Review of cyber-attacks on smart grid system

*Shreyas Mavale[1], Jayesh Katade[2], Nachiket Dunbary[3], Sparsh Nimje[4,] Balaji Patil[5]

School of Computer Engineering and Technology,
MIT World Peace University, Pune , India.

[1] *shreyasmavaleofficial@gmail.com; [2] jkatade@gmail.com ;
[3]nick.dunbray@gmail.com ; [4] sparshn00@gmail.com ; [5] balaji.patil@mitwpu.edu.in .

Abstract. With increase in use of technology along with new inventions, consumption of energy required is increased in exponential manner. In recent development of communication infrastructure in smart grids, it leads to new issues in physical power system related to cyber security. In traditional ways to handle cyber-attacks on power system, it generally involves separation of cyber domain and physical domain. Therefore it is very important to have unification of cyber and physical power system. So to handle these issues cyber physical power system (CPPS) is introduced. The CPPS mainly consist of core physical power system tightly integrated with cyber system. The purpose of CPPS is to monitor and control the smart grids efficiently and reliably.

CPPS consist of various phases such as power transmission, power generation, power distribution, utilization of power, Supervisory control and data acquisition system (SCADA), utilization of power, etc. These phases in smart grids are prone to cyber-attacks so, it is important to summarize, analyze and monitor cyber-attack methods on CPPS for the defense against different cyber-attacks. In this paper, we provide a comprehensive review of different kinds of cyber-attacks on physical power system phases. Also paper analyses various scenarios of cyber-attacks on systems and equipment such as SCADA system, smart meters and communication system. Finally, according to several characteristics of cyber-attack methods, some preventions and detection methods are presented.

Keywords: Cyber-physical system (CPS), Cyber physical power system (CPPS), Cyber security, Cyber-attack, Smart grid, Supervisory control and data acquisition (SCADA), Distributed denial of service (DDoS), False data injection (FDI).

1 Introduction:

Now-a-days with increase in rate of natural disasters such as floods, hurricanes, tornados are compromising the reliability and performance of electricity grid. With ongoing industrial 4.0 revolution, use of internet get exponentially increased which leads to whole new sector known as Cyber Security and further which leads to soaring risk of intentional physical cyber-attack on smart grids. The advancements in smart grid technologies also expected to expand cyber flaws and vulnerabilities of power grid system through remote access points. Cyber-attacks on Ukraine's physical power system in 2015 is great example of how cyber security compromisation can affect whole power system. More than thousands of homes and other facilities experienced a power outage for days. This cyber-attack was done by malware known as 'BlackEnergy' which was installed on central control center. [1]. Also attacks on substation transformers in California are recent examples in cyber physical attacks on smart grid system.

Compared to physical intrusions in power system, cyber attacks are hard to locate as attackers can be anywhere with network access. Cyber-attacks mostly depend on configurations of communication network in power grid. As we cannot perform different kinds of scenarios and testing on physical power system directly, different types of testbeds have been developed for power grids which serve the purpose of analysing, modelling, testing and impacts on other subsystems.

With integration of cyber system and physical power system, information sharing and communication network between them become important sector. Because of large-scale usage of communication technologies in physical power system, automation within it and remote access control of system have been gradually increased. Because of installation of intelligent electronic devices (IEDs) on physical power grid system, physical power system operators are able to control and monitor whole system from a remote control center. All of these control and monitoring centers are based on information and communication technology (ICT).

The remainder of this paper is organized as follows: The literature survey is represented in section II. Goals of in smart grid system are presented along with overview of whole cyber physical system (CPS) in section III. Section IV presents CPPS system architecture along with various types of levels in CPPS model. Section V gives an outlook of the applicable scenarios of different cyber-attack in CPPS. Finally conclusion is in Section VI.

2 Literature survey:

In cyber physical attacks, detection and prevention are being the subjects of comprehensive research in recent years [2] and various attacks which specially targeting stability of power systems have been studied [3]. Cyber-attack mainly targets the information principles which are confidentiality, integrity, and availability.

