International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

A Comprehensive Review Study of Cyber-Attacks and Cyber Security

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA. doctorabhilashmaroju@gmail.com

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. rohit.vallabhaneni.2222@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA. sravanthi.dontu13@gmail.com

ABSTRACT

In today's world, the majority of governmental, cultural, social, economic, and commercial interactions and activities take place online. This includes interactions between nations, individuals, NGOs, and government agencies. The threat of cyberattacks and wireless communication technologies has recently become an issue for numerous private organisations and government agencies across the globe. Nowadays, our world relies heavily on electronic technology, and safeguarding this data from cyber-attacks is no easy feat. Cybercriminals target businesses with the intention of stealing money. Cyberattacks may also serve political or military objectives in certain instances. Computer viruses, information breaches, data distribution services (DDS), and other attack vectors are among the causes of these damages. In order to accomplish this goal, different organisations employ different strategies to safeguard against cyberattacks. The most recent information technology data is tracked in real-time by cyber security. So far, academics from all around the globe have suggested a number of ways to either stop cyberattacks in their tracks or at least mitigate the harm they do. A few of the approaches have moved on to the study phase, while others are still in the operational stage. The purpose of this research is to examine the offered approaches, identify their strengths and shortcomings, and conduct a thorough evaluation of the standard advancements made in the area of cyber security.

1. INTRODUCTION

Integration of cutting-edge generating schemes, control techniques, data transmission advancements through open communication networks, and security measures of communication networks through smart systems are all contributing to the field of power systems' ongoing improvement. On the other hand, power systems are facing new problems as a result of integrating new technology. Incorporating RES into power generation is a great way to reduce pollution and help the environment, but running power systems that rely on RES results in poor frequency stability performance because the power they produce is intermittent. Nevertheless, as RES technologies have expanded, smart inverters have become more popular, and smart controlled loads have been developed to accommodate both distributed generation and RES, RES have become a substantial energy source in several nations. With their ability to manage power flow and detect faults, smart inverters are indispensable in power networks that utilise distributed energy resources (DER). They also serve as an interface between the grid and DER. Cyberattacks are a real threat to smart technologies because of the power system instability they might cause and the fact that they support both wired and wireless communication technologies. Another factor that can make smart power grids with intermittent DER more susceptible to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

attacks is the development of wide-area control and monitoring tools based on the Internet of Things (IoT). Consequently, from the perspective of power system operations, increase of stability and attack-resilient control of power systems are crucial areas that necessitate ongoing research. The focus of this research is on the load frequency control (LFC) system's cyber-security and frequency stability in relation to this [2].

Any significant frequency deviance from the nominal value has the potential to compromise the operational safety, dependability, and security of a power system, making frequency performance monitoring and regulation an absolute necessity. A frequency deviation from the nominal value occurs when there is an imbalance between the power consumption by the load and the power generation. The primary goal of implementing the LFC scheme is to eliminate non-zero frequency deviation by balancing the power system's load and frequency. There are three tiers to the process of improving frequency performance through the adoption of various frequency regulating technologies. The control of generation units carries out the first two levels, while loads, such as in the case of load shedding, implement the third level. Governor control, sometimes known as main control, secondary control, or supplemental control, and tertiary control are the three levels of frequency control [3].

Unlike traditional LFCs, which relied on dedicated communication channels to transfer signals between the generator unit, control centre, and remote terminal units (RTUs), modern deregulated power system LFC methods make use of open communication infrastructure. Attacks such as channel jamming, fake data injection, power system load modifications, and others are more likely to affect the highly decentralised LFC design with an open communication network [4]. Furthermore, LFC techniques are required to produce control signals on a second-by-second basis. Hence, sophisticated data validation algorithms for estimating and validating measurement data are out of the question for the LFC loop. Because of this, malicious actors can exploit it to alter the measurement results using less complex mathematical techniques. The LFC system is susceptible to cyber-attacks due of these conditions. Consequently, it is crucial to investigate and assess the effects of attacks on the LFC system. Investigating the cyber-security of LFC systems also aids in the creation of defence and detection methods that lessen the effects of cyber-attacks. Breach of operational frequency is a measure of the impact of the attack on the LFC system. Resilient control algorithms are a common component of LFC system defence systems.

2. CYBERSECURITY IN POWER GRIDS

Power systems are vulnerable to cyber assaults because of the amount of information and communication technology they use. Criminals can trigger blackouts, economic losses, and system instability by interfering with the information exchange process using fraudulent data. Another technique that can be used to hide power system failures is false data injection (FDI). The operator's ability to see the problems and take corrective action will be compromised.

