International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 09 | Sep 2021 www.irjet.net p-ISSN: 2395-0072

REVIEW AND ANALYSIS ON INTELLIGENT SMART GRID POWER SYSTEM PROTOCOL

SHAHANA FEROZ JAHAN

Master of Technology, Dept. of Electrical and Electronics Engineering

---

ABSTRACT: The new and advanced system of existing grid systems is the smart grid, often known as a power system of the next generation. More importantly, by integrating modern computer and communication technology, the Smart Grid will boost the efficiency and confident Ness of future renewable energies systems and the responsiveness of scattered intelligence and demand. Besides the Smart Grid's invisible properties, cyber security is a key issue since millions of devices are networked via the communication networks using vital power plants that have an immediate influence on the stability of large infrastructure. An out-of-date infrastructure is the power grid, and the Smart Grid will offer many new features to fulfil the increasing power requirements of customers. The update of an electricity grid as complicated as the system can introduce new security vulnerabilities. This paper mentions cyber security activities related to the Smart Grid.

Key words: Smart grid, Security, Protocol, Power system.

1. INTRODUCTION

In the past 70 years, the electric power systems created by huge central generators are fed into a high-voltage interconnect network known as the transfer grid by means of generator transformers. Each unit is up to 1000 MW of hydro, nuclear or fossil fuel driven power.The transmission system transports electricity, frequently across huge distances and extracts and transfers that electricity in a number of distribution transformation systems to final systems to be delivered to end users. A highly full feeding load distribution system, with little communication and little LOM management, is practically fully passive. In other words, the voltages given for or the current spent by the charging, such as very high charges, are not monitored in real time (such as the steelworks and the aluminummelters). The interaction between loads and power systems is very minimal other than the load energy supply, whenever required.

In recent decades, the upgrading of electricity grids has not been consistent with industrial and social development that significantly raises demand for energy supply. Statistics[1] indicate, for example, that in the United States, energy production and consumption rose approximately two or three times between 1950 and 2008.The most demanding areas for power in the USA in 2008 are public and commercial services, industry and residential sectors. A key issue in addressing this surge in demand is that a number of fossil fuel sources (e.g., coal, oil and gas and renewable sources (solary, hydroelectronics, for instance) be handled efficiently[2]. [2]. Therefore the NIST has made national efforts to build a new generation, frequently called the Smart Grid[3]. the Standard and Technology National Institute (NIST).

In comparison to traditional power systems, Smart Grid is designed to fully integrate high-speed and bi-directional communications technologies in millions of electricity systems, to build an advanced metropolitan infrastructure (MIP) dynamic and interactive energy management infrastructure[9] and to meet demand[10]. However, such a strong dependence on the network of information unavoidably overcomes possible communications and networking systems weaknesses inside the Smart Grid.It increases the possibility that the reliability and security of the electrical system, the ultimate objective of the smart grid, would be compromised.For instance,[11] the probable admission of opponents into the network shows numerous serious impacts on the intelligent grid, from customer information leakage to cascade failures such heavy blackouts and the destruction of infrastructure.

1.1 Smart Grid Cyber Security Risks

In the current electricity system the intelligent grid delivers additional functions. However, there are various more security vulnerabilities to the system. The electricity we rely on from the grid is fundamental of our electrical dependency. The disruption of electricity supplies will have a considerable societal impact. Network safety is a key problem. Apart from its connectivity requirements, system automation, new technologies and data collecting, the Smart Grid presents a number of additional security challenges.

The network is the backbone of the intelligent system. This network connects the various elements of the smart grid to allow bidirectional communication. Networking of components causes security risks in the system, although many of the key features of the Smart Grid have to be implemented. The networking of many components will raise the complexity and the potential

for a new security vulnerability of the electricity grid. In addition, when all components are connected, the number of input points that can be used to access power systems grows.

