U.Porto Journal of Engineering, 8:2 (2022) 51-64
ISSN 2183-6493
DOI: 10.24840/2183-6493_008.002_0005

Received: 21 September, 2021
Accepted: 20 October, 2021
Published: 28 April, 2022

Impact of Cyber-Attacks on Economy of Smart Grid and their Prevention

Soumya Mudgal[1], Saurabh Pranjale[2], Tharun Balaji[3], Syed Aamir Ahmed Ahmed[4], Neeraj Kumar Singh[5], Praveen Kumar Gupta[6], Vasundhara Mahajan[7]

[1]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (mudgalsoumya@gmail.com) ORCID 0000-0003-4783-0012; [2]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (saurabhpranjale@gmail.com) ORCID 0000-0002-9338-145X; [3]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (tharunbalaji@gmail.com); [4]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (syedaamir0801@gmail.com) ORCID 0000-0001-6482-2124; [5]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (neerajksssingh90@gmail.com) ORCID 0000-0002-6005-1016; [6]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (praveenpragati12@gmail.com) ORCID 0000-0002-9128-4365; [7]Electrical Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395007, India (vasu.daygood@gmail.com) ORCID 0000-0002-2698-6096

Abstract

The technical improvements in modern power systems by the use of smart sensors, smart meters, multi-direction communication networks, and computers have given birth to the cyber-physical smart grid networks. Any attack on the grid is a threat to the grid's operation and the data collected from it. Therefore, the security of this diverse network is the primary concern. Two attacks on a smart grid network tested in this paper are: Denial of Service (DoS) and Man In The Middle (MITM). Remote monitoring of the smart meter under either of the attacks indicates load fluctuations on the consumer side. It is seen that the location of these fluctuations is not limited to the area under attack. The supplier has to bear the economic effects. This paper discusses the cyber, physical and monetary impact of different cyber-attacks on a smart meter. An experiment is conducted on a hardware setup connected to a constant load, and the findings are noted. The two attacks are then extended to an IEEE-30 bus system and their impact is studied using MATPOWER simulations. For the same experimental setup, a protection scheme is also tested. The protection scheme is divided based on the attack condition: pre-attack, under-attack and post-attack conditions. Cryptographic data security in the pre-attack conditions is explored using MATLAB simulations where a binary coded password scheme is devised and then extended for a smart grid system. Multi-level encryption methods are used to prevent data breaches during attacks. The importance of firewall and antivirus databases is also analyzed.

Author Keywords. Denial of Service Attack, Man in the Middle Attack, False Data Injection, Cyber-protection, Cryptography Data Security.

Type: Research Article
Open Access Peer Reviewed CC BY

1. Introduction

Smart grids are an essential part of the modern power system network. There is a bi-directional flow of information and electricity which promises better sustainability and reliability than the conventional power grids, thereby reducing the probability of blackouts and losses in the network (Kotsalos 2017). The easy incorporation of Renewable Energy

Sources (RES) and Energy Storage Devices (ESD) in a smart grid makes it an eco-friendly network. The infrastructure of the grid is a blend of cyber and physical components. This dependency of smart grid upon information and energy data raises the concern for its security (Liu et al. 2014).

In this paper, the effects of two attacks; Denial of Service (DoS) and Man In The Middle (MITM) are analyzed. The paper's primary focus is the economical impact that a smart grid can have on a power system network. One of the most crucial parts of the electrical power industry is the number of units consumed. This directly links to their economics and revenue generation. A cyber threat can cause damage to the physical parameters of the system. The central purpose of an attacker is to fiddle with the load data and this can be done only by getting access to it. A MITM attack is best suited for the purpose. Energy companies can face economic loss and the electricity bills of consumers can change even if some load data is missed by the server. This can be done by flooding the bandwidth of the server, which is known as DoS attack.

Therefore, a smart grid needs to be secure to prevent it from failures, errors, cyber-attacks or blackouts. Care should be taken to ensure communication between the components is not compromised. A smart protection system needs to be installed that blends the communication technology with grid security, avoiding any threats to the network. The protection systems vary depending upon the type and intensity of attacks.

2. Literature Review

The literature emphasizes a smart grid in perspectives of smart infrastructure, smart management and smart protection system (Fang et al. 2012).

- Smart Infrastructure system includes the communication, information and energy infrastructure of the smart grid. This leads to advanced generation, metering, monitoring, communication and consumption.
- Smart Management system provides advanced control strategies and management methods for the smart grid.
- Smart Protection system in smart grid provides failure protection, reliability analysis, privacy protection and security services.

A brief review of the basic concepts of smart grid technologies can be seen in the literature (Fang et al. 2012; Chen et al. 2009; Yu and Luan 2009). In Rohjans et al. (2010), the authors review the standards of smart grids and recommend some standards for future grids also.

