International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 6 June 2023, pp: 659-662 www.ijaem.net ISSN: 2395-5252

Review on Temporal Correlation Algorithm to Detect a Cyber-attack in Optimal Power Flow by using Machine Learning

Mr. Swapnil N. Gulhane, Prof. T. N. Ghorsad

ME Final year CSE, Dr. Sau. K.G.I.E.T. Amravati, Maharashtra
Prof. Dr. Sau. K.G.I.E.T. Amravati, Maharashtra

Date of Submission: 14-06-2023 Date of Acceptance: 24-06-2023

ABSTRACT: The optimal operation of power systems is of paramount importance for maintaining grid stability and ensuring efficient electricity generation and distribution. However, with the increasing connectivity and reliance on digital infrastructure, power systems are susceptible to cyber-attacks that can disrupt normal operations and compromise system security. Therefore, developing effective cyber-attack detection mechanisms becomes crucial to safeguard the integrity of the power grid.

This research proposes a novel Temporal Correlation Algorithm (TCA) that leverages machine learning techniques to detect cyber-attacks in the context of Optimal Power Flow (OPF). The OPF is a fundamental optimization problem used in power systems to determine the optimal dispatch of power generation and control variables, such as voltage and reactive power, to minimize costs and maintain operational constraints.

KEYWORDS: TCA, Cyber Attack, Detection

I. INTRODUCTION

Critical infrastructure systems are of major importance to society, as they have a great impact on people's lives and the economy. Examples include the energy systems, telecom systems, and water supply. These Physical systems are operated by means of computers and applications using two-way communication capabilities and distributed intelligence to enhance effectiveness, trusty, and stability.Nevertheless, the strong interconnection between cyber and physical operations renders these systems highly susceptible to cyberattacks.Thus, these systems are susceptible to various cyber-physical attacks and, hence, need to be accompanied with appropriate security enforcements.

Over the past century, the electric grid has transformed from a collection of small, independent community-based systems into arguably the most extensive and intricate cyber-physical system on a global scale.The increasing demand for reliable energy has motivated the development of a smart electric grid. The smart grid is poised to enhance the existing capabilities of the generation, transmission, and distribution systems within the grid. It will establish an infrastructure that can effectively cater to the future demands of distributed generation, renewable energy sources, electric vehicles, and the efficient management of electricity from the demand side. The increasing reliance on cyber-infrastructure to manage highly complex smart grids comes with the risk of cyberattacks by adversaries around the globe. For example, the hacking of Ukrainian electrical power utilities in 2015 caused a sustained loss of electricity to roughly 80,000 customers. In addition, the cyber-attack on Pacific Gas & Electric's Metcalf substation in northern California caused more than $15 million in damage. Both of those attacks manipulated sensors to directly blind and disrupt the control centres. The successful functioning of complex cyber-physical systems depends on the reliable operation of a control loop that takes sensor data as input and produces control decisions as output.While certain attacks can be categorized as either cyber-attacks, such as hacking into a controller and redirecting power, or physical attacks, like damaging physical equipment, all significant attacks have invariably involved the manipulation of the operator control loop. This manipulation aims to conceal or magnify the impact of the attack. The operator control loop refers to the feedback loop through which operators evaluate the situation and make informed decisions.Through manipulation of this loop, even without directly causing physical damage, attackers can indirectly unleash widespread and devastating consequences, such as brown-outs, surges, and black-outs. The common thread among these attacks is the compromise of sensor data integrity. Notably, sensors are often the least fortified components, susceptible to cyber network access and challenging to fortify or physically safeguard. In the context of the smart grid, such sensors may encompass supervisory control and data acquisition (SCADA) sensors (e.g., bus voltage, line current, system frequency, real power, reactive power), phase measurement units (PMUs), or smart meters employed in advanced metering infrastructures (AMIs).