In order to keep the electricity system automatically, the Smart Grid uses data transferred via the electric grid and software. Security difficulties occur from depending on the transmission system to the electricity grid network. Some elements demand real-time data, with undesirable effects on the electricity network due to delay or data loss. The system state management software also runs a risk of malicious malware, which can modify its functioning. A communications breakdown or the software of state governance can lead to power outage, injuries, or death in severe instances.

2. SMART GRID USE CASES WITH CRITICAL SECURITY REQUIREMENTS

We find that the present work focuses on either the substation or the SCADA systems in our study on cyber-security threats on electrical grids.However, in these two networks, communication possibilities in the Smart Grid are not restricted, such as wide range measuring network PMU synchronization and AMI meter readings. The NIST report suggests a number of core usage cases for safety consideration to facilitate research on Smart Grid Security. We have presented a complete Smart Grid vulnerability research based on these instances. First, we sum up usage instances with critical security requirements in two discrete classes: the communication of AMI and Home networks shall be based primarily in the context of the customer-Utility interactions. (2) transmission and distribution operation in which critical time communication is necessary for monitoring, control and safety; In the two classes accordingly, we discuss possible network security concerns.

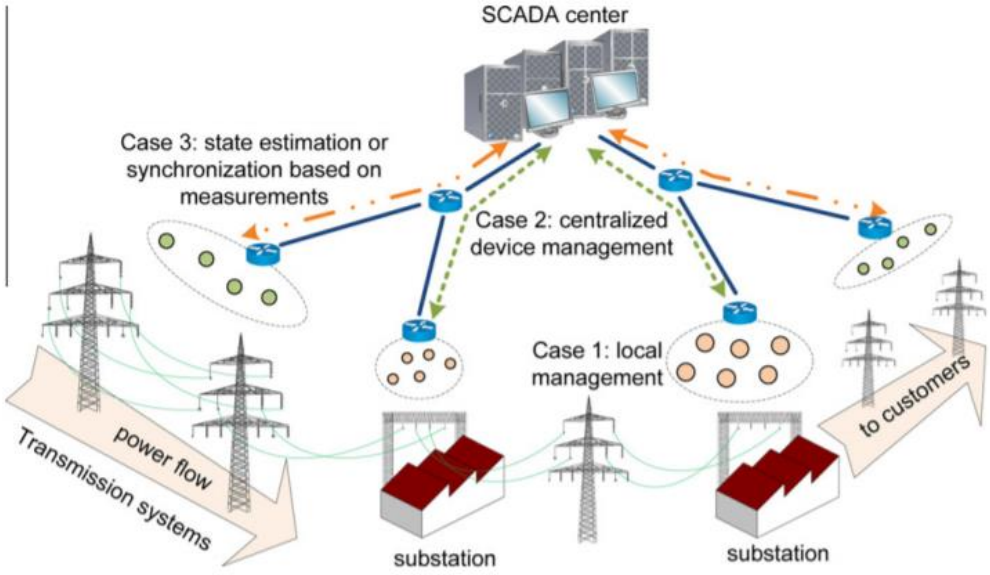

Fig. 1.1. Cases for key applications in Smart Grid distribution and transfer systems.

2.1 Distribution and transmission operation

The power and transmission networks are crucial components of electricity systems, since producers and customers may access the sound energy supply. The ScadaA sever is connected with these devices for centralized administration [14-20] and millions of important electric equipmentsare used for monitoring and control applications. According to this, the availability and integrity of such systems is critical, while data confidentiality is less important because private information to clients is not included. Three core usage situations with essential availableness and comprehensiveness criteria are also considered, as illustrated in the figures 1.1 and Table 1.

Table 1:Key applications in distribution and transmission networks with critical security requirements.

