Pegem Journal of Education and Instruction, Vol. 13, No. 3 , 2023 (pp. 478-488)

RESEARCH ARTICLE WWW.PEGEGOG.NET

OPTIMIZING DISTRIBUTED SYSTEM SECURITY:MACHINE LEARNING BASED CYBERATTACK CORRELATION AND MITIGATION

[1]Dr.U.Srilakshmi, [2]M. Shreya, [2]Shamlet Malathi, [4]B. Prasanna Lakshmi

[1]Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

Email: drusl.swec@gmail.com

[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT

Cyber-physical system security for electric distribution systems is critical. In direct switching attacks, often coordinated, attackers seek to toggle remote-controlled switches in the distribution network. Due to the typically radial operation, certain configurations may lead to outages and/or voltage violations. Existing optimization methods that model the interactions between the attacker and the power system operator (defender) assume knowledge of the attacker's parameters. This reduces their usability. Furthermore, the trend with coordinated cyberattack detection has been the use of centralized mechanisms,correlating data from dispersed security systems. This can be prone to single point failures. In this paper, novel mathematical models are presented for the attacker and the defender. The models do not assume any knowledge of the attacker's parameters by the defender. Instead, a machine learning (ML) technique implemented by a multi-agent system correlates detected attacks in a decentralized manner, predicting the targets of the attacker. Furthermore, agents learn optimal mitigation of the communication level through Q-learning. The learned attacker motive is also used by the defender to determine a new configuration of the distribution network. Simulations of the technique have been performed using the IEEE 123-Node Test Feeder. The simulation results validate the capability and performance of the algorithm.

Keywords: Existing optimization methods that model the interactions between the attacker and the power system operator (defender) assume knowledge of the attacker's parameters.

in fault or under attack will cause unusual

INTRODUCTION

It is important to protect smart distribution grids, but also a challenging task because of the inherent distributed energy resources (DER) and topology complexities Raw electrical waveforms, signals of electrical networks, together with those in cyber networks provide great potentials in cyber attack detection .For example, devices in power networks must leave clues of their operational status and health (including faults or attacks) information in the raw electrical waveform signals: a cyberdevice

Corresponding Author e-mail: drusl.swec@gmail.com
How to cite this article: 1Dr.U.Srilakshmi, 2M. Shreya, 2Shamlet Malathi, 4B. Prasanna Lakshmi. OPTIMIZING DISTRIBUTED SYSTEM SECURITY:MACHINE LEARNING BASED CYBERATTACK CORRELATION AND MITIGATION.Pegem Journal of Education and Instruction, Vol. 13, No. 3, 2023, 478-488
Source of support: Nil **Conflicts of Interest:** None.
DOI: 10.48047pegegog.13.03.48
Received: 12.09.2023
Accepted: 22.10.2023 **Published:** 24.11.2023

energy consumption pattern in power networks a power electronics or electric machine in fault or under attack may cause unusual harmonics or energy profile in

electrical networks By analyzing the electrical waveform signals and their root cause, waveform analytics can present utilities with a complete picture of the health and status of their system, both during outages and normal operating conditions. It could also provide a variety of operational benefits to system operators, asset management personnel, and repair crew. Electronic sensors placed on powergrids and distribution systems can either measure the electricity properties, such as phasor measurement unit (PMU) sensors CYBER attack localization is or directly record the raw electrical waveform using waveform measurement unit (WMU) depending on the needed fidelity of monitoring applications. Thanks to developed network connectivity, the streaming monitoring data flow can be obtained and analyzed online and in realtime The network of the waveform sensors form an Internet of Things (IoT) system where the waveform sensors are viewed as networked IoT sensing devices. Therefore, we can potentially use the information embedded in electrical signals to enable security monitoring, diagnosis, and prognosis in the power networks. The possibility may be well beyond what we can imagine now. It broadly applies to many cyber-physical systems (CPS) and applications, such as power distribution

networks, multi-stage manufacturing systems, electric vehicles, and so on Cyber attacks towards connected IOT devices trigger anomalies in system statistics, energy consumption, as well as electrical waveforms Thus, recorded waveform which carries high fidelity current and voltage information should be adequate for cyber attack characterization. Furthermore, the transmission of the high-frequency waveform data is feasible in practice