With the proliferation of sensors and the emergence of numerous low-cost sensor options, there is an increasing demand for a reliable method to establish trust in sensor data. This trust is crucial for operators to promptly respond to erroneous sensor data and prevent costly damages to the grid. Existing methods for detecting sensor data attacks were primarily developed for ensuring system reliability and offer limited effectiveness in countering cyber-physical attacks. These detection methods typically rely on out-of-range alerts that flag sensors exhibiting values significantly deviating from expected ranges. While such methods can identify blatant integrity attacks, more sophisticated integrity attacks can remain undetected within the expected range, evading system alerts. One attack, known as a replay attack, involves the manipulation of sensor signals by replaying previously recorded signals from the same sensor, further complicating detection efforts. AsConsequently, these sensors inherently produce readings that lie within an acceptable range, thereby avoiding triggering any alerts.To enhance the detection of integrity attacks under various operating conditions, a novel approach involving multiple sensors is necessary. Recent advancements in attack detection mechanisms for smart grids have addressed this need. These studies have demonstrated that by leveraging knowledge about the power network's topology, sophisticated data-injection attacks can evade current SCADA system's bad data detection schemes. In response, algorithms have been proposed to incorporate encrypted devices within the system, effectively increasing the security index against such attacks. Furthermore, a computationally efficient algorithm has been developed to detect and pinpoint attacks using the generalized likelihood ratio test. Additionally, a graph theoretic approach has been introduced to identify data integrity cyberattacks, utilizing secure PMUs as countermeasures against a range of potential cyberattacks.An innovative approach utilizing deep learning is presented for the detection of data integrity cyberattacks. This approach considers time-varying network topologies by leveraging real-time data from PMUs and smart meters, enabling the real-time security assessment of large-scale emerging energy systems. Furthermore, the trade-off between detection speed and performance has been explored in previous research. However, most of the mentioned approaches neglect the incorporation of the physical laws governing the electric grid, making them unsuitable for real-time implementation. In a physical system, sensors provide information based on activities governed by the unchangeable laws of physics. For instance, current and voltage differences are directly proportional, with the constant of proportionality determined by the line's resistance, often unknown. More intricate physical systems like power grids have more complex underlying laws. As additional sensor readings are collected, a greater number of dependencies become observable. By inferring the governing laws of the sensors, any deviations from these laws can indicate data integrity failures.In this paper, we propose a cyber-physical attack detection (CPAD) mechanism for false data that automatically infers underlying physical relationships analytics to detect sensor failures, replay attacks, and other data integrity issues within smart grids in real-time. It focuses on inferring and exploiting the underlying physics of the system in order to quickly identify sensor measurements that, although they may appear reasonable in isolation, are implausible when viewed in a larger context.

The experimental results demonstrated that the proposed CPAD (Cyber-Physical Attack Detector) achieved an impressive 99% accuracy in detecting replay attacks. Notably, our findings revealed that the most effective approach was not to create physics-based features based on prior knowledge of the system, but rather to utilize a neural network (NN) to autonomously learn the underlying laws. Subsequently, the outputs of the NN were employed to construct a classifier capable of identifying instances and locations of data spoofing. Thus, it is preferable to leverage a unified machine learning solution that infers and exploits the physics, rather than initially incorporating features and subsequently building a detector using machine learning techniques. By effectively capturing temporal correlations within power system data, the TCA (Temporal Correlation Analysis) algorithm offers an efficient and accurate method for detecting cyber-attacks. The integration of machine learning techniques into power system security is of utmost importance to ensure the resilience and reliability of modern power grids amidst evolving cyber threats.