S.No	Network	Information delivery	Brief description
1.	Power substation networks	Single-hop, peer-to-peer	Local power equipment and devices monitoring, control, and protection in

			substations
2.	SCADA and wide-area power systems	Multi-hop, hierarchical	SCADA Center centralized power monitoring and control
3.	SCADA and large-scale power systems	Multi-hop, hierarchical	State assessment or synchronization based on raw data measurement (e.g., from PMUs)

These three applications comprise critical data flows for distribution of power and transmission networks. We discuss about numerous possibilities of communication and discuss potential security concerns in each situation.

The initial case is Case 1, which is the local control of an installation. A one-stop network of power stations provides access to external networks and dozens of IEDs that monitor all feeding devices continuously to make sure that they run reliably on the substation.The IED-to-IED (peer-to-peer) communications will trigger local protective actions once an aberrant condition has been found. DNP3 based on a serial-port (e.g., RS232) for legacy power systems is commonly used in power-to-power communication. The Ethernet-based IEC 61850 for the Smart Grid was, however, already used in substations for effective interchange of information. Furthermore, for power substation communication, the usage of wireless communications (e.g. Wi-Fi) is advocated. The following are possible cyber attacks:

DoS attacks: Since IEC 61850, IEDs sub - contracted via Ethernet and TCP / IP, such traffic floods, and TCP SYN attacks might become targets for door attacks. Local attacks by affected IEDs are however limited and may not have a substantial effect on communication performance, as the number of (tens) of IEDs in power stations is restricted. Consequently, the threat of large-scale DoS attacks, which are mostly from outside of a substation, overwhelms a substation network. In that respect, the TCP/IP DoS attacks primarily target the substation computer (the network gateway of the substation).

Attacks targeted at integrity: Spoofing attacks can lead to loss of availability and integrity in this one-hop network. Especially the spoofing attacks on the defensive system should be dealt with. If an IED is aware of a situation that is aberrant (for example high current), open and shut messages are transmitted to switches to preserve the power infrastructure at the stations and so balance the power charge (or simply break the circuit for protection).

The second scenario, called Case 2, concerns the monitoring, control and protection of systems not confined to local areas. This means that the SCADA Center for centralized administration can also be provided with electronic device status and measurements on local area systems. Fig. 1.1 depicts the Case 2, which is Internet equivalent and sensor network analogous, includes a standard server-client communication architecture within a multi-hop, hierarchic network. Thus, in Case 2, like in conventional communication networks, network assaults represent grave security vulnerabilities to the smart grid:

DoS attacks: As a sink node provided by data packets is the SCADA Center, it is an important aim to attack distributed DoS (DDoS) locally from multiple systems. In order to prevent DDoS attack, theSCADACenter may apply existing DDoS defense aggression strategies.

Attacks targeting integrity: For Case 2, communications between local power units and SCADA should be safeguarded through end-to-end authentication programs to avoid the substation of integrity attacks, including relays or mid-term attacks, when an assailant is trying to act as an intermediate node between the two nodes in the injection of fraudulent information.

3. LITERATURE RE IEW

3.1 Power System State Estimation Security

The state estimate of power system is also a sort of examination of cyber security. The intelligent grid is capable of controlling the physical qualities of electricity. This is done to keep the Smart System stable in the electricity grid. To make informed assessments and action, the Smart Grid must shape the current state of the electricity system. The PCS comprises the model for state estimates.

As the Smart Grid is used for electricity conservation, the security of the status estimate model of the power system is significant. The state-evaluation model of the power system is a tool for modeling sensor and agent data using the Smart Grid PCS. This means that safety objectives are also crucial for PCSs. Accessibility, followed by integrity, is very crucial. Security is the least critical goal since it adds a real-time system overhead.

The security of the state estimation model of the power system is a difficulty because erroneous input data can be received in the model. The insertion of erroneous data in the model has several reasons. The instability of the system and financial gains motivate the attackers. Many PCSs have the security problem of misdata injections and it is difficult to differentiate between true and fraudulent

data. There are usually systems which can discriminate between bad data and normal data, but they do not work effectively against attacks on false information.