Data-driven methods have been widely adopted for event localization in power electronics networks and active distribution systems. Rulebased data-driven analytics [23], signal propertybased approach and neural networks (NN) based algorithms, such as autoencoders convolutional neural network (CNN) have been developed. However, N based algorithms typically require a large amount of training data to capture the sophisticated features, which cannot be fully simulated or acquired from real applications. Thus, combining the rule-based signal processing methods and machine learning methods could lead to a solution tackling the challenging problem using an affordable data size.There have been numerous works targeting the event and cyber attack localization problem Dynamic data analytics based localization is always a major branch for the distribution networks, DC microgrid, islanded microgrid This paper proposes a new adaptive hierarchical framework for efficient and accurate cyber attack detection and localization by taking advantage of the electrical waveforms (Fig. 1). The proposed approach has a hierarchical architecture that divides the whole network into sub-groups and then locates the cyber attack within one local cluster. Based on a modified unsupervised clustering and an deep learning based anomaly detection method, cyber attacks in the active distribution systems can be adaptively detected and located. The performance of the proposed approach has been tested by multiple cyber attack scenarios in two representative case studies.Our contributions are summarized as follows:We propose an adaptive hierarchical cyber attack detection and localization framework for active distribution systems with DERs using the electrical waveform; _ High fidelity models of DER and cyber attacks are built to analyze the impacts of cyber attacks towards the distribution networks; _ Extensive experiments are utilized to evaluate the proposed approach performances with quantitative analytics **W**ITH the integration of advanced communication technology, the power grid is increasingly remotely monitored and

controlled. Nevertheless, the advancement has also made the smart grid more vulnerable to cyber attacks. In December 2015, six distribution utilities in Ukraine suffered cyber attacks. The ensuing outage affected about 225,000 customers [1]. Significant research has been conducted in the area of distribution system cyber security, and several techniques have been proposed for different applications.

LITERATURE REVIEW

"Smart grid cyber-physical attack and defense: A review," Recent advances in the cyber-physical smart grid (CPSG) have enabled a broad range of new devices based on the information and communication technology (ICT). However, these ICT-enabled devices are susceptible to a growing threat of cyber-physical attacks. This paper performs a thorough review of the state-of-the-art cyber-physical security of the smart grid. By focusing on the physical layer of the CPSG, this paper provides an abstracted and unifed state- space model, in which cyber-physical attack and defense models can be effectively generalized. The existing cyber- physical attacks are categorized in terms of their target components. We then discuss several operational and informational defense approaches that present the current state-of-the-art in the feld, including moving target defense, watermarking, and datadriven approaches. Finally, we discuss challenges and future opportunities associated with the smart grid cyber- physical security. CYBER-PHYSICAL systems (CPSs) are smart systems that include engineered interacting networks of physical and computational components [1]. The comprehensively interconnected and integrated systems contribute new functionalities to enable technological development in critical infrastructures, such as electric power systems, water networks, transportation, home automation, and health care. A CPS encompasses complex systems of control, awareness, computing, and communication. The complexity and heterogeneity have indicated the potential challenges to the security and resilience of CPSs. The interconnection of bulk physical layer components is challenging the protection against inherent physical vulnerabilities therein. On the other hand, cyber-integration, which relies on network communication and the internet of things (IoT) based devices, requires extraordinary investments in security designs and upgrades against unanticipated threats from cyberspace [2]. A cyberphysical attack is defned as a security breach in cyberspace that adversely affects the physical space of a CPS. [3]. Cyberphysical attacks compromise the confdentiality, integrity, and availability of information by coupling