In Wang, Xu, and Khanna (2011), a detailed analysis of communication systems for an electric network is shown by the authors. Its applications in an automation system were analyzed and the challenges in power system networks were also explored. Different types of wireless communication systems and their importance in power systems are discussed in Nguyen, Benjapolakul, and Visavateeranon (2007). In Gunther et al. (2009), the authors divide the communication network into 7 subsystems: bulk generation, efficient transmission, distribution, reliable operation, energy market, customers and service provider. One of the most important components of the communication system, a smart meter is also discussed in the literature (Vasconcelos 2008). Their potential benefits and importance were also discussed in detail.

Ironically, the backbone of a smart grid- its communication network, is also its vulnerability to cyberattacks. In the past, several cyber-spies were reported to penetrate the US electrical grid (Gorman 2009). The authors of Liu et al. (2011) were the first ones to observe the effects of

cyber-attacks on a smart meter. Based upon the intensity of the attack and the number of meters corrupted, the attacks were divided into two regimes: strong and weak.

- Strong attack regime affects multiple meters without any observable measurement error. The attack doesn't get detected by the control centre.
- Weak attack regime affects limited meters. They get detected by the control centre due to their measurement errors.

One of the attacks on the cyber-system is Man In The Middle Attack (MITM). In such types of attacks, the attacker secretly transfers and changes the alliance between two parties who are under the misconception of communicating privately with each other. Mallik et al. (2019) and Callegati, Cerroni, and Ramilli (2009) explain the case of dynamic eavesdropping in MITM attacks. The attacker independently associates with victims at both ends, thereby influencing them to trust they have a private association. The attacker can intercept as well as modify the data exchanged between the 2 victims. Literature also suggests the effect of MITM attack on Address Resolution Protocol (Mohsenian-Rad et al. 2014). A detailed survey of MITM attack, their methodology and effects can be seen in Jain, Jain, and Borade (2016) and Nayak and Samaddar (2010).

Another threat to the smart grid network is Denial of Service attack (DoS). Packet streams from a large number of hosts exhaust the resource, thereby denying service to the victim (Douligeris and Mitrokotsa 2004). As per the State of the Internet (SOTI) fourth quarterly report (2012) given by Akamai Technologies, DoS attacks increased by 200% as compared to 2011 (Belson 2010). The yearly increase in internet traffic of DOS attacks between 2001 to 2010 can be seen in a study by Arbor Networks (Vamosi 2008). The authors in Specht and Lee (2003) divide the DoS attacks as:

- Bandwidth depletion: In this case, the victim is flooded with large traffic. The attack gets amplified when the traffic is sent to the broadcast IP address.
- Resource depletion: The attacker makes the processor and memory unavailable, thereby denying any services to the victim.

With the existing tools, the execution of DoS attacks by an attacker has become easier (Specht and Lee 2003). Nmap is one such tool that can exploit the operating system and port vulnerabilities (Bennieston 2004). The authors in Srivastava et al. (2011) have given a detailed survey on DoS attacks.

The detection of cyber threats on the smart grid by state estimation is divided into four categories:

- Alternated Estimation: This includes CUSUM, Kalman filter and Rao test.
- Distributed Estimation: The cyber system is divided into several subsystems and then individually analyzed (Gu et al. 2013).
- Optimization Techniques: The optimal cost of protection units and the optimal position of measurement units are used to detect False Data Injection (FDI).
- Cryptographic Techniques: This involves studies detecting FDI attacks using cryptographic techniques.

The present literature defines several vulnerabilities in a smart grid based on its: architecture, communication network, hardware, interface, HANs and interoperability (Singh and Mahajan 2021a, 2021b); the authors review smart grid cybersecurity in detail.

The contributions made to the presented paper are:

- A hardware experiment is set up to analyse the financial aspects of cyber-attacks in a smart grid network. Bidirectional communication is established between the

components of the network, just like in a smart grid. The smart meter is attacked and the losses in terms of power and revenue are analyzed.

- A protection scheme is suggested for the setup that involves password protection using binary methods and multi-level encryption strategies.

In the paper, section 3 discusses the methodology and modelling adopted in the analysis. Subsection 3.1 describes the network connection of the smart grid. In subsection 3.2, two different cyber-attacks, DoS and MITM are discussed. Their basic theory, attack algorithms and efficiency calculations are shown. The security system for the explained attacks is explained in subsection 3.3. The experimental setup and results obtained are discussed in section 4. Section 5 concludes with the highlights of this research.

3. Modelling

3.1. Modelling of Network Topology

The smart grid is an intelligent power network featured a two-way flow of electricity and information. It allows interconnection and communication between various parts of the power system network. For simplicity, it may be divided into three distinct parts: Smart homes/smart meters, servers and the control center. This is illustrated in Figure 1.

