*Article*

**SMART GRID CYBER ATTACK MODELING**

|  |
| --- |
| **Citation:** To be added by editorial staff during production.  Academic Editor: Firstname Lastname  Received: date  Accepted: date  Published: date  **Publisher’s Note:** MDPI stays neutral concerning jurisdictional claims in published maps and institutional affiliations.    **Copyright:** © 2022 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/). |

1 Affiliation 1; e-mail@e-mail.com

2 Affiliation 2; e-mail@e-mail.com

**\*** Correspondence: e-mail@e-mail.com; Tel.: (optional; include country code; if there are multiple corresponding authors, add author initials)

**Abstract:** The smart grids used today are vulnerable to attacks against these networks. Since the infrastructures of these networks used in electrical power distribution are vital, they are very likely targets to be attacked by powerful and equipped attackers. Such attacks rely on Malware that infiltrates and spreads through the MicroGrid system in a controlled manner, putting control and communication in smart grids into contact with an outside entity. In this article, we will be discussing what can be done to determine the characteristics and observation of attacks by testing the attacks that can be made on smart networks on a created smart network model, by looking at the damage that the attacks will cause on the system and the fluctuations in the system. The model includes a wide range of smart grid power distribution systems and some renewable energy sources, including electric vehicle charging stations in each location. One of these devices is also included in the data to be taken in the attacks. Considering the previous research and models, in light of this information, we simulate and observe the current malware, its techniques, and the negative damage it can cause on smart networks, and then we examine the possible outcomes during these attacks. For this purpose, we apply and analyze malware with FDI (false data injection) on the smart system created on the model. Our model used in practice provides a basis for modeling and analyzing attacks on smart grid systems and providing ideas on what can happen during these attacks. Thus, preventing predicted malware in the future, helps utility power distribution companies prepare cybersecurity defense systems by preventing them from being vulnerable to future attacks.

**Keywords:** Smart Grid, Community Micro Grid, Electric Vehicles, Smart Grid Cyber Security.

# 1. Introduction

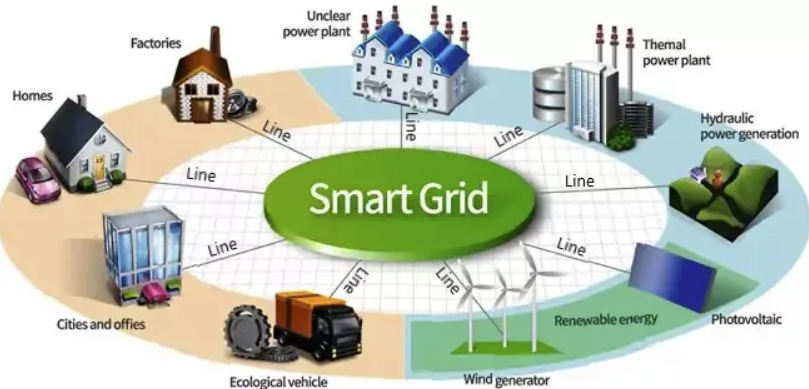
After the industrial revolution, energy became an important thing in our daily life. All these enormous infrastructures require energy to maintain. In recent years, the importance of energy, renewable energy sources, and energy storage techniques has been increasing with the increase in technology and production potential. Due to the growing population and advances in technology, more and more energy is needed every day, so people convert various natural resources into energy for their own needs. Microgrids are groups of interconnected renewable and conventional energy sources and loads located in a specific area that appear as a single unit to the AC (Alternating Current) grid [1]. Smart Grids are adapted electricity grids that use information and communication technology to improve efficiency. When we consider the importance of energy, there are two types of energy, the first one is fossil fuels. Fossil fuels are often the first source of energy, but they have negative impacts on soil degradation, air pollution, global warming, water pollution, acidification of oceans, acid rain, and health. Without precautions, irreversible damage can occur [2]. So far, several transformations have involved renewable energy sources. Regarding the solutions created to reduce environmental pollution and stop climate disasters, it is important. Renewable energies are significant factors of nature that can be obtained from carbon-neutral natural resources which are generated by electricity such as light from the sun, winds, rains, and waves that could be obtained from sources that are naturally renewed on a human timescale. Renewable energy has corresponded to integrated resources and has a good impact on the grid system, defined in three positive ways: economically, socially, and environmentally. Fossil fuels have a major negative impact on climate change. So, the usage of these fuel types can damage the environment [3].Over the past ten years, renewable energy has progressively increased the amount of energy produced worldwide. By 2017, renewable energy represented more than 50% of newly installed capacity globally or 60.0%. (167 GW). Falling costs for solar and wind energy technologies have inspired many nations to use renewable energy sources, transferring incentives from fossil fuel projects to clean energy sources [4][5].