cyber and physical spaces in a CPS. In the past decades, several noteworthy cyber-physical attacks have been reported in the industry, facilitating synergistic efforts from industry practitioners and research communities towards a new CPS security era [4]. The frst proclaimed cyber-physical attack dated back to 1982 in the Siberian wilderness, where attackers manipulated the pipeline control software, which led the valves' control to misbehave, resulting in severe crossing of pressure limits and eventually a massive explosion [5]. In 2003, the Slammer worm invaded the control system of the David-Besse nuclear plant in Ohio through a contractor's network, which disabled the supervisory system for 5 hours [6]. In June 2010, a cyber worm dubbed "Stuxnet" struck the Iranian nuclear fuel enrichment plant by utilizing four zero-day vulnerabilities and digitally signed certifcates to bypass intrusion detection. The targets were the programmable logic controllers in the supervisory control and data acquisition (SCADA) system [7]. The Stuxnet maliciously alternated the frequency of electrical current powering the centrifuges and then switched them between high and low speeds at intervals for which the machines were not designed [8]. In December 2015, a coordinated cyberattack compromised three Ukrainian electric power distribution companies. Thirty substations suffered blackout for about three hours, resulting in wide-area power outages affecting approximately 225,000 customers. BlackEnergy3 malware was

used to steal the authorized users' virtual private network credentials, and a telephonic denialof-service (DoS) attack was executed to frustrate reports of outages [9]. The smart grid landscape, arguably one of the most complex CPSs in history, is undergoing a radical transformation. Particularly, increased renewable energy resources, demand diversifcation, and integration of information and communication technologies (ICTs) [10]. The cyber-physical smart grid (CPSG) that has organized a universal cyberinfrastructure interwoven with the bulk physical systems is susceptible to cyber-physical attacks. A wide variety of motivations exist for launching such an attack in the smart grid, ranging from economic reasons, to terrorism, to a grudge (a disgruntled employee [11]). A large body of recent work has been dedicated to addressing the cyber-physical security of smart grids, with many warnings becomes prominent [12]– [15] and new vulnerabilities are continuously unveiled [16]. Regarding cyber and physical security, neither of them alone can provide broad

solutions without incorporating the other. In this regard, the investigations of the cyber-physical attacks and the developments of effective defense strategies are still incomprehensive. Thereby, it has become paramount to keep up with the latest progress along the research frontier of smart grid security, especially from a joint perspective of cyber and physical security. This paper tries to bridge this gap by providing a comprehensive review of cyber-physical threat models and defense mechanisms. Over the last fve years, several survey and review papers on the cyber-physical security of the smart grid have been published. Table 1 lists a comparison between this paper and other works in terms of the publication year, smart grid models, attack taxonomy, technological focus, challenges and opportunities, and the review scope. The contributions of this paper, as illustrated in Table 1, are four-fold. First, a discrete-time nonlinear time-invariant system is proposed to represent a CPSG by using the statespace representation. Such a high-level abstraction is a useful strategy to form the foundation and generalize a defense analysis across all attack types. Second, the state-of-theart cyber-physical attack models are summarized based on the proposed abstraction and categorized according to the control-feedback loop segment each attack involves. This new taxonomy provides the grid operator with intuitive situational awareness on how to enhance the system's cyberphysical security. Third, cyber-physical security of the smart grid is an extremely hot research topic, and a lot of good works have been published every year. Therefore, it is a much needed effort to keep up with the progress and furnish a concise summary and a clear categorization for readers to understand the current state-of-the-art. In order to provide a timely review, this paper surveys the most recent publications, including 78 in the last fve years (i.e., 2016- 2020) 49 of which were published in the past three years (i.e., 2018-2020). A thorough review of the cutting-edge defense approaches such as data-driven machine learning, moving target defense, and watermarking is provided. Finally, the challenges and opportunities of future CPSGs are discussed, which may shed light on cyber-physical security issues that the next-generation smart grid needs to tackle. **IN "Smart grid security: Attacks and defenses,"**

The smart grid (SG) consists of three main components, that is, Information Technology (IT), Operational Technology (OT), and Advanced Metring Infrastructure (AMI). Due to the integration of these components, electricity is efficiently managed and transmitted. Over the past few