3.2 Definition of Smart Grid

The Smart Grid concept brings together a variety of technology, end user solutions, policies and regulatory drivers. It has no single clearly defined definition. The Smart Grid[2] is defined by the European Technology Platform:

"A SmartGrid is a power network that integrates the actions of all users intelligently Connected - generators, users and both – to provide sustainable, inexpensive and secure sources of energy efficiently.."

3.3 Purpose of implement the S mart Grid now

The interest in the smart grid has grown from roughly 2005. Recognizing that ICT offers substantial prospects for modernizing the functioning of electricity networks, the energy industry can only be de-carbonised at a realistic cost, if monitored and controlled efficiently.

Moreover, several more detailed factors for stimulating interest in a smart grid have now coincided.

- Ageing assets and lack of circuit capacity
- Thermal constraints
- Operational constraints
- Security of supply
- National initiatives

3.4 Review of literature

The review of many PCS risk security measures in Jiaxi, Anjia and Zhizhong is also conducted in[1]. Work is needed in relation to PCS security risk so that current security concerns can be taken into account when updating systems or designing new systems. There is also a short description of the cyber safety issues associated with PCS[1]. This is, however, not the principal contribution and will be covered later in this study.

Many writers have worked in electrical power systems with PCS security risks. In this area, Watts worked[2] and reviewed the risks facing the current systems of electricity. The contribution of Watts to the project[2] is a review of cyber security vulnerabilities posed by electricity systems. The focus of this publication is on PCS safety hazards. Watts addresses the security concerns of electrical power systems with a clear and complete analysis. A list of security mitigation measures and any implementing concerns are also offered.

The advantage of the study of Watts [2] is that the PCS security and other network threats are well assessed. One drawback to the work is that the security hazards in older systems are significant. No new security issues in the Smart Grid can be addressed by this work. The first work in the intelligent grid is the text. It mostly includes energy infrastructure self-healing technology.

Redundant Smart Meter Reading

In [3] Varodayan and Gao proposed a method of securing redundant smart meter readings. Many clients worry about the accuracy of Smart Meter readings. One way of verifying Smart Meters' accuracy is to install a secondary power meter that compares its reads to the reads received from the Smart Meter by the electricity provider. It poses confidentiality problems. The problem is this technique. Attackers may intercept the information required to check Smart Meter integrity. Figure 2.1 shows the redundant feedback loop of the Smart Meter.

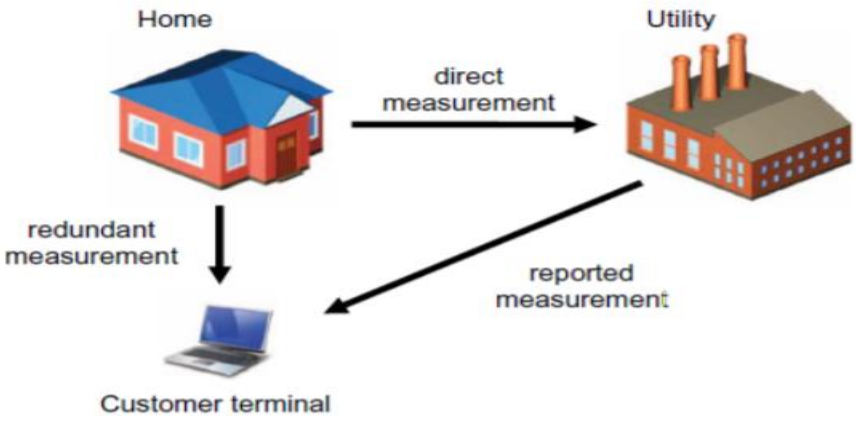

Figure 2.1: Smart Meter Redundant Meter Reading, reproduced.

Ding et al [4] explored control theory for industrial cyber-physique systems, outlining attack detection and control safety. Two physical solutions, including the creation of redundancy of contact systems and a more complicated system of communication security, were explored and tested on the physical hazards of communication-based security systems.