Liu et al. modeled local FDI attacks, which made use of reduced network information and passed the examination of the state estimator [4]. Zhang et al. presented a data integrity attack detection method based on a grey relational analysis method, which evaluated the correlation between measurements and control variables [5]. According to ISA 84/IEC61511 [6], functional safety is aimed toward protecting and monitoring devices from accidental failures or failings so as to realize or maintain a secure state of the system. Security refers to cyber security. Consistent with ISA99, cyber security attempts to guard the cyber environment of the authorised users or organization, including networks, information in storage or transit, devices, processes, all software, etc.

One of the most important studies related to cyber security in power grids is false data injection (FDI). work of Dán and Sandberg [7], who study the problem of identifying the best k sensors to protect in order to minimize the impact of attacks, and Kosut et al. [8], who consider attackers trying to minimize the error introduced in the estimate, and defenders with a new detection algorithm that attempts to detect false data injection attacks.

In 2020 Yohanandhan, R.V. and his team, explained different cyber-attacks and analysis, modeling and simulation of those attacks [9]. North American Electric Reliability Corporation (NERC) states various assets as well as rules and regulations for protection and smooth operation of physical power system [10]. Jahromi, A.A. and team in 2020 address the vulnerabilities which are present in communication-assisted protection scheme. DDoS, FDI, etc. these kind of vulnerabilities can be found in this scheme [11]. In 2016 Jokar P. and his team used a consumption pattern based energy theft detector which doesn't invade customer's privacy and use to detect malicious consumption patterns. They also used anomaly detectors and transformer meters to make algorithm robust against malicious changes [13]. Amin, S. and his team gave elaboration about how parameter tampering in meters can affect whole power consumption of customer also about consumption test, the nonparametric cumulative sum (CUSUM) algorithm to evaluate electricity theft detection system [14]. In 2008 Ten C.W. and his team emphasizes on three level substation model for cyber system. Ten C.W. also explained about reducing password threshold for lower probability of intrusion attempts [19].

3 Smart grid:

With advancements in technologies integrating with physical power system, new term is introduced as smart grids. Smart grid is same as electrical grid which consists of several of components such as smart distribution system, advanced metering system for power distribution and integration of different circuit breakers.

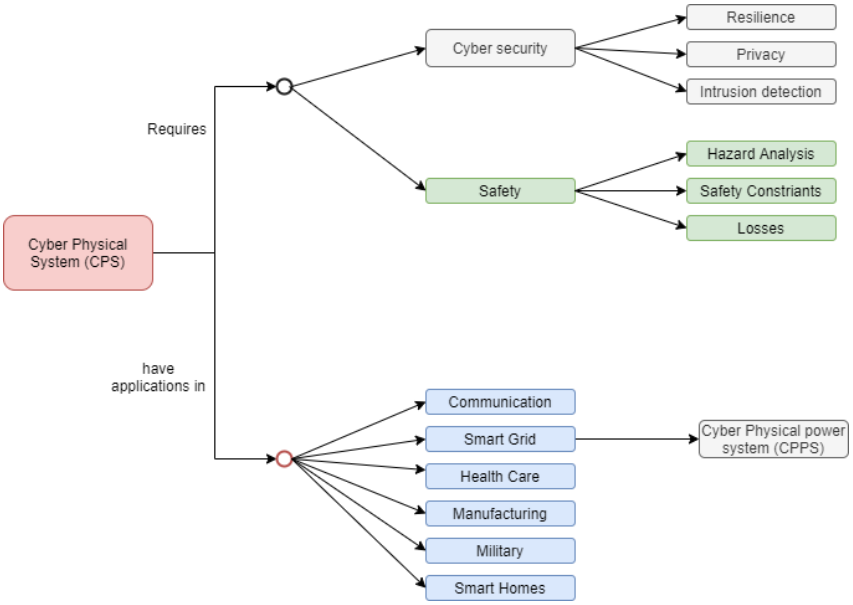

Fig1. Overview of cyber physical system.