Smart Grids have many advantages. It has advantages as well as disadvantages such as being easy to manage, making its use a part of human life, diversity of energy sources, the longevity of devices, and providing communication between devices with IoT independently of people. An IoT system consists of web-enabled smart devices that collect environmental data, transmit it to a receiver, and take appropriate action using embedded systems including CPUs, sensors, and communication tools. By connecting to an IoT gateway or other edge device that allows data to be transferred to the cloud for analysis or local review, IoT devices exchange the sensor data they collect. These devices occasionally exchange information with other similar devices and act on this information. Most of the workforce is done by tools without human intervention, but people can still work with them to access, set up, or instruct data . One of these important disadvantages is that smart grids are prone to cyber-attacks. Recent cyber-attacks are proving the importance of the security of a smart grid network.The European Network and Information Agency (ENISA) states that three key security principles in smart grids must be strictly followed [6]. Therefore, in smart grids, accessibility, integrity, and confidentiality must be guaranteed.

1. Accessibility: Principle that ensures authorized parties can obtain the information when necessary.
2. Integrity: The principle against modification of confidential data held in sensors, control commands, software, and electronic equipment to prevent data traffic and decision-making.
3. Confidentiality: The saved and sent data is only accessible to the proper recipients. With these principles on systems as sophisticated and diversified as the evolving smart grid, a sizable number of potential cyberattacks are becoming more likely.

Smart grid networks as seen in a model in Figure 1 can communicate with each other and other services via fiber cables, radio transmitters, and cellular networks. These networks can also create vulnerabilities so that attackers can penetrate the grid and take control. [7][8]. The majority of non-traditional malware can work hidden in an infected environment [9]. This process complicates things further and can go as far as using heavy multi-layer concealment [10]. In December 2015, a power grid in Ukraine was hijacked by hackers. Hackers used phishing emails to install required malware to strike a smart grid network. After months of reconnaissance operations, attackers cut the power of a wide area. This attack affected up to 225.000 customers [11]. According to reports published in the Atlanta Journal-Constitution, Atlanta lost about $2.7 million to repair damage from cyberattacks. As stated in the Information Technology Professionals Security Report, which can also be referred to as Cyber Security, in 2018, it is said that 50% of companies have been exposed to Distributed Denial of service attack (DDoS) attacks in the past years. [12]

Since smart grids are connected to a public or private network, disruption of these channels is possible by server-side failure. DoS (Denial of service) or DDoS is a collective type of cyber-attacks on a network. DoS and DDoS attacks usually aim to prevent the server or client from continuing its normal operations. These attacks can block communications between server and client, stop monitoring and management, and eventually lead to system failures that can lead to a smart grid shutdown [13]. During the 2015 Ukrainian Power plant cyber-attack, attackers used a DoS attack pattern on telephonic networks to prevent customers from reporting power outages [14]. All energy resources, especially the acceptance of companies' Electric Vehicles (EV) batteries and solar panels as positive effects on life which are used as an important resource in the intelligent management of microgrids in a sustainable environment, have an economic matter in the protection of nature [15]. There are various architectures for IoT which define an available and divide IoT into five different layers: sensing, network, middleware, application, and relations. Since they frequently function in exterior environments. The system has no protection against MITM and Dos attacks at the network layer. Applications are susceptible to threats that frequently afflict traditional computer systems [16].