years, cyberattacks on the SG have risen. Several studies are being conducted to mitigate these attacks. A survey on cyberattacks on IT, OT, and AMI is conducted. We have also identified new research challenges and explored future research directions Recently, the smart grid (SG) has served as a control centre that manages electricity generation and efficiently distributes electricity to households, industrial areas, and social infrastructures. The SG integrates Information Technology (IT), Operational Technology (OT), and Advanced Metring Infrastructure (AMI) components. It is also responsible for controlling and managing each of these components. OT refers to hardware and software controlling and monitoring industrial infrastructure's physical devices and work processes. IT consists of an application server, a storage server, and a historical data storage server. AMI is a communication protocol that enables data sharing between smart metres and SG control centres [1, 2]. Almost, every component within the SG is vulnerable to cyberattacks [3-6]. For example, in 2016, a power grid in northern Ukraine was attacked by Russian hackers. They infiltrated an IT-based data network and caused malfunctions in the substations' OT devices (automatic control system). The attacks caused several hours of power outages during the Christmas season [7]. In another similar incident, a DoS attack was carried out on smart metres [8]. With the growing importance of SG security, researchers have proposed various detection and defence mechanisms to protect the SG infrastructure. Several studies have introduced solutions for securing communication among devices under the ISO/IEC protocol, AMI, DCS, ICS, and SCADA [9-12]. Some researchers have studied the communication security between EVs and a Charging Station (CS) through the AMI network. Other researchers have focussed on mutual authentication and secure data transmission between EVs and CSs. These studies propose a secure PLC communication method using the SAE J1772 protocol

[13, 14]. Other studies classify various cyberattacks against the SG according to their characteristics. Also, they propose methodologies that enable a selection of an appropriate defence strategy . In the previous surveys on SG security, attacks have been classified according to protocol and equipment types . In one of the recent survey studies, there is a study that categorises cyber-physical attacks on smart metres in AMI and countermeasures A study measures the impact of total failure of the

SG by the cascading effect of malfunctioning in dispensing electricity [. A technical review discusses the conceptual model of cyber-physical attacks. It analyses the physical consequences of attacks merged with cyber-physical distributions. Another study introduced a protection mechanism for user privacy on the AMI. Also, it classifies other mechanisms by security objectives, such as integrity, confidentiality, and authority . There is a survey on the security issues of IoT devices in OT facilities It explains that cyberattacks on these devices can develop into a serious security threat to the entire SG infrastructure.

EXISTING SYSTEM

With the integration of advanced communication technology, the power grid is increasingly remotely monitored and controlled. Nevertheless, the advancement has also made the smart grid more vulnerable to cyberattacks. In December 2015, six distribution utilities in Ukraine suffered cyberattacks. The ensuing outage affected about 225,000 customers [1]. Significant research has been conducted in the area of distribution system cybersecurity, and several techniques have been proposed for different applications.

Drawback in Existing System

- **Data Quality and Quantity:**

  Insufficient Training Data: Machine learning models require large and diverse datasets for effective training. In the case of cyberattacks on distribution systems, obtaining sufficient labeled data for different attack scenarios can be challenging.

- **Interpretability and Explainability:**

  Black Box Nature: Many machine learning models, especially complex ones, operate as "black boxes," making it challenging to understand the reasoning behind their decisions. Lack of interpretability can hinder trust and make it difficult for operators to comprehend the model's outputs.

- **Integration with Existing Systems:**

  Compatibility Issues: Integrating machine learning solutions with existing distribution system components and cybersecurity infrastructure can be complex. Ensuring seamless integration without causing disruptions is crucial.

- **Resource Intensiveness:**

  Computational Resources: Some advanced machine learning models, especially those based on deep learning, can be computationally

intensive. Implementing these models in real-time systems may require significant computational resources.

IMPLEMENTATION

- The proposed algorithm consists of a decentralized system implemented by a multi-agent system (MAS), and a centralized system that performs network reconfiguration.
- A novel real-time decentralized mechanism for establishing coordination of attacks and predicting the targets of an attack is proposed.
- The proposed algorithm is hierarchical, enforcing a hybrid mitigation. A step-by-step summary is given in Fig. 1. The next sections detail the parts of the proposed algorithm.
- The proposed technique is also superior as it is not prone to single point failures; should the central agent be compromised, communication level mitigation is still enforced by the dispersed agents.