The practical smart grid has a network of smart homes forming the Home Area Network (HAN). For modelling, a single smart meter is used. Electricity consumption data from each household is measured using the smart meter and sent to the server where it is stored. This data is accessible to the energy company on a website. The smart grid has a two-way data flow; hence the control center can also send back data to the consumers.

3.2. Modelling of Cyber Attacks

This section deals with two common cyber-attacks as stated below.

A. Denial of Service Attack

The aim of this attack is to disrupt the service by limiting access to any resource without disturbing the service itself. This is achieved by sending a stream of packets to swamp the network of the victim, denying them access to resources. The attacker crashes the security of the grid, resulting in resource exhaustion.

The algorithm for a DoS attack is not very complicated. The architecture of the attacking network and the flowchart of the attack can be seen in Figure 2 and Figure 3 respectively.

- Selection of agent: In this step, the attacker selects an agent for performing the attack. Agents generate spoofed packets of data that are sent to the victim network. The handlers run a program before sending these data packets to agents. To generate attack streams, the agents should have enough resources.
- Compromise: The vulnerability of the agent is used by the attacker to deny the services of the victim. The owners of the agent system are unaware that they are compromised and are participating in a DoS attack. To minimize the change in the performance of the agent system, the bandwidths of the programs used are very small.
- Communication: The attackers, agents and handlers communicate via a common communication platform to find the agents available for attack.
- Attack: The attacker calls for the start of the attack.

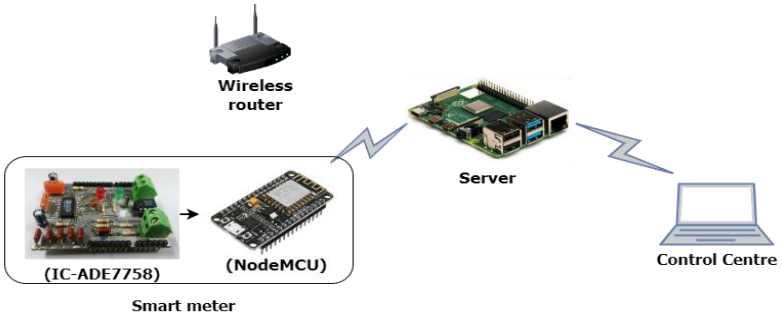


Figure 1: Smart grid network topology

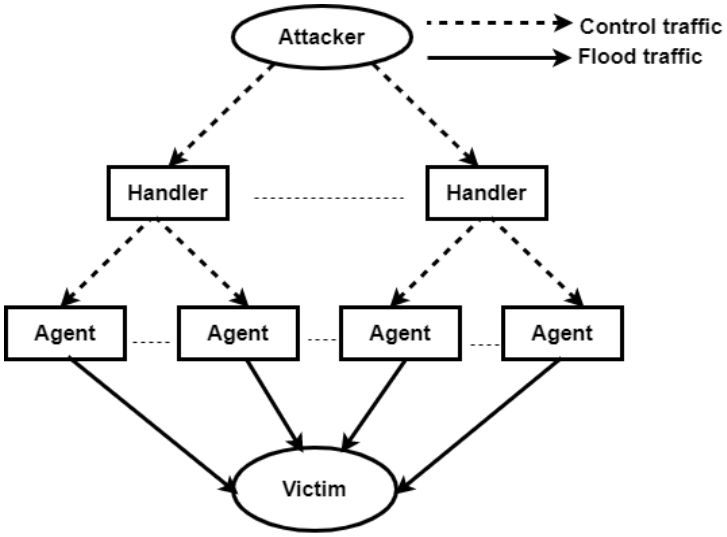


Figure 2: Architecture of the attacking network

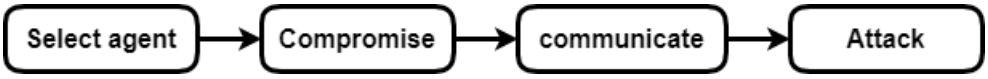


Figure 3: Flowchart: DoS attack

The efficiency of a DoS attack $\boldsymbol{\eta}$ is defined as:

$$\eta\text{DoS} \propto \frac{nc \times na \times fc \times ta}{NS} \quad (1)$$

where *nc* is number of characters/packets flooded, *na* is number of attackers, *fc* is frequency of flooding the characters/packets, *ta* is duration of attack and *NS* is the level of the security of the network.