Now a day's cyber physical system (CPS) is widely used in various sectors. As CPS is mainly integration of sections such as physical systems and cyber system. CPS consists of embedded systems which uses various wireless network protocols for real time monitoring. CPS has not only applications in power grids sector but also in public health sector, safety and precautions sector, water system, military, etc. There are many reasons for updating in electric power grid system to smart grid system. Some of them are as follows:

i. Efficiency: With increase in demand for electricity every year it is necessary to minimize power losses and optimize power transmission. Efficiency also depends upon several factors such as implementation of new technologies and renewable sources for power generation.

ii. Reliability: Power grid system should be reliable and able to provide required power supply to given areas. With the help of newly developed sensors and actuators, power grid system can receive real time data of operations and detection of attacks can be done in better way. For example, smart meters are installed to monitor consumption of energy not only inside of house but also of outside.

iii. Consumer choice: There should be transparency between consumer and power provider, as most of the consumers only receive monthly bills and updates related to their energy usage. Customers are also not aware about their energy consumption and prices they are paying at different times in a day. Also they do not know about how much energy is generated through renewable resources.

Smart grid systems are designed to overcome above problems, but while integrating traditional physical power systems with modern technologies it also gives birth to new problems in cyber sector such as loss of energy, false billing to customers for energy usage, etc.

4 System architecture of CPPS:

In smart grids it is very efficient to manage system remotely as well as organizations can easily track the power consumptions data. To improve efficiency and stability in smart grid system, demand response program provides a mechanism to control energy usage by providing incentives to consumers for reducing energy consumptions during peak hours. At present, these demand-response programs are mainly used by government and commercial consumers for large buildings and areas. And functioning of these programs are practically based on sending incentive signals vi calls or messages. For example, a company can send signals to consumers that to lower their consumption of energy in peak times.

Consumers with energy generation and storage capabilities are known as prosumers. Demand-response program can be extremely useful for prosumers as they can exchange energy with each other and can maintain their own security protocols. Many vulnerabilities and problems occur while controlling physical power system with remote technologies, it leads to a term called Cyber physical power system (CPPS).

It is integration of cyber security and physical power system. CPPS mainly cover various areas such as transmission, distribution and power generation. CPPS is integration of computation, networking and physical power system which includes different types modelling, innovations and creations. CPPS uses embedded computer network for communication, computation and organization of physical power system. In CPPS there are three levels of interaction.

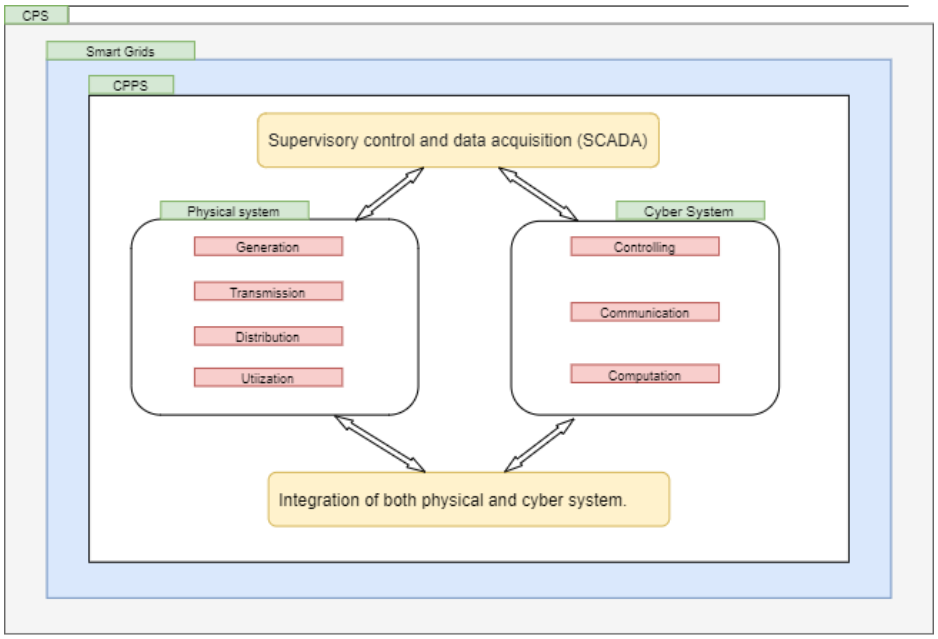

Fig2. Overview of Smart grid system

1] Level 1:

First level of CPPS is between transformer, generator and transmission line, etc. with controller of physical power system. Controller of physical power system calculates the control signal and also fetches information from other system components. This information is further used optimize the operations of power system.

