INL/CON-23-72952-Revision-0

AI-based Detection and Defense Against Cyberattacks in Distributed Energy Resources

October 2023

Palash Kumar Bhowmik, Syed Alam, Sajedul Talukder, Piyush Sabharwall

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-72952-Revision-0

AI-based Detection and Defense Against Cyberattacks in Distributed Energy Resources

Palash Kumar Bhowmik, Syed Alam, Sajedul Talukder, Piyush Sabharwall

October 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

AI-based Detection and Defense Against Cyberattacks in Distributed Energy Resources

Palash Kumar Bhowmik
Irradiation Experiment and Thermal Hydraulics Analysis
Idaho National Laboratory
Idaho Falls, USA
palashkumar.bhowmik@inl.gov

Syed Alam
Nuclear Engineering and Radiation Science
Missouri University of Science and Technology
Rolla, USA
alams@mst.edu

Sajedul Talukder
Computer Science
University of Alabama at Birmingham, USA
stalukder@uab.edu

Piyush Sabharwall
Irradiation Experiment and Thermal Hydraulics Analysis
Idaho National Laboratory
Idaho Falls, USA
piyush.sabharwall@inl.gov

***Abstract*—This study will provide comprehensive artificial intelligence (AI)-based solution tools for network security, malware prevention, and sensor data anomaly detection for distributed energy resource (DER) research, development, and demonstration. DER technologies are energy systems (e.g., solar panels, wind turbines, and energy storage systems) that are often connected to the internet and thus vulnerable to cyberattacks. Cybersecurity should be of primary concern for DERs, which is why we propose an integrated multi-layer cyber-defense system for DERs. This system encompasses risk assessments, network security, malware prevention, and detection of anomalies in the sensor data. Implementation of a comprehensive risk assessment with an overview of the model architecture should be the primary step, and should include the potential impact of experiencing, at a given time, one or more cyberattacks on the system. The second step is to ensure that the network security includes firewalls, intrusion detection, and malware prevention. The third step is to provide solution tools that enable sensor data anomaly detection for DERs. By incorporating these considerations into DER research, development, and demonstration, organizations can help ensure the safety and security of their systems and protect against potential cyberattacks.**

Keywords—Intelligence Interaction, Systems Safety and Security, Networking and Decision-Making

I. INTRODUCTION

Distributed energy resources (DERs) are small-scale power generation units (often renewable) located close to the point of consumption. DER types include solar panels, wind turbines, and battery storage systems. DERs are becoming increasingly important in modern energy systems, due to their ability to provide flexible, sustainable energy solutions. These resources are often integrated with communication networks and control systems to enable remote monitoring/control. While such connectivity provides many benefits, it also creates new vulnerabilities to cyberattacks. Cyberattacks on DERs can compromise the confidentiality, integrity, and availability of sensitive data, leading to severe consequences such as system failure, data theft, and unauthorized access. This project explores potential cyberattack threats to DERs and offers recommendations for securing these systems.

II. CYBERATTACKS ON DERS

Cyberattacks on DERs take various forms, including malware attacks, denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, spoofing attacks, and physical attacks [1]. These cyber-attacks needs to be adequately characterized to prepare appropriate defense system to ensure secured operation and control of DERs system.

A. Types of Cyberattacks

Malware attacks involve injecting malicious code into DER control systems so as to take control or steal sensitive data [2]. DoS attacks entail flooding the DERs with requests in order to make them unresponsive, potentially leading to disruption of the power supply. Physical attacks on DERs can involve tampering with equipment or stealing components, potentially leading to disruption of power supply or the damaging of critical infrastructure. The impact of cyberattacks on DERs can be severe. Besides disrupting the power supply and damaging critical infrastructure, cyberattacks can lead to the theft of sensitive data and the loss of revenue for energy providers. Cyberattacks on DERs can also have a cascading effect, as disruptions to one DER can cause disruptions in other parts of the grid. In some cases, cyberattacks on DERs can cause physical harm to people or equipment. For example, a cyberattack on an electric vehicle charging station could cause a fire or explosion.

B. Proposed Cyberattack Defense System

In the proposed study, we plan to develop an integrated multi-layer DER cyber-defense system that encompasses risk assessments, network security, malware prevention, and detection of anomalies in the sensor data (see Fig. 1). DER system operators are burdened with numerous responsibilities, causing them to adopt reactive monitoring approaches (i.e., responding to alarms and events). Proactive monitoring, however, is essential for early detection and mitigation of anomalies in the sensor data, and implementing proactive strategies can help avoid potential safety hazards and economic consequences. This makes transitioning to proactive monitoring crucial for enhancing plant safety and efficiency. Furthermore, the proposed research supports integrating the existing process data from DERs so as to achieve cost-effective, fast-to-deploy, system-level-to-component-level sensor data anomaly detection, thereby enabling the prediction of catastrophic failures and supporting safe, flexible operation via preventive maintenance.