For instance, malevolent actors opened substation breakers in 2015 as part of an assault on the Ukrainian power grid [5]. Examining the effects of FDI on the power system is important for developing appropriate safeguards to increase system resilience. Foreign direct investment (FDI) attack mechanism and effect have thus been the subject of much research.

Figure 1 shows the three main ways in which foreign direct investment (FDI) negatively impacts power systems: state estimate, command generation, and control action actuation. By aiming squarely at economic dispatch, FDI has the potential to trigger the production of erroneous control commands. The line flows above their overload tripping threshold, resulting in line outages and potentially cascade failure, as described in [6, 7], caused by the injection of bogus load data into security-constrained economic dispatch. A higher operational cost or illicit profit from electricity markets can be achieved through the deliberate manipulation of economic dispatch, as shown in [8]. When the perpetrators do not possess complete knowledge of the network's details, the possible danger of FDI assaults on economic dispatch is examined in [9]. A power system can also be compromised by FDI if it attacks the measurement and estimation of the system's status and damages the integrity of the information pertaining to the power system's state. Two examples of such attacks are given in [10] and [11], respectively, where FDI is employed to compromise the SCADA system and inject fabricated data into the PMU to deceive the control centre. Cybercriminals can fool operators into thinking the system is running well when, in fact, it isn't, leaving them vulnerable to attacks. The use of FDI to introduce random estimate errors into the state estimator is covered in [12], while FDI is used for nonlinear state estimation in power systems and the related countermeasures are addressed in [13]. The stability of the electricity system can also be negatively affected by FDI since it changes the control input to the system. A cluster of distributed generators disagrees because FDI corrupts the input signal to a follower distributed generator. In [13], FDI is employed to create a synchronisation issue in isolated

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

microgrids, instability is induced by controlling system breakers, and transient instability is initiated by altering the gains of voltage control devices. In order to introduce frequency instability into the system, an attacker uses mimicked inertia control.