SG's major ICT, sensing, measuring, control and technological automation, energy supply and energy storage problems, were thoroughly examined by Colaket al.[5].Colak et al. The SG covered the various security aspects and solutions.

The author categorised the main components of the modern electricity system architecture as SCADA systems, AMIs, hybrid plug-in vehicles and communications protocols and standards in the literature[6]. They also showed the difference in security architecture and the aims, technologies and services quality between IT networks and smart power grid.

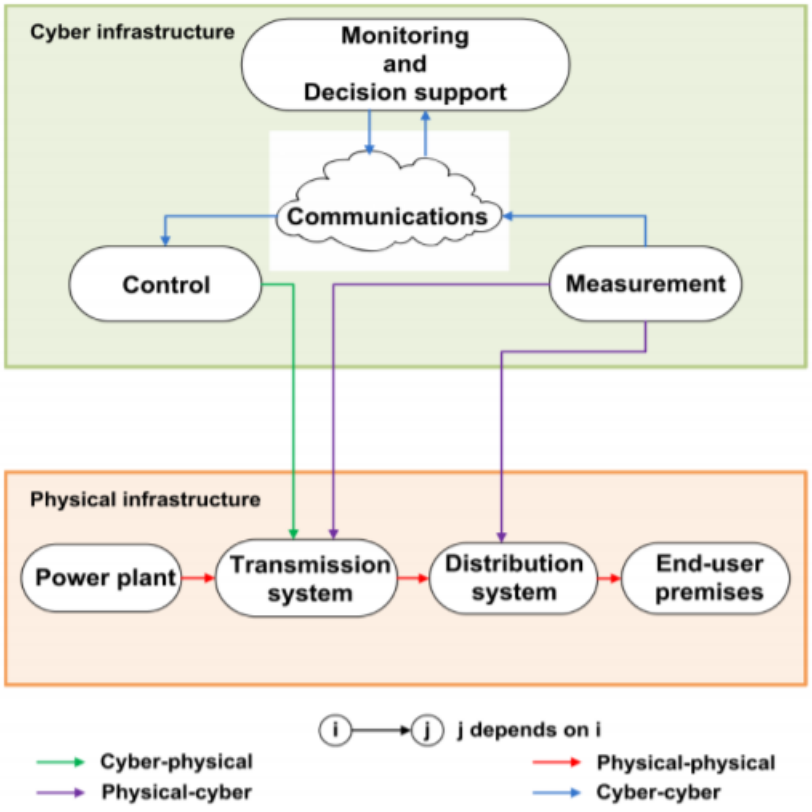

Fig. 2.2: Cyber-physical interdependency graph of a SG

In order to mirror addictions, Marashiet al.[7] selected a directed graph to show addiction where a rim between node I and node j arises if the components failure I influences the component J's functional state during the single phase. The time range is selected as being small enough to directly effect you and too short for a cascade. Figure 2.2 presents the dependency diagram for an abstract SG model. The edges of dependency may imply four types of dependency, cyber, physical, and physical.

Sou et al.[8] proposed that data with a small number of sensors should be injected poorly because of the overall restriction of the number of devices broken by the foe. In [8], the authors presented a graph theory based approach that helps to predict the number of signaux an attacker can receive and to reduce efforts to keep poor data attacks hidden.

Similarly, an attacker with physical access can no longer handle control commands by authorized encryption and firewalls. Approval can be compromised through physical protection of sensors and actuators. Unable to mitigate such an attack, standard anti jamming technologies. Furthermore, cybersecurity has no prescriptive tools to deal with SG's physical safety because it does not allow reliable and performance features. For instance, a reboot device is the traditional approach to compromise the detection of a software program.This can be problematic, though, by grid dynamics and stability.Alternatively, steps should be done in the cyber-physical system[9] to ensure smooth decline.