2] Level 2:

Second level of CPPS is between communication infrastructure and physical power system. Communication infrastructure works with coordination of sensors, actuators, controlling units and communication units. There are some challenges in communication infrastructure such as time delay, bad data and loss of data, etc. which may affect operations of physical power system.

3] Level 3:

Third level of CPPS is between cyber security system and communication infrastructure. Components of cyber security system are communication servers, master servers, communication structures, computing stations, application softwares, cyber-attack and defense models, etc. This layer performs actions like operation planning, analysis of power system, optimization of voltage and power supply, monitoring of system, etc.

In CPPS, distribution system and network transmission is very huge, complex and heterogeneous which generate possibility of cyber-attacks. Various components of cyber security system like operating systems, remote access points, connection ports, etc. are prone to cyber threats. It is extremely important to calculate the impact cause by cyber-attack on physical power system as attack does not directly impact physical power system but causes instability in whole system.

Traditional methods used in power system are totally based on physical parts of power grids. Optimization of CPPS is needed for ensuring secure and safe operation of power grid.

With the help of simulation tools and testbeds we can predict the impact of cyber-attack and also analyze it. The risk factor of cyber-attack by vulnerabilities and their impact is shown as [9]

$$R = [T] * [V] * [I]$$

Where,
R stands for risk.
T stands for threat to power system.
V stands for vulnerability.
I stands for impact.

Here vulnerability can be of various types and threat can evaluate as motivation of attack and resources available for attack, etc. Developing an integrated risk assessment modeling framework is main motive of research in cyber security.

5 Scenarios of different cyber-attacks in CPPS:

CPPS consist of different phases as generation, transmission, distribution, communication, computation and controlling, etc. Many phases are vulnerable to cyber-attacks such as DDOS, false data injection, etc. which can compromise whole system. Cyber-attacks on smart grids are mainly on fallowing phases.

A. Intelligent Electronic Devices (IEDs)
B. Advanced metering system
C. Supervisory control and data acquisition (SCADA)
D. Communication channel

In Cyber-attacks on above phases, it causes compromisation of communication networks, malfunctioning of sensors and actuators, compromisation of whole system.