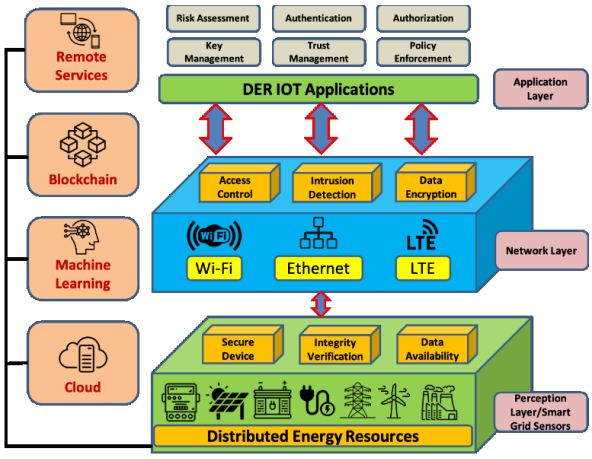

Fig. 1: High-level schematic of the proposed integrated multi-layer cyber-defense system for DERs.

C. *Proposed System Control Strategies*

DER system control strategies—whether categorized as active or passive—are designed for enabling quick responses to changes in operating conditions, thereby ensuring system safety and stability. Passive safety systems rely on natural phenomena (e.g., gravity or free convection) to provide safety functions, and their response times are typically on the order of seconds to minutes. Active safety systems, however, use powered components such as pumps, motors, or control rods, and offer faster response times (on the order of milliseconds [for digital control systems] to seconds [for mechanical systems such as control rod movement]). Therefore, it is pivotal to develop real-time sensor data prediction and control algorithms that align with system response times. During a cyberattack, the sensor and control system will respond accordingly, requiring detection and defense within a timeframe of anywhere from 1 millisecond to a manner of seconds

III. Technical Approach to the Solution

Secure monitoring of various aspects of DERs requires safe, reliable communications among sensors, control panels, and various human-system interfaces. The attack scenario will consider various commonly used networking technologies such as Wi-Fi, Ethernet, HART, WirelessHART, Zigbee, LoRaWAN, and cellular networks (4G-LTE or 5G). With these technologies, several potential cyberattack threats to DERs can occur at different levels (e.g., within the physical, data link, network, and application layers). This proposed multilayer system will help enhance cyber-defense against targeted attacks.

A. *Cybersecurity Solutions*

This task will be directed toward reducing the cybersecurity risks faced by DERs. Technically, the biggest security risk to DERs is its users, who unwillingly allow unauthorized access to hackers. In addition, vulnerabilities in the software employed, as well as in portable devices, pose a similarly big threat to DER networks. Under this task, we will explore robust solutions to address network vulnerabilities to such things as DoS, MITM, and spoofing attacks, as well as to human vulnerabilities such as targeted ransomware, spear phishing, social engineering, and insider threats. Particular focus will be placed on AI-based solutions coupled with permissioned blockchain and privacy-preserving mechanisms that prevent attacks at their earliest stages [3] by distilling complex chains of unusual behavior into digestible reports easily understood by people with varying levels of familiarity with information technology and operational technologies. To protect DERs from cyberattacks, several measures should be put into place, including (a) network segmentation, (b) authentication and access control, (c) securing of communication channels, (d) patch management, (e) monitoring and detection, and (f) physical security systems.

B. *Sensor Data Anomaly Detection*

For enhanced safety and efficiency, DER system operators must transition from reactive to proactive monitoring. Active and passive DER safety systems must be able to respond quickly to changing conditions. Real-time sensor data prediction and control algorithms are crucial, especially during cyberattacks. The proposed research aims to integrate process data (i.e., time series data from a real-time system) in order to enable a cost-effective, fast-to-deploy anomaly prediction system. This study will utilize previously developed explainable and interpretable predictive ML/AI models (see Fig. 2, which illustrates the physics corrector module and data-driven methods) [5].

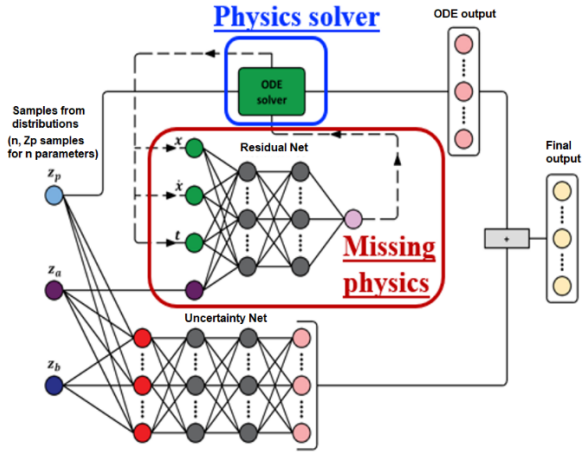

Fig. 2: AI model with physics corrector module [4].

References:

[1] S. Talukder, M. I. I. Sakib, M. F. Hossen, Z. R. Talukder, M. S. Hossain, "Attacks and Defenses in Mobile IP: Modeling with Stochastic Game Petri Net," In proceedings of the IEEE International Conference on Current Trends in Computer, Electrical, Electronics and Communication, September 2017.

[2] S. Talukder, Z. Talukder, "A Survey on Malware Detection and Analysis Tools," International Journal of Network Security & Its Applications (IJNSA), Vol. 12, No. 2, March 2020.

[3] A. Shahid, N. Pissinou, S. Talukder, "Protecting Location Privacy in Blockchain-based Mobile Internet of Things," Book Chapter in Principles and Practice of Blockchains, Springer Nature, Switzerland, 2022.

[4] S. Garg, S. Chakraborty, B. Hazra, "Physics-integrated hybrid framework for model form error identification in nonlinear dynamical systems," Sep. 2021. doi: 10.1016/j.ymssp.2022.109039.