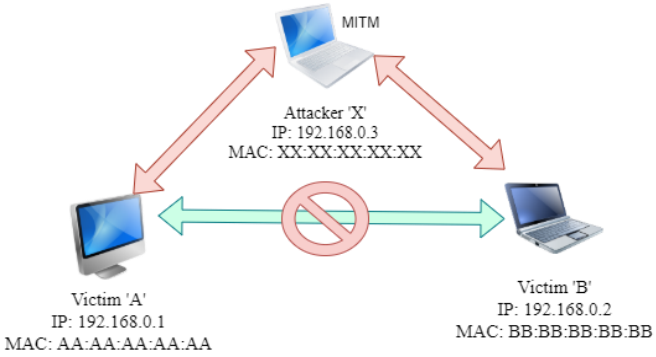
B. Man In The Middle Attack (MITM)

An MITM is an attack in which the perpetrator tries to intercept the link between two devices in a network. This is done either to tweak the packets flowing between them or eavesdrop secretly. A position is established between the victim and the server as seen in Figure 4.

Hence, the packets of data flowing between them are relayed. This is an active attack which can heavily compromise the reliability of the smart grid. Once MITM is established, confidential information such as login credentials can be sniffed, resulting in crippling of the grid.

A major attack that can be deployed once MITM is established is FDI. Data flowing from the smart metre to the server via an attacker can be modified. This will lead to a more serious problem causing economic loss to the energy company. FDI can be done by following a few steps.

- ARP spoofing: The ARP cache table of the victim is modified to make it the MITM.
- Packet Sniffing: The flow of data in the network is analyzed and its framework is observed.
- Packet filtering: The data that needs to be modified is selected and replaced with the values desired to the attacker.
- Packet relaying: To make the attack successful, the received packets are forwarded in real-time. Packets that are received have to be forwarded in real-time to achieve a successful attack.



ARP cache of 'A'	
Before spoofing	IP(b): 192.168.0.2 MAC(b): BB:BB:BB:BB:BB
After spoofing	IP(b): 192.168.0.2 MAC(b): XX:XX:XX:XX:XX

Figure 4: An intruder as man in the middle

The pseudo-code with its algorithm demonstrating a MITM attack is discussed below.

➔ The pseudo-code for the attack is compiled using Ette filter in the Ettercap directory and is shown below.

```
If(ip.proto = = TCP && TCP.dst = = 80)
{
  If(search(DATA.data, reading))
  {
    replace(reading, reading*0.95);
    #First argument is original value, Second is forged
    msg("filter ran successfully");
  }
}
```

Select filter from the filter menu and load it.

Run the MITM attack.

If there is an exchange of n packets, each packet taking time t, then

Total time taken for data transferred = $n \times t$

If the router drops m packets during the attacks then, (n - m) packets are processed. This means the processing time has lowered and also lower buffer size is required to store the data.

The efficiency of MITM attack $\boldsymbol{\eta}_{\text{MITM}}$ is defined as:

$$\boldsymbol{\eta}\text{MITM} \propto_{\beta} \rho\, a \qquad (2)$$

where, a is the data quantity exchanged, ρ is the severeness of the attack and $_{\beta}$ is the scale factor, that is the modifications made by the attacker.

3.3. Modelling of the security system

Smart grid networks are heterogeneous and interconnected. Thus, even an “internet bug" or “internet worm" can contaminate the entire system without much difficulty. To prevent this, several protection schemes are suggested. These schemes, although efficient, are not sufficient for the security of the system. It is essential to have a security scheme that overlooks the following prospects.

- The **pre-attack security measures** should be proficient at avoiding easy access into the network.
- **Successful detection models** are mandatory to detect any intrusion or malpractice in the network.
- There should be defined actions and protocols when the network is under attack.
- **Post-attack strategies** should be defined to overcome losses incurred by the attack and avoid any potential threats in the future

This paper discusses the above-stated points in detail. For any security system, the National Institute of Standards and Technology (NIST) has defined three concerns: Availability, Confidentiality and Integrity. Literature suggests another essential concern, accountability.

- **Availability:** A continuous power flow ensures reliable and timely access to the information. Therefore, it is the most crucial concern.
- **Confidentiality:** Confidentiality means restrictions on disclosure and access to information by authorized personnel. This helps in preserving the data privacy and disclosure of proprietary information to attackers.
- **Integrity:** It is essential to prevent unauthorized modification, alteration or destruction of data. This demands non-repudiation and authenticity. Non-repudiation means that any entity, individual or organization cannot deny any action performed by them. Authenticity ensures the legitimacy of the data source.
- **Accountability:** It is vital to have a track of the actions performed in a system and record them. The recordings are proof against the attackers.

A. The pre-attack security measures

The smart grid must always be prepared for any threats on the network. The security measures are applied to devices, networks and data.

- **Device Security:** Device security is done by securing the endpoints of all the devices in the grid. Literature suggests the use of antivirus software, host ID, and host Data Loss Prevention System (DLP).
- **Network Security:** The most critical component of a grid is the network. Firewalls, used for securing the network, allow/deny threats on the network based on pre-set policies and rules. However, it proves ineffective against advanced attacks. It can be associated with different security systems, as discussed here.
  - ➔ The **Intrusion Detection System (IDS)** is used for the identification/detection of undesired activities on the network.
  - ➔ The **Security Information and Event Management System (SIEM)** collects data and gathers information from all devices connected to the network. The collected data gets transferred to the centralized server to process it for threats.
  - ➔ The **Data Loss Prevention System (DLP)** helps in any data breach within the network. Some additional security protocols like TLS, DNP3, SSL and IP (sec) are also used for smart grid protection.