**Figure 1:** A Smart Grid System with Regenerative Sources, Houses, etc.

The management of energy systems, which are gaining value daily, and smart grid systems, which are modernized systems for this, continue to gain value. Still, today, the smart grid offers a system that is open to attacks as mentioned in Table 1 which includes some cyber attacks in recent years as well as its smart technologies. It is very important to detect these attacks before or immediately after the attack. According to a survey on malware and malware detection systems [17], there are plenty of different malware types that can be disturbing or break the Smart Grid System. In response, researchers and manufacturers are developing new methods to produce advanced techniques for creating anti-malware [18]. To prevent these and similar attacks and to develop security systems, our application includes cyber-attack system modeling to simulate the effects of cyber-attacks on smart power systems and examine the outputs obtained as a result of a possible attack and pioneer future studies to respond to these attacks [19].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Description | Date | Country | Impact | References |
| Breached electrical grids | May 2022 | Germany | Disrupted system operation for a short period. | [20] |
| Supply chain attacks on SolarWinds | Sep. 2020 | USA | Millions of customers are affected. Many company services and products are disrupted. 300,000 customers have been affected. | [21] |
| Interrupted power distributions and other critical infrastructures | Jun. 2017 | Ukraine | Banks, metro systems, and electricity distribution systems are disrupted. | [22] |
| Widespread blackouts, leaving approximately 250,000 customers without electricity | Dec. 2015 | Ukraine | Power blackout affected more than 225,000 people. | [23] |
| Stuxnet malware and FDI attacks on nuclear power plants. | Nov. 2010 | Iran | Almost 1000 centrifuges are damaged. | [24] |

**Table 1:** Recent most disruptive cyber-attacks on smart grid networks.

# 2. STATE OF THE ART

Cyber-attack on complex mıcrogrıds

In systems as sophisticated and varied as emerging smart grids, the potential for a sizable number of cyber attacks is growing, as shown by cybersecurity breakthroughs and academic research. Besides, having an active user can lead to the emergence of new security threats. For this reason, new security measures should be taken to prevent these and similar events. V. Y. Pillitteri and T. L. Brewer claim a number of broadcasts recently addressed the apparent potential of cyberattacks against metering infrastructures [27]. More comprehensive articles than this have looked at risks to power substructures at large and AMI (Advanced Metering Infrastructure) systems especially, while more in-depth studies [28] have attempted to identify a component of the system in the event of a sudden attack. Sridhar et al. thoroughly examined the dangers of the power system grappling with malware. [29][30]. However, since their examination was done using such limited criteria, both the approach and the results do not provide a general idea of how to protect the energy infrastructure. The report touches on topics such as control circulation integrity and load-reducing attacks on AMI systems but does not go into the necessary details about how an attack could affect the network or predict the consequences of certain scenarios. The worst possible attack scenario according to the characteristics of the AMI network, the impact of the critical failure or the point where the system's ability to maintain power flow is impaired, and the time it takes to become critical are the main topics of this study.

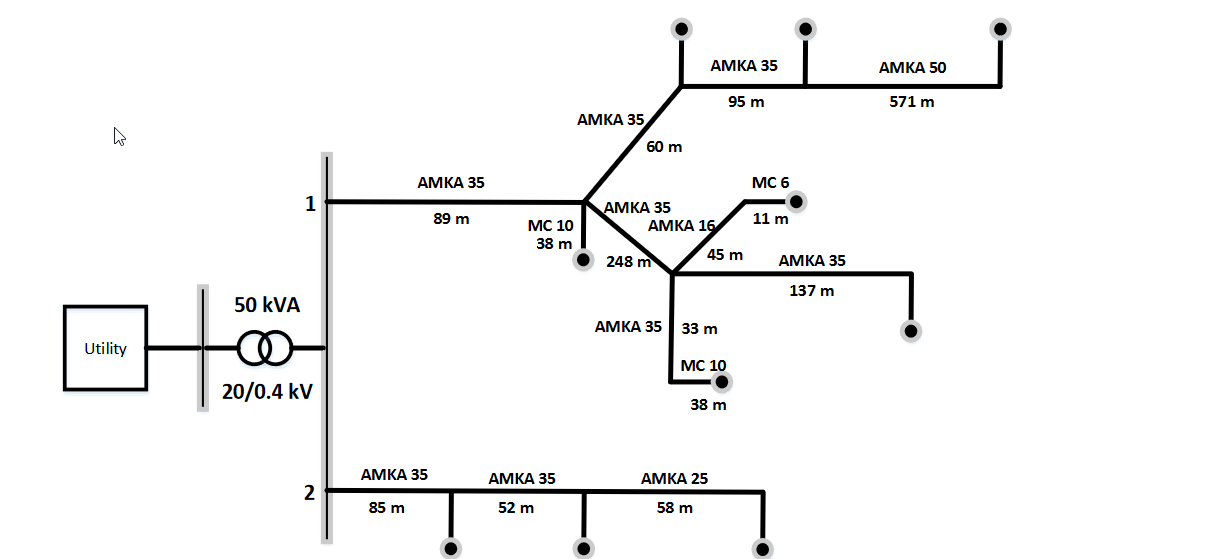
The management of energy and renewable energy sources, which will become more important in our lives in the coming days, and the compatibility of these systems with power distribution systems are of vital importance. According to C. P. Vineetha and C. A. Babu [25], every type of data generated by smart grids, when it comes to production and consumption, facilitates human existence. And must be safeguarded against potential attacks during its production cycle. Data integrity, confidentiality, and availability are typically provided as part of data security precautions. The effective and secure data exchange between the network's participants is a prerequisite for the smart grids' anticipated outcome.In addition, Hoosyar and Iravani conducted a study trying to classify some of the difficulties encountered in protecting microgrids and their types [26]. In addition, smart grid systems are vulnerable to malware such as DDoS, Dos and FDI and blackmail software.

