020258.

[2] Husam Suleiman, Israa Alqassem, Ali Diabat, Edin Arnautovic, Davor Svetinovic,"Integrated smart grid systems security threat model",Information Systems,53, 2015,pp.147-160,https://doi.org/10.1016/j.is.2014.12.002.

[3] Gottschalk M., Uslar M., Delfs C. “The Smart Grid Architecture Model – SGAM. In: The Use Case and Smart Grid Architecture Model Approach”. Springer Briefs in Energy. Springer,2017, pp 41-66. https://doi.org/10.1007/978-3-319-49229-2_3

[4] Bahmanyar, A. Estebsari, A. Bahmanyar and E. Bompard, "Nonsy load flow: Smart grid load flow using non-synchronized measurements," 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2017, pp. 1-5, doi: 10.1109/EEEIC.2017.7977509.

[5] Etimad Fadel, V.C. Gungor, Laila Nassef, Nadine Akkari, M.G. Abbas Malik, Suleiman Almasri, Ian F. Akyildiz,"A survey on wireless sensor networks for smartgrid",ComputerCommunications,71,2015,pp.2233,https://doi.org/10.1016/j.comcom.2015.09.006.

[6] Yasin Kabalci,"A survey on smart metering and smart grid communication",Renewable and Sustainable Energy Reviews,57,2016,pp.302-318,ISSN 1364-0321, https://doi.org/10.1016/j.rser.2015.12.114.

[7] Energy Networks, “An introduction to the smartgrid architecture model”. 2018. https://www.energynetworks.com.au/sgam/hybrid/index.htm?goto=1:8

[8] S. Hu, X. Chen, W. Ni, X. Wang and E. Hossain, "Modeling and Analysis of Energy Harvesting and Smart Grid-Powered Wireless Communication Networks: A Contemporary Survey," in IEEE Transactions on Green Communications and Networking, vol. 4, no. 2, pp. 461-496, June 2020, doi: 10.1109/TGCN.2020.2988270.

[9] Baseem Khan, Habtamu Getachew, Hassan Haes Alhelou,"Solving Urban Infrastructure Problems Using Smart City Technologies",Elsevier,Components of the smart-grid system, 2021,pp.385-397,https://doi.org/10.1016/B97-0-12-816816-5.00017-6. Thales, “Smart grid security issues: Addressing threats to seize benefits”, Digital identity and security, 2016.

[10] R. R. Ambekar and H. A. Mangalvedekar, "Power system state estimation by linear programming under false data injection attack and contingency," 2017

[11] L. Barbierato et al., "A Distributed IoT Infrastructure to Test and Deploy Real-Time Demand Response in Smart Grids," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 1136-1146, Feb. 2019, doi: 10.1109/JIOT.2018.2867511.

[12] R. Morello, C. De Capua, G. Fulco and S. C. Mukhopadhyay, "A Smart Power Meter to Monitor Energy Flow in Smart Grids: The Role of Advanced Sensing and IoT in the Electric Grid of the Future," in IEEE Sensors Journal, vol. 17, no. 23, pp. 7828-7837, 1 Dec.1, 2017, doi: 10.1109/JSEN.2017.2760014.

[13] M. Harvey, D. Long and K. Reinhard, "Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security," 2014 Power and Energy Conference at Illinois (PECI), 2014, pp. 1-8, doi: 10.1109/PECI.2014.6804566.

[14] Rafał Leszczyna, "Standards on cyber security assessment of smart grid",International Journal of Critical Infrastructure Protection,2018, 22,pp. 70-89,https://doi.org/10.1016/j.ijcip.2018.05.006.

[15] Ruland, K.C., Sassmannshausen, J., Waedt, K. et al. Smart grid security – an overview of standards and guidelines. Elektrotech. Inftech. 134, (2017). pp. 19-25. https://doi.org/10.1007/s00502-017-0472-8.

[16] International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 698-703, doi: 10.1109/ICIMIA.2017.7975555.

[17] Mohammad Ashrafuzzaman, Saikat Das, Yacine Chakhchoukh, Sajjan Shiva, Frederick T. Sheldon,"Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning",Computers & Security,97, 2020,101994. https://doi.org/10.1016/j.cose.2020.101994.

[18] J. R. K. R. and B. Sikdar, "Detection of Stealthy Cyber-Physical Line Disconnection Attacks in Smart Grid," in IEEE Transactions on Smart Grid, doi: 10.1109/TSG.2021.3082543.

[19] Hojabri, M.; Dersch, U.; Papaemmanouil, A.; Bosshart, P. A Comprehensive Survey on Phasor Measurement Unit Applications in Distribution Systems. Energies 2019, 12, 4552. https://doi.org/10.3390/en12234552

[20] Qu Zhaoyang, Dong Yunchang, Qu Nan, Li Huashun, Cui Mingshi, Bo Xiaoyong, Wu Yun, Mugemanyi Sylvère"False Data Injection Attack Detection in Power Systems Based on Cyber-Physical Attack Genes", Frontiers in Energy Research, 9, 2021, 57, DOI=10.3389/fenrg.2021.644489

[21] Song, G.; Chen, H.; Guo, B. A Layered Fault Tree Model for Reliability Evaluation of Smart Grids. Energies 2014, 7, 4835-4857. https://doi.org/10.3390/en7084835

[22] N. K. Singh and V. Mahajan, "Mathematical Model of Cyber Intrusion in Smart Grid," 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), 2019, pp. 965-969, doi: 10.1109/GTDAsia.2019.8715946.