- **Cryptographic Data Security:** For data security, the primary approach is a combination of authentication and encryption. Authentication means verification of an object's identity like for using a password \cite{prot5}. Encryption means converting the data into a secret code without disturbing its integrity, configuration or repudiation. Similar to this, one encryption and authentication model is designed for this paper.

B. Detection of Attacks

Over time, there has been substantial research on different attacks and the security protocols appointed against them. The spatial and temporal based detection schemes are discussed in Jiang et al. (2018); Jamming channel attack detection in El Mrabet et al. (2018); use of online CUSUM detectors in Yan, Tang, and He (2016) and FDI in Yan et al. (2016). Studies suggest that solutions like “security by obscurity" and “defense in depth" prove insufficient with the more advanced attacks

C. Mitigation Strategy for System Under Attack

For a DoS attack, the mitigation technique involves reconfiguration and pushback. During reconfiguration, the topology of the network is altered to isolate the attacker. In pushback, the router is configured to block traffic from the attacker's IP. The mitigation for other attacks like replay attacks, jamming attacks, DDoS, MITM, CPU exhaustion, FDI and buffer flow are discussed in the literature.

D. Post Attack Strategies

It is necessary to identify the entity involved in the attack. In order to be alert for any future attacks, IDS, antivirus database and security policies need to be up to date. For the study of the attack, the primary technique employed is Forensic Analysis. The collected data is intercepted and analyzed for the identification of the attacker. This method also helps to determine the cyber and physical vulnerabilities of the grid to prevent potential threats in future.

4. Results and Discussion

For the purpose of this paper, a hardware experiment was set up, mainly consisting of the three parts: smart meter, server and a control center. IC-ADE7758 embedded on an Arduino board with Atmega16 is used for the conversion and calculation purpose. To interface the smart meter with the server over the internet, a NodeMCU with wifi chipset called ESP8266 is used. The converted data from the Arduino board is given to the NodeMCU as an input which further sends it to the server using TCP/IP protocol. The power usage data received from the smart meter is stored in a database. For modelling purposes, Raspberry Pi 3B+ is used. It also has a task to host a web dashboard from which this data can be monitored. A constant load of 2 kW is detected by the smart meter and is to be transmitted and stored in the database. For authorization of the person using the website, a login is required with a unique username and password.

The system is analyzed for the following:

- DoS attack
- MITM attack
- Extension of the cyber-attacks on IEEE 30 bus system
- Security of the system

4.1. Results for DoS Attack

In the DoS attack, 3 attackers attacked the communication network by flooding 65535 characters per second per attacker. This attack was carried out for 3 days.

In Figure 5 the data received by the server with and without a cyber-attack on the communication network are compared for each individual day. The difference in results of 3 days is due to constant change in the network connection. With a change in network bandwidth, the rate of data transfer may vary. The overall loss is computed for 3 days.

The estimation of the financial impact of the cyber-attack on a utility provider is done. The data obtained from a utility provider for the region of Surat, Gujarat, India, is used. The monetary losses have been calculated based on the loss percentage for both cyber-attacks. Usage data has been collected for Residential General Purpose (RGP) loads, which are loads based in the Residential area of Surat and are rated under 20kW. The average cost per unit has been taken as Rs.4 based on the data from the utility provider. The total losses have been calculated in Table 1.

It is seen that the load output on the 3 days that the attack was conducted was approximately 41 kW, 43 kW, and 44 kW. This change in the load is due to changes in the attacker's bandwidth and also the attack environment. The average load loss over three days is 10.423%. For the service provider with almost 400,000 customers, a monetary loss worth approximately Rs. 9,00,00,000 is seen.

4.2. Results for MITM Attack

The second attack performed on the network is MITM. Network security tools such as Ettercap and Better cap available in Kali Linux are used for ARP spoofing. This results in the attacker becoming Man-In-The-Middle.

Once MITM is established, two different attacks are possible: Packet Sniffing and FDI. Packet sniffing is deployed between the control centre and the server. The login credentials used by the authorised personnel to access the server have been stolen. FDI is launched at the smart metre end. Data sent from the smart metre to the server is forged. As this is an active attack, unlike DoS, any desired change in the reading can be fabricated. This "desired change" needs to be carefully determined. If the value is very large, the attack can be easily detected because there's a significant variation in the load profile. On the other hand, if the value is very small, the purpose of the attacker is not fulfilled. Therefore, the preferable range is 3-5 %. For the purpose of this paper, we selected a decrease of 3.5% in the data, as seen in Figure 6.