SG is exposed to a vast number of assaults on physical and running systems. Operating systems are generally constructed with insecurity characteristics. Most physical appliances are old-fashioned and lack memory space. Due to their limited computing capacity, they cannot implement high-level security methods. For instance, intelligent meters with restricted memory and computing resources are intended for reduced power use. Therefore, it is unable to support numerous critical security technologies, such as cryptography accelerators and random number generators. The whole system is compromised by a potential vector[10] if these components are affected.

In [11] the Petri Net was exhaustively analyzed and used to detect errors in SG modelling. The approach, however, was confined to collecting information about the security system for fault detection or failure recognition in the distribution system using DGs.

De Santis et al. [12] have also developed a system for detecting failures in medium-voltage feeder grid activity in Rome, Italy. Furthermore, for a particular kind of AMI encryption, the encryption solution for an advanced SG metering network (AMI).

The number of IoT connected objects [13] showed that breaches of cyber crime are rising dramatically. Therefore, up to 2.5 trillion dollars worldwide by 2022 the cost of data violations will rise. In addition, they project that by 2023, cyber records of 33 billion will be stolen and the figures will continue to increase.

N. Umekar, [14], Pooja The smart grid is designed to provide electricity from generating locations to active customers in a controlled, mart-oriented way. Demand response (DR) may offer a number of potential benefits internationally to system operation and extension as well as to market efficiency through promotion of client connection and response.

Md Musabbir Hossain, [15], As a crucial infrastructure, the SG demands extreme protection. In this study, we are expressly concentrating in a comprehensive and systematical examination on cyberphysical attack variants, interdependencies, requirements and security standards. To ensure safety at the beginning, a full architecture is needed efficiently. Some important steps should be taken to emphasize important results and achievements. First of all, a set of needs and criteria is required for the interconnection.

Goel, S., [16], Moreover, most power grid systems use an optical fibre-based ground wire that operates efficiently over long distances with lower losses and hence quickly, reliably, and safely. This facilitates the usage of SGs with optical fibers and eliminates the need for further connection. The present employed TCP/IP protocol failed to provide communications security across infrastructure components while meeting SG requirements.

Advances in grid power resilience were investigated in the use of micro grids to repair significant stress at Xu et al. and Shahidehpour et al. [17] (e.g. hospital, street lighting, internet, etc.). The study is directed at the feeds if the consequences of extreme events are not available (e.g. flood, earthquake, hurricanes, etc.).

According to Goel and Hong (2015) and Sharifi and Yamagata (2016) [18], some militant elements against resilience are natural catastrophes, severe temperatures, high and low fossil fuels, a global energy market instability, terror, sabotaging, vandalism, and so on. The 2012 sandy hurricane in the USA, with a total loss of 70 billion dollars, leaving about 8 million customers free of energy, is a good illustration while evident situations in vandalism, terrorism, and the war in countries such as Syria, Iraq, Afghanistan, Nigeria, etc.

Saha [19] It describes IoT, Cloud, independent control, and artificial intelligence tendencies. This work deals with the Internet need, wireless sensors and actuators synchronized to enable the use of IoT technologies in

combination with dispersed computers. Interesting is the regulatory component mentioned here.

Nahrstedt, K and others are operating [20] Submit an IoT mobility study, bearing in mind that this is a humane component and has numerous technical resources, such as the use of auto sensors and clever gadgets. We include these sources which are relevant to the study of electrical mobility because electric mobility is a key factor for the management of energy, the environment and, naturally, the improvement of the quality of lives of particularly vulnerable people, for example the most vulnerable, the elderly and others.

CONCLUSION

This review paper has analysed the different ways on the protection of smart grid power system by various authors. And also describes their reviews and used techniques for securing intelligent power grids.