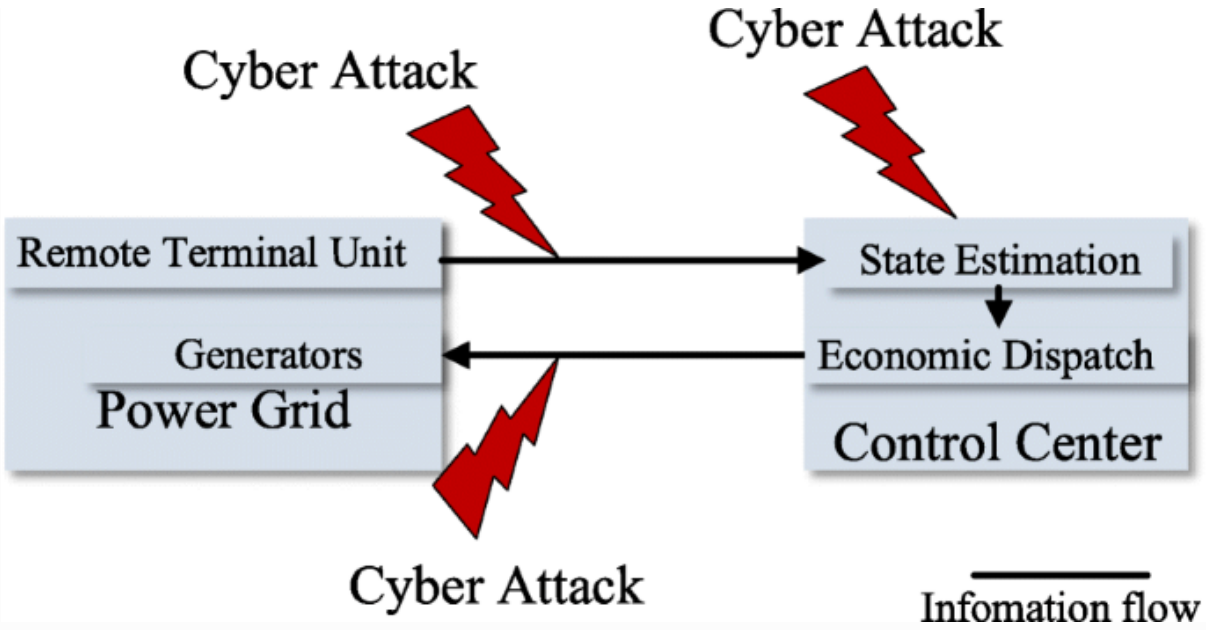

Fig 1: Cyber-attacks on a power system

Research on the effects of foreign direct investment (FDI) thus far has mostly relied on models that account for a single snapshot in time or a steady-state power system, rather than the dynamic, transient nature of such a system. At each attack time instant, skilled attackers may alter the injected data to either evade detection or decrease energy use. Also, since actual power systems are networked control systems, the steady-state model isn't good enough to assess the FDI risk. While economic dispatch and system state estimates are resistant to FDI, the automatic generation control system is still vulnerable and could be used to compromise the power system's secure operation. To completely uncover the danger of FDI and subsequently develop appropriate countermeasures, it is crucial to analyse the dynamic characteristic of FDI as well as the transient characteristic of the power system.

This study takes a complete look at the research on foreign direct investment (FDI) attacks on economic dispatch, state estimation, and power system dynamic stability (Fig. 1) to reveal the risk of FDI.

3. REVIEW STUDY OF CYBER-ATTACKS AND CYBER SECURITY

The Internet has been an integral part of people's daily lives and a major player in international communication for over 20 years. The Internet now has approximately 3 billion users globally, all thanks to innovations and cheap costs in this sector, which have greatly boosted the availability, use, and performance of the Internet. The worldwide web that the Internet has made possible is worth billions of dollars to economies around the world every year [14].

Cyberspace is now the primary venue for the vast majority of international economic, commercial, cultural, social, and governmental exchanges, involving nations, individuals, NGOs, and governmental and non-governmental organisations at all levels [15]. Many important and delicate systems and infrastructures are either already present in cyberspace or are managed, controlled, or exploited via it. Additionally, the majority of important and delicate data is either transported to or created in cyberspace.

A large percentage of residents' time and energy is spent interacting in this space, and the majority of media activities are moved here as well. It's also where most financial

transactions take place. Income from internet firms as a percentage of countries' GDP has grown substantially, and cyberspace indicators make up a sizable portion of the metrics used to gauge the level of progress. Spending a large portion of national financial and spiritual capital on this space, as well as a large portion of individual residents' material income and spiritual accomplishments, is concentrated here [16].

What this means is that many parts of people's life are dependent on this area, and that problems, uncertainty, and instability here will have repercussions in other parts of people's lives. Cyberspace, however, has presented nations with new security concerns. Cyberspace is home to both powerful and vulnerable actors, including nations, terrorist organisations, and even individuals, who pose risks like cybercrime, cyberterrorism, cyberespionage, and cyberwarfare due to factors like the area's anonymity, low barrier to entry, and lack of public transparency [17].

This is what sets cyber threats apart from more conventional forms of national security, which are more open and whose perpetrators are easily identifiable governments and nations in a particular region; this has made conventional forms of national security less effective in this area. The potential repercussions of cyberattacks have been considered by experts for over ten years. Severe and sometimes widespread physical or economic damage can occur in a variety of ways. For example, a virus could launch an attack on a country's financial documents or stock market, or it could send the wrong message and cause the power plant to shut down or fail. Another possibility is that it could disrupt the air traffic control system, leading to air accidents [18].

Consequently, professionals will have a hard time addressing the issue's many and diversified elements and providing legal guidance and analysis unless governments agree on a universally accepted definition of a cyber-attack. Now we need to know what exactly constitutes a cyber-attack, what makes one different from another, and whether or not any attack that happens in cyberspace qualifies as an attack in the conventional sense [19].

In order to continue and identify the repercussions of this form of cyberattack, the legal environment must take into account the existence of a thorough definition of cyberattack. Without a definitive and all-encompassing definition, the leading legal road becomes murky, different interpretations and practices emerge, and, in the end, often conflicting legal conclusions are reached [20]. So, it's crucial to have a good definition, at least for the topic's introduction, explanation, adaption, and analysis; in-depth research is also required. [21-22] Following an explanation of what a cyberattack is and how it works, this study go on to classify and divide cyberattacks, before finally looking at current definitions from the perspective of international organisations and experts. The paper concludes with this section.