In this article, we examined FDI, a cyber-attack scenario in a smart grid using different methods and approaches from system disciplines. With this study showing how systems engineering can be used to address challenges on the cyber-physical security side, we were able to establish appropriate performance criteria for the design and systematic evaluation of risk mitigation algorithms. The analysis will include additional failure effects that will be significant in the future and the intervention to the system will be developed in more detail. While the results of the simulations developed and conducted for this study are not directly applicable to the protection of distributed smart grid systems, we hope that the methods and concepts discussed here will provide some new insights into how to approach the risks posed by smart grid upgrades and utilities.

# 3. MODEL

With the recent developments in battery technologies, many governments have shifted their attention to EVs. With the rise of EVs, many challenging issues will appear as well. Increasing the load on the current power grid is one of these concerns [12]. In this paper, we modeled a 10-house community smart microgrid to analyze the load created by EVs to the grid.

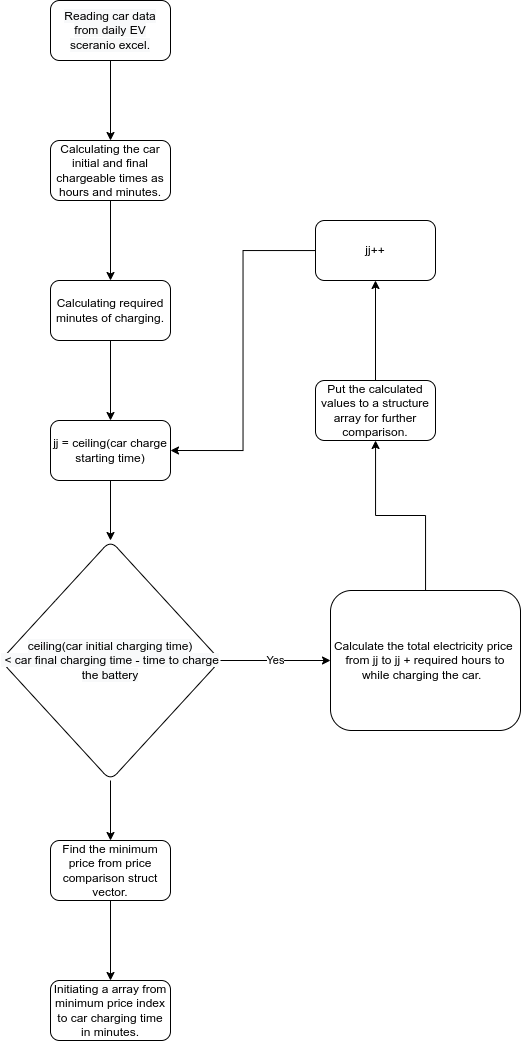
The model of the microgrid system we used in our project consists of 10 houses with solar panels and electric vehicle charging stations. There are power distribution and transportation mechanisms to the houses in the simulation, and a natural habitat formation is based on this. Each house has its own consumption data, and these data are produced in minutes using an excel file. In addition, hourly electric vehicle charging for electric vehicle stations, using the data in Comed [30], energy calculation algorithms, and scenarios were created using the data of different types of electric vehicles in the houses and included in the simulation. The solar panels in the houses were produced from an excel file in a way that is different but close to each other in each house and included in the simulation to reduce the consumption rate in the houses when the sun rises.