The data used in the DoS attack has been utilised in order to estimate the financial losses if such an attack were to take place in a smart grid network. Table 2 shows overall losses for the considered data. Here, the error is decided by the attacker since data is modified by the Man-In-The-Middle.

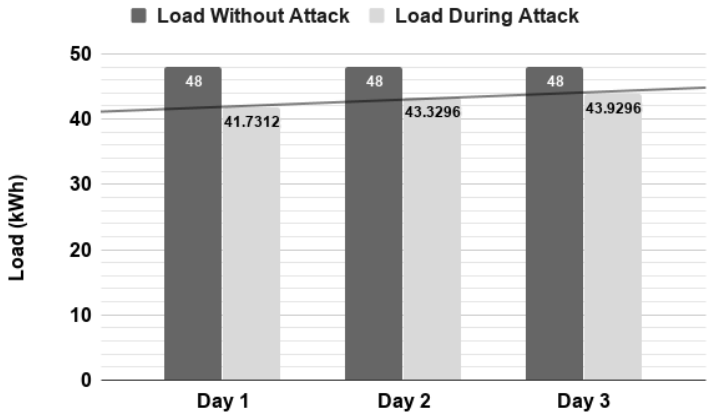


Figure 5: Daily change in load due to DOS attack

No. of customers	**413,434**
No. of units sold (in M kWh)	222.55
Percentage change in Power	10.4233 %
Units lost due to attack (in M kWh)	23.197 units
Cost per unit	Rs. 4
Total loss (in Rs.)	Rs. 92,788,216.60

Table 1: Economic Impact due to DOS Attack

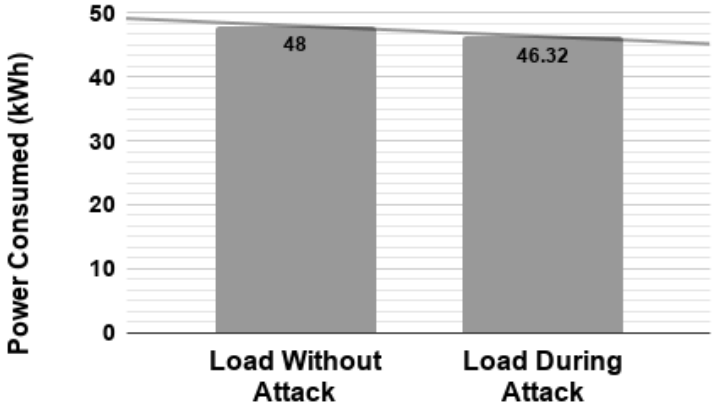


Figure 6: Power output for MITM attack

No. of customers	**413,434**
No. of units sold (in M kWh)	222.55
Percentage change in Power	3.5 %
Units lost due to attack (in M kWh)	7.78925 units
Cost per unit	Rs. 4
Total loss (in Rs.)	Rs. 31,157,000.00

Table 2: Economic impact due to FDI attack

It is seen that the load output decreased from 48 kW to 46.32 kW corresponding to a 3.5 % change in load. For the service provider with almost 400,000 customers, a monetary loss worth approximately Rs. 3,10,00,000 is seen.

4.3. Results of Cyber Attacks Extended for IEEE 30 Bus System

The IEEE 30 bus system has been attacked by the same intensity of DoS and FDI attacks, as seen in the above section. The results are calculated using MATPOWER simulations and can be seen in Table 3.

	P_l (MW)	P_g (MW)	P_{loss} (MW)	P_{attack} (MW)
Test Case	3765.08	3814.2	49.12	-
DOS attack	3372.65	3421.77	49.12	392.43
MITM attack	3633.30	3682.42	49.12	131.78

Table 3: Impact of cyber-attack on IEEE 30 bus network

The simulation results of the original IEEE 30 bus test case have been noted. For the case of DoS attack, the smart meter readings were modified. The load power P_l decreased by 10.423 %. The line losses P_{loss} remained constant, as in the test case. This is because the resistance in lines is considered constant, thereby giving constant I^2R losses. This results in a change in generated power P_g that is reflected as P_{attack} equal to 392 MW. Similarly, from subsection 3.2, the change in load is 3.5 %, resulting in P_{attack} equal to 131 MW.

4.4. Cyber security

For the attacks discussed earlier, a pre-attack protection scheme was designed using multi-step verification during login and encryption of data that is being exchanged.

To prevent the DoS attacks, the firewall, security policies and antivirus database were updated. For a MITM attack, the system network needed to be secure. This was done by securing the server by setting up a password-protected account.