CONCLUSION

In this new millennium, cyberspace and associated technologies have emerged as a major driving force. Because of cyberspace's features—its cheap entry prices, anonymity, vulnerability, and asymmetry—the phenomenon of power dissipation has emerged. This suggests that private companies, organised criminal groups, individuals, and terrorist organisations are the new power brokers, although governments still play a significant role. Governments' ability to maintain national security will, of course, be unaffected by this occurrence. Several methods exist for assessing this impact. The idea of safety comes first. Nowadays, the danger of a decline in the quality of life of citizens poses a greater threat to national security than traditional military concerns and internal/external border difficulties. Second, the physical location of cyber threats is becoming irrelevant. There used to be a designated place where military dangers could be found. This made it easy to handle, at least from an identifying standpoint. The third factor is the seriousness of cyber dangers.

REFERENCES

1. Arbab Zavar, B.; Palacios-Garcia, E.J.; Vasquez, J.C.; Guerrero, J.M. Smart inverters for microgrid applications: A review. *Energies* 2019, *12*, 840
2. Wang, Q.; Wang, H.; Zhu, L.; Wu, X.; Tang, Y. A Multi-Communication-Based Demand Response Implementation Structure and Control Strategy. *Appl. Sci.* 2019, *9*, 3218.
3. Oshnoei, A.; Khezri, R.; Muyeen, S.M.; Blaabjerg, F. On the contribution of wind farms in automatic generation control: review and new control approach. *Appl. Sci.* 2018, *8*, 1848.
4. Shen, Y.; Fei, M.; Du, D. Cyber security study for power systems under denial of service attacks. *Trans. Inst. Meas. Control* 2019, *41*, 1600–1614.
5. Liang, G., Zhao, J., Luo, F. J., Weller, S., & Dong, Z. (2017). A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid, 8(4), 1630–1638. Google Scholar

6. Che, L., Liu, X., Shuai, Z., Li, Z., & Wen, Y. (2018). Cyber cascades screening considering the impacts of false data injection attacks. IEEE Transactions on Power Apparatus and Systems, 33(6), 6545–6556. Google Scholar
7. Che, L., Liu, X., Li, Z., & Wen, Y. (2019). False data injection attacks induced sequential outages in power systems. IEEE Transactions on Power Apparatus and Systems, 34(2), 1513–1522. Google Scholar
8. Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load redistribution attacks in power systems. IEEE Transactions on Smart Grid, 3(3), 382–390. Google Scholar
9. Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power system: A fast solution. IEEE Transactions on Smart Grid, 8(2), 1023–1025. Google Scholar
10. Xiang, Y., Ding, Z., Zhang, Y., & Wang, L. (2017). Power system reliability evaluation considering load redistribution attacks. IEEE Transactions on Smart Grid, 8(2), 889–901. Google Scholar
11. Liu, X., & Li, Z. (2014). Local load redistribution attacks in power systems with incomplete network information. IEEE Transactions on Smart Grid, 5(4), 1665–1676. Google Scholar
12. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Transactions on Smart Grid, 6(4), 170–1721. Google Scholar
13. Zhang, Z., Gong, S., Dimitrovski, A., & Li, H. (2013). Time synchronization attack in smart grid: Impact and analysis. IEEE Transactions on Smart Grid, 4(1), 87–98
14. Aghajani and Ghadimi, 2018 Aghajani G., Ghadimi N. Multi-objective energy management in a micro-grid Energy Rep., 4 (2018), pp. 218-225
15. Ahmed Jamal et al., 2021 Ahmed Jamal A., et al. A review on security analysis of cyber physical systems using machine learning Mater. Today: Proc. (2021)
16. Akhavan-Hejazi and Mohsenian-Rad, 2018 Akhavan-Hejazi H., Mohsenian-Rad H. Power systems big data analytics: An assessment of paradigm shift barriers and prospects Energy Rep., 4 (2018), pp. 91-100
17. Li et al., 2021 Li J., Sun C., Su Q. Analysis of cascading failures of power cyber–physical systems considering false data injection attacks Glob. Energy Interconnect., 4 (2) (2021), pp. 204-213
18. Sarker, 2021 Sarker I.H. Cyberlearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks Internet Things, 14 (2021), Article 100393
19. Chandra and Snowe, 2020 Chandra A., Snowe M.J. A taxonomy of cybercrime: Theory and design Int. J. Account. Inf. Syst., 38 (2020), Article 100467
20. Chen et al., 2021 Chen J.-K., et al. Cyber deviance among adolescents in Taiwan: Prevalence and correlates Child. Youth Serv. Rev., 126 (2021), Article 106042.
21. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
22. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D.Dissertation.University of South Alabama