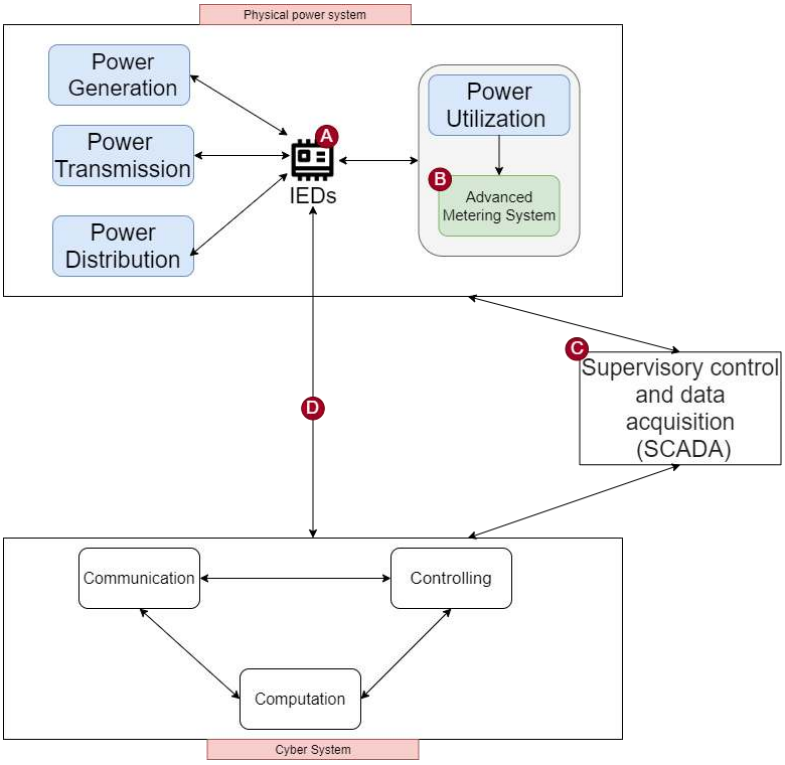

Fig3. Attack prone systems or devices in CPPS

5.1 Intelligent Electronic Devices (IED) :

In recent years' traditional devices which were used in power systems have been replaced by intelligent electronic devices (IEDs) and intelligent controllers. IED provide remote control centre and digital communication. North American Electric Reliability Corporation (NERC) succeeds to develop a system called critical infrastructure protection (CIP) for "identification and protection of important cyber assets for reliable operation of physical power system [10].

IEDs are connected with phases of physical power system which are power generation, power transmission, power distribution which can be access remotely. Generally, most of the power substations are unmanned and operated via remote control technologies; there are high chances of cyber-attack on substation communication networks (SCN). Once an attacker exploits the system via methods like password cracking, malware installation, they gain access to important data of substations such as maintenance records, status of operations, system topology, measurements and operating plans of system). If there is vulnerability in communication system, then attackers can access multiple substations at a time which may lead to triggering number of cascading events on physical power system causing a blackout.

DDoS or false data injection attack extend the duration of fault clearing time at critical transmission lines by different methods such as packet flooding or by alternating signals which may leads to blackout and instability in smart grid system. This kind of attacks could be occurring with help of malware injection or adding new communication device which can access the network channel [11]. DDoS corrupts network with extensive packet flooding which makes internal communication of power stations impossible.

Also there was certain type of attack where attacker used electromagnetic interference to cause an actuator to follow his commands. Traditionally most of the attacks on CPPS are software based attacks, but system can be compromised by physical way by injecting false signals or injecting malware into system. This types of attacks are known as transduction attacks. Attacker can manipulate system and its environment by altering sensor data and injecting false data.

5.2 Advanced metering system (AMI) :

AMI is a smart metering system for customer-side which helps to build relationship between power consumer and providers directly. Traditionally used meters are mainly used for recording usage of power by consumer but smart meters are able to record not only energy flow inside of house but also out of house. So with the help of smart meters consumers can become producers by installing solar panels or wind generators.

Smart meter can be also work as a controller and home appliances can be controlled by mobile phones with the help of internet. It can be also serves as router in home area network (HANs). Now-a-days most of the smart meters are developed on basis of ZigBee protocol which is defined in IEEE 802.15.4 [12]. ZigBee is mainly developed for low power consumption devices, so it has limit for communication distance.

As smart meters are connected with internet, cyber-attacks are most likely to happen on that certain point. ZigBee end-device sabotage attack is possible by activating sensors to send messages every time when device turn on from sleep mode. So by this method a sensor which is under attack is forced down to reply the malicious user and compromise system. Also attacks such as DoS, DDOS, Sinkhole, and wormhole are executed to disconnect nodes from connected networks. In Sinkhole, attack node which is compromised will attract other network packets to create confusion in routing phase. While in wormhole attack node which is compromised will receive malicious code and forward malicious packets to all connected network. [13]

Smart meters can be compromised while attacker can modify the values for reading of energy consumptions. Different detection systems have been developed for energy theft [14–16]. It causes increase or decrease in billing of energy consumption, cutting down power of different locality remotely, etc. One of the solutions for energy theft is by monitoring load profiles and recognizes changes such as drastic change in power usage at certain time or unusual power usage readings by meters.

5.3 Supervisory control and data acquisition (SCADA) :

For online operation and monitoring of the critical infrastructures, SCADA systems are deployed in various industries, like power, oil and gas, transportation and manufacturing. Abnormal operating conditions of an influence system are often detected from a foreign location through a SCADA system. Thus, the reaction time to correct an abnormality is reduced. Additionally, utilities can reduce routine and emergency visits of field crews to remote sites.

In SCADA systems many critical vulnerabilities may occur such as disrupts in communication, leakage of critical information, injection of malicious codes and commands, false data injection in control center of system. In any cyber attacks on physical power system vulnerability index is calculated based on effect caused by the intrusion on power grids.