**Figure 2:** Low voltage electrical distribution system model schema from Hannu Laaksonen, Pekka Saari, and Risto Komulainen [31]

We modeled a community microgrid that contains 10 houses. Each house also contains an EV and PV (Photovoltaic Panels). Every house has a unique and dynamic changing load and PV generation data. Every EV also has unique charging characteristics. In our simulation, scheduling for electric car charging is done by an optimization algorithm. This algorithm generates unique charging characteristics data for each house.

The algorithm first read the EV data from a .csv file to the MATLAB workspace. After that by subtracting the initial capacity from the final capacity, we can get the required rise on the battery as a percentage. By multiplying this percentage by battery capacity, we can quickly determine the required charge in watts. We can get the required charging time by dividing the charge required in watts by charging power. After calculating the required values for the given EV, the algorithm optimizes the charging price using Linear Programming. Traversing from the initial charging time to the end charging time algorithm correctly finds the minimum price for the given calculation. After calculating the minimum price that can be obtainable, the algorithm creates simulation data accordingly. Selecting the index time as the starting hour for the charging operation for the minimum price index. From the minimum price index to the required charging time in minutes, EV charger power is passed as a load value.

From our simulation results, we can conclude that EVs can put serious weight on electricity grid networks.



**Figure 3:** The algorithm used to optimize pricing for EV charging.

## 4. A. CYBER ATTACK MODELING

In our study we analyzed the impact of a potential cyber attack caused by FDI on smart grid networks. Our study considers the electric vehicle charging algorithm has been hijacked and price data has FDI into them. Since our charging algorithm optimizes charging start times according to the total electricity usage price caused by EV charging, injected false data on pricing can cause customers to pay more. In our attack scenario, we have switched the highest 8 hours price with the lowest 8-hour price between 8 and 24 hours.

During our study, we analyzed some sample price cases from ComED. Highly differentiated pricing profiles are chosen as normal pricing scenarios. These fluctuating prices can maximize the pricing impact of an FDI attack.



**Figure 4:** Hijacked prices sent to EV charging algorithm. The highest 8 prices are swapped by the lowest 8 prices between 8 and 24 hours.

By swapping prices, the algorithm simply continues to operate at normal. It schedules the car charging to a minimal EVs charging price. Also, by cumulating the minimal prices on a limited period, load on transformer will be increased due to the load created by EV charging operations for hijacked low price index.

# 

# 5. Simulation & Results

In our study, we analyzed the impact of a FDI attack on a 10-house community microgrid. Using Simulink and MATLAB as simulation tools, a realistic approach to the problem was possible. As can be seen from the Figure 5 graph, the total power drawn by the system simulation containing 10 houses in a day was drawn by looking at the main transformer data and the graph was obtained. At the same time, 2 blue and red lines appear on the Figure 6 graph, the pricing algorithm whose data were changed with the blue line attack, and the red line normal pricing algorithm are shown on the same chart. The economic loss in the system after a FDI intervention will be based on much more extreme levels as the number of people using the system increases. For this reason, these and similar attacks should be prevented before the attack with control methods at the time of the attack or before it occurs, and possible damages should be protected.



**Figure 5:** 24-hour load data on 10-house microgrid transformer without EVs.

# 

**Figure 6:** EV charging price change caused by FDI attack.

# 6. Discussion

In this study, the types of cyber attacks on smart grids were examined. The possible effects of cyber attack types on the system were observed and graphed. An algorithm was designed to quickly gather the data of a smart grid system consisting of ten digits. Graphics were created through simulations of the designed algorithm. Factors such as the variety of graphics created and their availability in a short time reduced the detection time of cyber attack types. The developed detection mechanism not only detects the cyber attack event but also detects its type. With the recent improvements, it was aimed to increase the effectiveness of the response mechanism. The protection mechanism against malicious people who want to perform a cyber attack has been updated and made easy to update. Improvements were made to the response time, which was emphasized in the referenced articles. Detection and identification of the type of cyber attack were made very easy, and scenarios that could occur in the simulations were run. The results obtained were used as a source in the response mechanism.

Contributions were made to the studies in the literature, such as establishing a ten-digit network, creating a data algorithm, graphing the data, and creating a response algorithm. On top of all these contributions, technologies such as data types, databases, algorithms, and sensors can be added to the studies in this field. In addition to the algorithm to be developed for the system to be independent, the issue of keeping the data on systems that are completely independent of the authority can be examined. Smart grid systems to be developed on blockchain technology can be designed. Different response and defense mechanisms can be created.