For a secure password, five conditions need to be satisfied: lowercase alphabet, uppercase alphabet, numerals, special characters, and minimum length. For this paper, the minimum length criteria were set to 6. This is an essential condition for the password setup. The remaining 4 conditions determine the strength of the password. The number of bits in the password is 2n, where n is the number of conditions met. Whenever any one of the conditions is met, the corresponding bit becomes 1. Thus, the strength of the password is analysed based upon its binary configuration. The account is linked to the email for verification of the "One Time Password" generated for extra security. Therefore, for an attacker to hack the network, they need to first hack into the system email for a One Time Password (OTP). The system data was encrypted, transferred and then decrypted again to prevent any MITM attacks. For this experiment, the algorithm is designed for 8-level cryptography and the results are shown in Figure 7.

Original	2	1	8	7	9	4	3	4	5
Encrypted	(	,	0	0	=	=	Q	F	/

Figure 7: Encryption of data

5. Conclusion

In this paper, a detailed analysis of a smart grid was shown. All the components and technology involved with it were analyzed. An experiment was set up that behaved as an independent cyber-physical network. The hardware components were made to communicate with each other so that a bidirectional flow of data could take place. Due to this flow of data, remote monitoring of the smart grid system has become possible. The connection of all the components to the internet and a common server results in an unwanted exposure to cybercrimes. This results in cyber-attacks on the grid. Two such attacks were analyzed in the report. In the experimental setup, DoS and MITM attacks resulted in revenue losses to the service provider. On extending these results to IEEE 30 bus systems using MATPOWER simulations, a similar loss in load power reading of smart meters was seen. Different protection schemes were designed to secure a smart grid from cyber-attacks. The report states the protection schemes under 3 conditions: pre-attack, under-attack and post attack. Multi-step verification methods, password protection using binary methods and encryption strategies were discussed to prevent systems from potential attacks. The report also states that the firewall, antivirus database etc. should be up-to-date.

References

Belson, D. 2010. "Akamai state of the Internet report, Q4 2009". *Operating Systems Review (ACM)* 44, no. 3: 27-37. https://doi.org/10.1145/1842733.1842738.

Bennieston, A. J. 2004. NMAP - A Stealth Port Scanner. https://www.csc.villanova.edu/~nadi/csc8580/S11/nmap-tutorial.pdf.

Callegati, F., W. Cerroni, and M. Ramilli. 2009. "Man-in-the-middle attack to the HTTPS protocol". *IEEE Security and Privacy* 7, no. 1: 78-81. https://doi.org/10.1109/MSP.2009.12.

Chen, S., S. Song, L. Li, and J. Shen. 2009. "Survey on smart grid technology". *Power System Technology* 33, no. 8: 1-7.

Douligeris, C., and A. Mitrokotsa. 2004. "DDoS attacks and defense mechanisms: Classification and state-of-the-art". *Computer Networks* 44, no. 5: 643-66. https://doi.org/10.1016/j.comnet.2003.10.003.

El Mrabet, Z., N. Kaabouch, H. E. Ghazi, and H. E. Ghazi. 2018. "Cyber-security in smart grid: Survey and challenges". *Computers and Electrical Engineering* 67: 469-82. https://doi.org/10.1016/j.compeleceng.2018.01.015.

Fang, X., S. Misra, G. Xue, and D. Yang. 2012. "Smart grid - The new and improved power grid: A survey". *IEEE Communications Surveys and Tutorials* 14, no. 4: 944-80. https://doi.org/10.1109/SURV.2011.101911.00087.

Gorman, S. 2009. "Electricity grid in US penetrated by spies". *The Wall Street Journal*, April 8, 2009. https://www.wsj.com/articles/SB123914805204099085.

Gu, Y., T. Liu, D. Wang, X. Guan, and Z. Xu. 2013. "Bad data detection method for smart grids based on distributed state estimation". In *IEEE International Conference on Communications*, 4483-87. IEEE. https://doi.org/10.1109/ICC.2013.6655273.

Gunther, E. W, A. Snyder, G. Gilchrist, and D. R. Highfill. 2009. *Smart grid standards assessment and recommendations for adoption and development*. EnerNex Corporation.

Jain, K. M., M. V. Jain, and J. L. Borade. 2016. "A survey on Man in the Middle Attack". *International Journal of Science Technology and Engineering* 2, no. 9: 277-80. http://ijste.org/Article.php?manuscript=IJSTEV2I9103.

Jiang, Q., H. Chen, L. Xie, and K. Wang. 2018. "Real-time detection of false data injection attack using residual prewhitening in smart grid network". In *2017 IEEE International Conference on Smart Grid Communications, SmartGridComm 2017*, 83-88. IEEE. https://doi.org/10.1109/SmartGridComm.2017.8340659.

Kotsalos, K. 2017. "Decentralized voltage regulation in radial medium voltage networks with high presence of distributed generation". *U.Porto Journal of Engineering* 3, no. 1: 26-38. https://doi.org/10.24840/2183-6493_003.001_0003.