Most crucial attack in power system is when attacker gains access of SCADA system and launches different attacks which may cause catastrophic damages. With inclination of new technologies towards Internet Protocol (IP) based systems, results in new vulnerabilities associated with SCADA system. Awareness and personnel trainings for SCADA system are very crucial as the exponential increasing dependency on communications over Internet protocols. [17] [18]. As CPPS testbeds, SCADA testbeds are also effective solution for detecting vulnerabilities and analysis of them. [19]. But there is no systematic method for modelling and analysis of critical assets in power system infrastructure.

Remote access systems have capability of controlling other machines or systems via network. An intrusion in substation enables an attacker to create false data to cause unnecessary operations on internal devices. An attacker uses some of the following methods to get entry in network layer of power systems:

- Port Scanning: With the help of port scanning admins can determine the ports on machine which are in listening state for potential access.
- War dialing: It executes different scripts in surrounding networks to detect connection, which can be threat to power system

Traffic sniffing: Tools such as Wireshark are used as network analyzer to capture network traffic.

- Password cracking: In this method attacker uses randomly generated password list to gain unauthorized access.

Different types of attacks on SCADA system are as follows.

Directed attacks. Attacks which have short term effects on control system are known as directed attacks. This type of attacks leads to shutting down of SCADA system for certain amount of time or deletion of system files. DoS and DDoS attacks are examples of directed attacks.

Intelligent attacks. Attacks which are well planned and executed with proper management are known as intelligent attacks. In this type of attacks, attacker must have in- depth knowledge about internal working of system. This type of attacks can cause major power outage which may leads to catastrophic.

Access point vulnerability. An access point provides the port services to determine a connection for an intruder to penetrate the SCADA computer systems. The vulnerability of a scenario, through an access point is evaluated to work out its potential impact. The impact factor, represents the extent of impact on a system when a substation is removed, i.e., electrically disconnected, by switching actions because of the attack [20].

Most crucial element of cyber security is the software on which system is running. The number of vulnerabilities increases every year, so control system should be updated and upgraded. Vulnerabilities of Operating System are also most important as they can establish a malicious connection and can be easily compromised. In OS well known ports are from 0 to 1024 for establishing connection. Attacker generally uses unused ports and services to gain the access of control system. Cyber-attack can cause following consequences:

- Loss of information and loss of load
- Economic losses
- Damage of equipment.
- Line failures
- Instabilities in frequency.
- Increase in cost of operations.
- Blackout for great amount of time.

SCADA system security model. SCADA systems specifically have password policies and some firewall rules for security purpose. There are two sub models present as 1] Firewall model and 2] Password model.

Firewall model. In firewall model it mainly monitors packets between network layer and use different types of filters according to security levels. Firewall rules are mainly configured for filtering out unwanted traffic.

Some of the rules are as follows:

a) Ports which are currently used in service

b) IP address or range of IP addressed which are connected to system.

c) Types of protocol used in system.

Because of high volume of traffic, it is impossible to monitor or administer every detail in network. Hence firewall analyzer is installed to detect abnormal traffic in network.

*Password Model***.** It is used to locate previous attempts of breaking into system and analyze the log files which will help control system to develop a new model for prevention. Password model detect the response rate of machine with the help of central processing unit (CPU) and then study the behavior of attacks occur over a certain period of time.

Cyber-Net is a combination of firewall and password model. In the SCADA system there is already preinstalled algorithm present for minimizing the random error generated by sensors and actuators known as bad data detection. False data injection can cause malfunctioning of system by evading that detection algorithm and sending false data.

5.4 Communication channel:

Attacker can compromise communication paths between controllers, sensors and actuators with the help of DoS, false data injection attacks. Also, attackers can block or delay the controlling signals which further delay the future operations. Traditional methods in CPPS focus on separate parts of physical power system. Therefore, it is important to have integrated system for monitoring transmission, generation, and distribution combinely.

In Physical power system firewall work as a front-line defense for protection of system as it filters packets such that a packet can pass firewall if it fulfills the rules defined by the user of system. If attacker is trying to do IP scanning or port scanning, these events are recorded as log file in system. But firewall only examine and detect anomalies in lower layer of communication i.e., network layer, so attacks which are on application layer or transport layer cannot be detected easily. Different types of IDEs have been proposed for communication system. [21].