# 7. Conclusion

Cyber attacks that try to compromise the security of smart grids are a serious issue that provides a number of challenges. Worldwide cyberattacks against smart grids were recorded between 2010 and July 2022. Attack site, attack range, attack kind, and outcome differed between these occurrences. Modern methods are presented along with their attack methodology, effects, and detection strategies. A thorough thematic taxonomy of cyberattacks on smart grids is investigated. In this study a model was created, in the environment of MATLAB and Simulink in terms of the reality of the simulation, a realistic environment has been prepared by simulating power generation and distribution systems as well, and an attack was carried out by interfering with the normal working and pricing algorithms of the system by applying FDI malware on a microgrid, and the changes on the model were observed. Also, we simulate and observed the two price algorithms which are the following: hijacked algorithm pricing and normal algorithm pricing. In order to prevent this and similar attacks and to develop counter-defense mechanisms, it is essential to create a model in which the results of the attack and the situations experienced during the attack can be observed and to try the attacks on this model. In light of evolving technology and the ongoing discovery of new attack tactics, future research directions are thus outlined for the robust cybersecurity of smart grids against sophisticated assaults.

**References**

1. [1] Zubieta, L. E. Are microgrids the future of energy?: DC microgrids from concept to demonstration to deployment. *IEEE Electrification Magazine* 2016, *4*(2), pp. 37-44.
2. [2] Ersoz, B.; Bulbul, H.I. A Research on Importance of Using Renewable Energy Sources by Organizations within The Scope of Green Deal Preparations. *11th IEEE International Conference on Renewable Energy Research and Applications* 2016, pp. 213-214.
3. [3] Martins, F.; Felgueiras, C.; Smitková, M. Fossil fuel energy consumption in European countries. *5th International Conference on Energy and Environment Research. Energy Procedia*, 153, pp. 107-111, 2018.
4. [4] International Energy Agency. Africa energy Outlook. International Energy Agency, 2019.
5. [5] African Development Bank. Revisiting power sector reforms in Africa. Abidjan: Africa Development Bank and Association of Power Utilities of Africa, 2019.
6. [6] Western Electricity Coordinating Council, NERC/WECC Planning Standards, 2012.
7. [7] Ayadi, F.; Colak, I.; Garip, I.; Bulbul, H.I. Impacts of Renewable Energy Resources in Smart Grid. *IEEE International Conference on Smart Grid, 8,* pp. 183-184, 2020.
8. [8] Eder-Neuhauser, P.; Zseby, T.; Fabini, J.; Vormayr, G. Cyber attack models for smart grid environments. *Sustainable Energy, Grids and Networks, 12*, pp. 10-29, 2017.
9. [9] Sun, C. C.; Hahn, A.,; Liu, C. C. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems, 99*, pp. 45-56, 2018.
10. [10] Acarali, D.; Rajarajan, M.; Chema, D.,; Ginzburg, M. Modeling DoS Attacks & Interoperability in the Smart Grid. *29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-6, August 2020.
11. [11] Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Ong, Z. Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems, 32(4),* pp. 3317-3318, 2016.
12. [12] Saravanan, A.; Bama, S. S. A review on cyber security and the fifth generation cyberattacks. *Oriental Journal of Computer Science and Technology*, *12*(2), pp. 50-56, 2019.
13. [13] Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-attack modeling analysis techniques: An overview. *IEEE 4th international conference on future internet of things and cloud workshops*, pp. 69-76, August 2016.
14. [14] Li., P; Salour., M; Su., X. A survey of internet worm detection and containment, *Commun. Surv. Tutor. 10 (1),*  pp. 20–35, 2020, http://dx.doi.org/10.1109/COMST. 2008.4483668.
15. [15] Saeed, I.A.; Selamat, A.; Abuagoub, A.M.A. A survey on malware and malware detection systems, *Int. J. Comput. Appl. 67 (16)*, pp. 25–31, 2013, http://dx.doi. org/10.5120/11480-7108.
16. [16] Bruno, C.; Guidi, L.; Lorite-Espejo, A.; Pestonesi, D. Assessing a potential cyber[1]attack on the italian electric system, *IEEE Secur. Priv. 13 (5),* pp. 42–51, 2015, <http://dx.doi.org/10.1109/MSP.2015.99>.
17. [17] Vineetha, C. P.; Babu, C., A. Smart grid challenges, issues and solutions, *International Conference on Intelligent Green Building and Smart Grid (IGBSG)*, pp. 1–4, April 2014.
18. [18]Major german energy supplier hit by cyberattack. Available online: <https://therecord.media/major-german-energy-supplier-hit-by-cyberattack/>
19. [19] Martínez, J.; Durán, J. M.; Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study. *International Journal of Safety and Security Engineering, vol, 11(5)*, pp. 537-545, 2021.
20. [20] Significant cyber incidents. Available online: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
21. [21] Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Dong, Z. Y. "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," , *IEEE Transactions on Power Systems, vol. 32*, no. 4, pp. 3317-3318, July 2017, doi: 10.1109/TPWRS.2016.2631891,.
22. [22] Kesler, B. The vulnerability of nuclear facilities to cyber attack; strategic insights: *Strategic Insights*, Spring 2011.
23. [23] Pillitteri, V. Y.; Brewer, T. L. “NIST Guidelines for Smart GridvCybersecurity,” *NIST Interagency/Internal Report (NISTIR)- 7628 Rev 1*, Sept. 2014.
24. [24] Smart Grid Security Recommendations for Europe and Member States ENISA Report 2012-07-01.
25. [25] Cisco White Paper, Cisco Connected Grid Security for Field Area Network, 2012.
26. [26] Microgrid Protection By Ali Hooshyar, Member, IEEE and Re za Iravani Fellow, IEEE.
27. [27] Sridhar S,; Hahn A,; Govindarasu M, Cyber–Physical System Security for the Electric Power Grid, *Proceedings of the IEEE, Vol. 100*, No. 1, January 2012, DOI 10.1109/JPROC.2011.2165269.
28. [28] Tan, K. M.; Ramachandaramurthy, V. K.; Yong, J. Y. Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques. *Renewable and Sustainable Energy Reviews, 53*, pp. 720-732, 2016.
29. [29] <https://ev-database.org/>
30. [30] <https://hourlypricing.comed.com/>
31. [31] Laaksonen, H.; Saari P.; Komulainen, R. "Voltage and frequency control of inverter based weak LV network microgrid," *2005 International Conference on Future Power Systems*, pp. 6, 2005, doi: 10.1109/FPS.2005.204293.