II. SYSTEM MODEL

Algorithm:

Given an input list, L, comprising potential storms obtained from a spatial search output, along with specified parameters such as the maximum storm travel speed, U-max, and the minimum duration, min, as well as other storm identification criteria, typically temporal in nature, the algorithm aims to process this information effectively.

```
Output: List T of storm tracks
set T = empty list
NT = total number of time steps in data set
for i = 1 to NT do
    for all elements li ∈ L at time step i do
        start new track t at li
        continue = True
        j = i
        while continue do
            examine all lj+1 ∈ L at time step j + 1 for possible successors to storm lj
            if successor found then
                add lj+1 to track t
                j = j + 1
            else
                continue = False
            end if
        end while
        if track t meets or exceeds identification criteria then
            add t to T
        end if
    end for
end for
```

The given algorithm aims to identify and track storms based on a spatial search output. It begins by initializing an empty list called T, which will store the resulting storm tracks. The algorithm then proceeds to iterate over each time step in the dataset, starting from the first-time step.

At each time step, the algorithm examines the elements in the list L, which represents potential storms. For each element at time step i, a new track t is created, starting with the current storm. The algorithm sets a Boolean variable called "continue" to True, indicating that the track can still be extended.

Next, the algorithm enters a while loop, continuing as long as the variable "continue" remains True. Within the loop, the algorithm examines all elements lj+1 at the next time step (j + 1) to find possible successors to the current storm lj. If a successor storm is found, it is added to the track t, and the time step j is incremented by 1 to consider the next time step. This process continues until no successor storm is found, at which point the variable "continue" is set to False, and the while loop is exited.

Once the while loop concludes, the algorithm checks if the track t meets or exceeds the specified identification criteria. If it does, the track is considered valid and is added to the list T, which stores the storm tracks.

After iterating over all time steps and examining all potential storms, the algorithm concludes, and the resulting list T contains the identified storm tracks that satisfy the identification criteria.

In summary, the algorithm iteratively builds storm tracks by considering potential successor storms at each time step. It tracks storms until no further successors are found, and the resulting tracks are stored based on meeting the identification criteria. This approach allows for the identification and tracking of storms based on their spatial and temporal characteristics.

III. CONCLUSION

To summarize, the Temporal Correlation Algorithm proves to be a valuable solution for detecting cyber-attacks in Optimal Power Flow (OPF) scenarios through the utilization of Machine Learning techniques. By harnessing the temporal correlation patterns present in power system data, this algorithm effectively identifies anomalies that may signify a potential cyber-attack.

The algorithm leverages Machine Learning to effectively learn from historical data and recognize patterns that deviate from the normal behaviour of the system. This empowers the algorithm to differentiate between regular fluctuations and suspicious activities that could potentially signify a cyber-attack. Moreover, the algorithm's capability to analyze data over an extended period enables it to detect subtle changes or abnormal behaviours that might not be evident in isolated snapshots.

The Temporal Correlation Algorithm offers several notable advantages, including its capacity for real-time detection, adaptability to evolving attack strategies, and ability to handle substantial data volumes. Its integration with Optimal Power Flow (OPF), a crucial power system optimization problem, enables efficient detection and response to cyber threats while maintaining the reliable and secure operation of the power grid.

REFERENCES

[1]. H. Karimipour and V. Dinavahi, “Robust massively parallel dynamic state estimation of power systems against cyber-attack,” IEEE Access, vol. 6, pp. 2984–2995, 2018.

[2]. H. Karimipour and V. Dinavahi, “Parallel domain-decomposition-based distributed state estimation for large-scale power systems,” IEEE Transactions on Industry Applications, vol. 52, no. 2, pp. 1265–1269, March 2016.

[3]. H. Karimipour and V. Dinavahi, “On false data injection attack against dynamic state estimation on smart power grids,” in 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Aug 2017, pp. 388–393.

[4]. P. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, “Detection of false data injection attacks in smart-grid systems,” IEEE Communications Magazine, vol. 53, no. 2, pp. 206–213, Feb 2015.

[5]. M. Esmalifalak, R. Zheng, and Z. Han, “Detecting stealthy false data injection using machine learning in smart grid,” in 2013 IEEE Global Communications Conference (GLOBECOM), Dec 2013, pp. 808–813.

[6]. S.Mohammadi, V. Desai, and H. Karimipour, “Multivariate mutual information-based feature selection for cyber intrusion detection,” 10 2018, pp. 1–6.