Types of Intrusion detection system (IDS) in communication channel. Physical power system is mainly consisting of substations, power generation units, distribution systems and transmission systems while cyber systems consist of digital communication of data and SCADA system. In smart grids for different protection range, different types of IDSs are used such as for substations:

• Network Based IDSs:

Network based IDSs mainly monitor and analyze network traffic in local area network. It mainly checks header information of packets and content of packets which are passing through network layer.

• Host Based IDSs:

Host Based IDS is installed individually on more than one data servers. Host based IDS mainly detects interruptions in measurements and status of physical devices. Host based IDS (HIDS) can utilize log files to detect anomaly in power system.

All of the above cyber-attacks on smart grid phases, their prevention methods and impacts are summarize in table given below.

Sr. No.	Phases	Attacks	Preventions and Detection	Impacts
1	Generation Transmission Distribution (IEDs)	1. DDoS 2. DoS 3. FDI [4] 4. Alternating frequency signals 5. Malware Injection [8] 6. External 7. Electromagnetic interferences. 8. Transduction attacks [9].	1. Isolation of system to private network. 2. Bump-in-the-wire [9]. 3. Cryptographic algorithms 4. Firewall installations 5. Use of blockchain technology. 6. CPPS testbeds [18].	1. Instabilities in frequencies 2. Major economic losses 3. Increase in case of operations 4. Exploitation of maintenance records, status of operations, system topologies and operating plans of system. 5. Blackout and instabilities in smart grids.[1]
2	Power Utilization (AMI)	1. DDoS 2. Sinkhole 3. Wormhole [7] 4. Absolute slot number 5. Time synchronization tree attack 6. DoS	1. Monitoring of load profiles and recognize drastic changes. 2. Detect unusual power usage readings.	1. Modification of meter reading values [13]. 2. Cutting down of power in locality 3. Modification of readings of power generation [15].
3	SCADA	1. DDoS 2. DoS 3. Injection of malware or trojan on system software 4. FDI 5. Attack on system software	1. Firewall Model 2. Password Model 3. Cyber-net Model 4. Bad data detection algorithm[19].	1. Loss pf load. 2. Line failures.[10] 3. Compromisation of Whole system. 4. Blackout for great amount of time.
4	Communication network	1. DDoS 2. DoS 3. Man in the middle attack 4. Identity spoofing 5. FDI	Intrusion detection system such as network based IDS and host based IDS [21].	1. Compromise communication paths between controllers, sensors and actuators . 2. block or delay the controlling signals.

Table1. Attacks on CPPS phases and impact

6 Conclusion

Cyber security plays very vital role in cyber physical power system (CPPS) and has wide attention from governments and academics. The proposed paper is focused on different kinds of cyber-attacks possible on smart grid system along with preventions on them and impacts of those attacks. During our research work, we found vulnerabilities in smart grid phases:- with compromising sensors and actuators, exploiting a particular type of packet, attack on IEDs, injecting malware or Trojan in system, remotely reconfigure/program network nodes as the attacker wishes, hence compromising data communication security of the network. After analyzing various attacks on different phases of smart grids, we conclude that most of the phases are vulnerable to mainly DoS and DDOS type of attacks. This paper also discusses about prevention and detection methods against cyber-attacks.

It is necessary to understand and study the principles of different attacks and develop effective security. Research on security and safety integration in CPPS is still in progress and also needs future improvements and supplementation. A gap identifies in existing methodologies on security and safeties of physical power system are as follows:

i. Lack of security and safety measurements in cyber physical system. More research is needed in CPPS modeling and analysis.

ii. No unified method for detection and prevention of attack on physical system.

iii. Most of existing technologies for risk assessment are not able to find potential threats and cannot predict attack scenarios and evaluate probability of attack.

iv. Most of the previous works in CPPS are not able to differentiate between errors of risk caused by incidents and malicious attacks.

v. Insufficiency in statistical information on intrusion detection attempts to invade the energy infrastructure. This type of limitations can be removed with the help of test beds development. As test beds are powerful evaluation and development tools in field of cyber physical power system.