# Appendix A

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Car Model** | **Battery Capacity (kWh)** | **Normal Charging Power (Wh)** | **Initial Battery Capacity** | **Final Battery Capacity** | **Arrival Time** | **Normal Charge End Time** | **Car Departure Time** |
| 14 | 39200 | 7200 | 5 | 92 | 09:22 | 14:06 | 18:20 |
| 16 | 60000 | 7700 | 51 | 95 | 07:42 | 11:08 | 12:19 |
| 21 | 39200 | 11000 | 15 | 95 | 16:10 | 19:01 | 21:50 |
| 13 | 32000 | 7200 | 20 | 69 | 08:40 | 10:51 | 12:41 |
| 1 | 36000 | 3600 | 6 | 61 | 07:27 | 12:57 | 16:37 |
| 13 | 32000 | 7200 | 13 | 73 | 08:57 | 11:37 | 12:31 |
| 13 | 32000 | 7200 | 7 | 70 | 18:09 | 20:57 | 22:42 |
| 17 | 38300 | 7200 | 10 | 75 | 18:49 | 22:16 | 22:18 |
| 21 | 39200 | 11000 | 3 | 96 | 12:16 | 15:35 | 18:52 |
| 1 | 36000 | 3600 | 57 | 90 | 16:38 | 19:56 | 22:31 |
|  |  |  |  |  |  |  |  |

TABLE 1:Data table for electric vehicles used in simulation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Car ID** | **Car Names** | **Battery Capacity (kWh)** | **Normal Ch Power (kWh)** | **Fast Ch Power** |
| 1 | Nissan Leaf | 36 | 3.6 | 40 |
| 13 | VW e-Golf | 32 | 7.2 | 40 |
| 14 | Kia Soul EV | 39.2 | 7.2 | 40 |
| 16 | Chevy Bolt | 60 | 7.7 | 55 |
| 17 | Hyundai Ioniq EV | 38.3 | 7.2 | 36 |
| 21 | Hyundai Kona Electric | 39.2 | 11 | 35 |
|  |  |  |  |  |

TABLE 2: Electric vehicle model table used in simulation