Advantages

- **Automation of Routine Tasks:** ML systems can automate routine security tasks such as data analysis, anomaly detection, and correlation, freeing up human resources for more complex decision-making.
- **Efficient Resource Allocation:** ML models help prioritize security incidents, allowing for efficient allocation of resources to address the most critical threats.
- **Customization and Adaptation:** ML models can be customized to the specific needs and characteristics of a distribution system, allowing for adaptability to the unique challenges of each environment.
- **Continuous Improvement:** ML systems can learn from new data and experiences, leading to continuous improvement in the accuracy and effectiveness of cyber threat detection and mitigation.

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Test & Train Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack

Status, View Cyber Attack Status Ratio, Download Predicted Data Sets, View Cyber Attack Status Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER ATTACK STATUS, VIEW YOUR PROFILE.

CONCLUSION

This paper presents a decentralized attack correlation technique and a hybrid mitigation. Compared to interdiction models in the literature, this work assumes no explicit knowledge of the attacker's parameters by the defenders, which in this case, are agents. The targets of an attack are predicted in a decentralized manner using a learning mechanism, and new NIDS thresholds optimally found from reinforcement learning are applied. When enough alerts are received, physical mitigation is triggered. The proposed technique is also superior as it is not prone to single point failures; should the central agent be compromised, communication level mitigation is still enforced by the dispersed agents. Currently, the NIDS implemented by the algorithm is anomaly-based and makes use of only communication level thresholds. It is therefore limited to only man-in-the-middle attacks. Future work may consider improving the mechanism of intrusion detection by integrating machine learning or another suitable method. Also, the inclusion of physical level checks in intrusion detection may prove useful for detecting insider attacks.

REFERENCES

[1] Electricity Information Sharing and Analysis Center (E-ISAC). (Mar. 2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC)*, [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/ documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[2] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641– 29659, 2021.

[3] A. Gusrialdi and Z. Qu, ‘‘Smart grid security: Attacks and defenses,’’ in *Smart Grid Control* (Power Electronics and Power Systems), 1st ed. Cham, Switzerland: Springer, 2018, pp. 199–223.

[4] R. Deng, P. Zhuang, and H. Liang, ‘‘False data injection attacks against state estimation in power distribution systems,’’ *IEEE Trans. Smart Grid*,vol. 10, no. 3, pp. 2871–2881, May 2019.

[5] S. Lakshminarayana, J. Ospina, and C. Konstantinou, ‘‘Load-altering attacks against power grids under COVID-19 low-inertia conditions,’’ *IEEE Open Access J. Power Energy*, vol. 9, pp. 226–240, 2022.

[6] I.-S. Choi, J. Hong, and T.-W. Kim, ‘‘Multi-agent based cyber attack detection and mitigation for distribution automation system,’’ *IEEE Access*, vol. 8, pp. 183495–183504, 2020.

[7] J. Appiah-Kubi and C.-C. Liu, ‘‘Decentralized intrusion prevention (DIP) against co-ordinated cyberattacks on distribution automation systems,’’ *IEEE Open Access J. Power Energy*, vol. 7, pp. 389–402, 2020.

[8] C. Moya and J. Wang, ‘‘Developing correlation indices to identify coordinated cyber-attacks on power grids,’’ *IET Cyber- Phys. Syst., Theory Appl.*, vol. 3, no. 4, pp. 178–186, Dec. 2018.

[9] Y. Lin and Z. Bie, ‘‘Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding,’’ *Appl. Energy*, vol. 210, pp. 1266–1279, Jan. 2018.

[10] K. Lai, M. Illindala, and K. Subramaniam, ‘‘A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyberphysical environment,’’ *Appl. Energy*, vol. 235, pp. 204–218, Feb. 2019.

[11] A. Abedi, M. R. Hesamzadeh, and F. Romerio, ‘‘An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system,’’ *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106455.

[12] A. L. Motto, J. M. Arroyo, and F. D. Galiana, ‘‘A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat,’’ *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[13] C. E. Shannon, ‘‘A mathematical theory of communication,’’ *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

[14] J. R. Quinlan, ‘‘Induction of decision trees,’’ *Mach. Learn.*, vol. 1, no. 1, pp. 81– 106, Mar. 1986.

[15] W. Wu, B. Li, L. Chen, C. Zhang, and P. S. Yu, ‘‘Improved consistent weighted sampling revisited,’’ *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 12, pp. 2332–2345, Dec. 2019.