Liu, S., B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry. 2014. "A coordinated multi-switch attack for cascading failures in smart grid". *IEEE Transactions on Smart Grid* 5, no. 3: 1183-95. https://doi.org/10.1109/TSG.2014.2302476.

Liu, Y., P. Ning, and M. K. Reiter. 2011. "False data injection attacks against state estimation in electric power grids". *ACM Transactions on Information and System Security* 14, no. 1: Article number 13. https://doi.org/10.1145/1952982.1952995.

Mallik, A., A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou. 2019. "Man-in-the-middle-attack: Understanding in simple words". *International Journal of Data and Network Science* 3, no. 2: 77-92. https://doi.org/10.5267/j.ijdns.2019.1.001.

Mohsenian-Rad, H., F. Granelli, K. Ren, C. Develder, L. Chen, T. Jiang, and X. Liu. 2014. "Editorial: IEEE communications surveys & tutorials special section on energy and smart grid". *IEEE Communications Surveys and Tutorials* 16, no. 3: 1687-88. https://doi.org/10.1109/SURV.2014.042914.00001.

Nayak, G. N., and S. G. Samaddar. 2010. "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions". In *Proceedings - 2010 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2010*, 491-95. https://doi.org/10.1109/ICCSIT.2010.5563900.

Nguyen, V. I., W. Benjapolakul, and K. Visavateeranon. 2007. "A high-speed, low-cost and secure implementation based on embedded ethernet and internet for SCADA systems". In *SICE Annual Conference 2007*, 1692-99. https://doi.org/10.1109/SICE.2007.4421256.

Rohjans, S., M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, and T. Weidelt. 2010. "Survey of smart grid standardization studies and recommendations". In *2010 1st IEEE International Conference on Smart Grid Communications, SmartGridComm 2010*, 583-88. IEEE. https://doi.org/10.1109/SMARTGRID.2010.5621999.

Singh, N. K., and V. Mahajan. 2021a. "Analysis and evaluation of cyber-attack impact on critical power system infrastructure". *Smart Science* 9, no. 1: 1-13. https://doi.org/10.1080/23080477.2020.1861502.

———. 2021b. "End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure". *International Journal of Critical Infrastructure Protection* 34: Article number 100410. https://doi.org/10.1016/j.ijcip.2021.100410.

Specht, S. M, and R. B Lee. 2003. *Distributed Denial of service: Taxonomies of attacks, tools and countermeasures, Princeton architecture laboratory for multimedia and security Technical Report*. Princeton, NJ: ISCA.

Srivastava, A., B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra. 2011. "A recent survey on DDoS attacks and defense mechanisms". In *Advances in Parallel Distributed Computing. PDCTA 2011*, 570-80. Communications in Computer and Information Science. Springer. https://doi.org/10.1007/978-3-642-24037-9_57.

Vamosi, R. 2008. "Study: DDoS attacks threaten ISP infrastructure". https://www.cnet.com/news/privacy/study-ddos-attacks-threaten-isp-infrastructure/.

Vasconcelos, J. 2008. *Survey of regulatory and technological developments concerning smart metering in the European Union electricity market*. Policy Papers, RSCAS 2008/01. European University Institute (EUI), Robert Schuman Centre of Advanced Studies (RSCAS). https://hdl.handle.net/1814/9267.

Wang, W., Y. Xu, and M. Khanna. 2011. "A survey on the communication architectures in smart grid". *Computer Networks* 55, no. 15: 3604-29. https://doi.org/10.1016/j.comnet.2011.07.010.

Yan, J., B. Tang, and H. He. 2016. "Detection of false data attacks in smart grid with supervised learning". In *Proceedings of the International Joint Conference on Neural Networks*, 1395-402. IEEE. https://doi.org/10.1109/IJCNN.2016.7727361.

Yan, J., Y. Tang, T. Bo, H. He, and Y. Sun. 2016. "Power grid resilience against false data injection attacks". In *IEEE Power and Energy Society General Meeting*, 1-5. IEEE. https://doi.org/10.1109/PESGM.2016.7741850.

Yu, Y. X., and W. P. Luan. 2009. "Smart grid and its implementations". *Zhongguo Dianji Gongcheng Xuebao/Proceedings of the Chinese Society of Electrical Engineering* 29, no. 34: 1-8.

Abbreviations

ARP	Address Resolution Protocol
DoS	Denial of Service
DLP	Data Loss Prevention
DNP3	Distributed Network Protocol 3
ESD	Energy Storage Devices
FDI	False Data Injection
HAN	Home Area Network
IDS	Intrusion Detection System
IP	Internet Protocol
MITM	Man In The Middle
NIST	National Institute of Standards and Technology
OTP	One Time Password
RES	Renewable Energy Sources
RGP	Residential General Purpose
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management System
SOTI	State of the Internet
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security