To achieve high performance rate and high efficiency in physical power system CPPS is used. CPPS has gained considerable amount of attention in recent years for modeling, analyzing and simulation. Highly complex designs on testbeds can reduce performance of power system. So it is important to detect and prevent cyber-attacks against smart grids.

References

1. Assante, M.J. (2016). URL https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinatedattack-on-the-ukrainian-power-grid#.
2. Khaitan, S.K., Mccalley, J.D., and Liu, C.C. (2015) *Cyberphysical systems appraoch to smart electric power grid*, Springer-Verlag, Berlin Heidelberg.
3. Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., and Purry,K.B. (2011) Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, **6** (1), 2–2, doi:10. 1504/ijsn.2011.039629. URL.https://dx.doi.org/10.1504/ijsn.2011.039629.
4. Liu, X., Bao, Z., Lu, D., and Li, Z. (2015) Modeling of local false data injection attacks with reduced network information. *IEEE Trans. Smart Grid*, **6** (4), 1686–1696.
5. Zhang, Z., Wang, Y., and Xie, L. (2018) A novel data integrity attack detection algorithm based on improved grey relational analysis. *IEEE Access*, **6**, 73 423–73 433.
6. IEC 61511: 'Functional safety - safety instrumented systems for the process industry sector', 2016
7. Dán, G. and Sandberg, H. (2010) Stealth attacks and protection schemes for state estimators in power systems. *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*.
8. Kosut, O., Jia, L., Thomas, R., and Tong, L. (2010) Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*.
9. Yohanandhan, R.V., Elavarasan, R.M., Manoharan, P., and Mihet-Popa, L. (2020) Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access*, 8, 151 019–151 064, doi:10.1109/access.2020.3016826. URL https://dx.doi.org/10.1109/access.2020.3016826.
10. North American Electric Reliability Corporation (NERC). CIP Standard. Available online: http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf (accessed on 2 May 2006).
11. Jahromi, A.A., Kemmeugne, A., Kundur, D., and Haddadi, A. (2020) Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. *IEEE Transactions on Power Systems*, **35** (1), 440–450, doi:10.1109/tpwrs.2019.2924441. URL https://dx.doi.org/10.1109/tpwrs.2019.2924441.
12. (2007) Wireless Medium Access Control (MAC) and PHY Specifications for Low Rate Wireless Personal Area Networks (WPANs). *IEEE Standard*, **802**, 30–30.
13. Jokar, P., Arianpoo, N., and Leung, V.C.M. (2016) Electricity Theft Detection in AMI Using Customers' Consumption Patterns. *IEEE Transactions on Smart Grid*, **7** (1), 216–226, doi:10.1109/tsg.2015.2425222. URL

https://dx.doi.org/10.1109/tsg.2015.2425222.
14. Amin, S., Schwartz, G.A., Cardenas, A.A., and Sastry, S.S. (2015) Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure. *IEEE Trans. Smart Grid*, **35**, 66–81.
15. Liu, Y. and Hu, S. (2015) Cyberthreat Analysis and Detection for Energy Theft in Social Networking of Smart Homes. *IEEE Trans. Smart Grid*, **2**, 148–158.
16. Amin, M. (2002) Security challenges for the electricity infrastructure. *Computer*, **35** (4), supl8–supl10, doi:10.1109/mc.2002.1012423. URL https://dx.doi.org/10.1109/mc.2002.1012423.
17. URL http://www.tswg.org/tswg/ip/21StepsSCADA.pdf.
18. Davis, C.M., Tate, J.E., Okhravl, H., Grier, C., Overbye, T.J., and Nicol, D. (2006) SCADA cybersecurity test bed development. *Proc. 38th North Amer. Power Symp*, pp. 483–488.
19. Ten, C.W., Liu, C.C., and Manimaran, G. (2008) Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems*, **23** (4), 1836–1846, doi:10.1109/tpwrs.2008.2002298. URL https://dx.doi.org/10.1109/tpwrs.2008.2002298.
20. & Sun, C.C., & Liu, C.C., and Xie, J. (2016).
21. A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine," Electronics, vol. 9, no. 1, p. 173, Jan. 2020.