REFERENCES

1. Y. Jiaxi, M. Anjia, and G. Zhizhong, Cyber Security Vulnerability Assessment of Power Industry. IEEE, 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper. htm?arnumber=4142474
2. D. Watts, "Security and Vulnerability in Electric Power Systems," in 35th North American Power Symposium 2003, 2003, pp. 559–566. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.4104&rep=rep1&type=pdf
3. D. P. Varodayan and G. X. Gao, "Redundant Metering for Integrity with InformationTheoretic Confidentiality," in 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 345–349.
4. Ding, D., Han, Q.-L., Xiang, Y., et al.: 'A survey on security control and attack detection for industrial cyber–physical systems', Neurocomputing, 2018, 275, pp. 1674–1683
5. Colak, I., Sagiroglu, S., Fulli, G., et al.: 'A survey on the critical issues in smart grid technologies', Renew. Sustain. Energy Rev., 2016, 54, pp. 396–405
6. Liu, J., Xiao, Y., Li, S., et al.: 'Cyber security and privacy issues in smart grids', IEEE Commun. Surv., 2012, 14, (4), pp. 981–997
7. Marashi, K., Sarvestani, S.S., Hurson, A.R.: 'Consideration of cyber–physical interdependencies in reliability modeling of smart grids', IEEE Trans. Sustain. Comput., 2018, 3, (2), pp. 73–83
8. Sou, K.C., Sandberg, H., Johansson, K.H.: 'Electric power network security analysis via minimum cut relaxation'. 50th IEEE Conf. Decision and Control and European Control Conf., USA, December 2011, pp. 4054–4059
9. Weerakkody, S., Sinopoli, B.: 'Challenges and opportunities: cyber–physical security in the smart grid', in Stoustrup, J., Annaswamy, A., Chakrabortty, A., Qu, Z. (Eds.): 'Smart grid control: overview and research opportunities' (Springer International Publishing,Switzerland, 2019), pp. 257–273
10. Mrabet, Z.E., Kaabouch, N., Ghazi, H.E., et al.: 'Cyber-security in smart grid: survey and challenges', Comput. Electr. Eng., 2018, 67, pp. 469–482
11. Calderaro, V., Hadjicostis, C.N., Piccolo, A., et al.: 'Failure identification in smart grids based on Petri net modeling', IEEE Trans. Ind. Electron., 2011, 58, (10), pp. 4613–4623
12. De Santis, E., Rizzi, A., Sadeghian, A.: 'A learning intelligent system for classification and characterization of localized faults in smart grids'. IEEE Congress on Evolutionary Computation (CEC), Spain, July 2017, pp. 2669–2676
13. Moar, J.: 'The future of cybercrime & security: threat analysis, impact assessment & leading vendors 2017–2022 full research suite' (Juniper Research,UK, 2017)
14. Pooja N. Umekar, 2017, "Review on Smart Grid and Cyber Security".
15. Md Musabbir Hossain, 2019, "Cyber–physical security for on-going smart grid initiatives: a survey".
16. Goel, S., Hong, Y., 2015. Security Challenges in Smart Grid Implementation Smart Grid Security. Springer, pp. 1–39.
17. Xu, Y., Liu, C.C., Schneider, K., Tuffner, F., Ton, D., 2016. Microgrids for service restoration to critical load in a resilient distribution system. IEEE Trans. Smart Grid PP (99), 1, http://dx.doi.org/10.1109/TSG.2016.2591531.
18. Sharifi, A., Yamagata, Y., 2016. Principles and criteria for assessing urban energy resilience: a literature review. Renew. Sustain. Energy Rev. 60, 1654–1677.
19. Saha, H.N.; Mandal, A.; Sinha, A. Recent trends in the Internet of Things. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–4.
20. Nahrstedt, K.; Li, H.; Nguyen, P.; Chang, S.; Vu, L. Internet of Mobile Things: Mobility-Driven Challenges, Designs and Implementations. In Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, 4–8 April 2016; pp. 25–36.