IJMRSET

MULTIDISCIPLINARY · SCIENCE · ENGINEERING · TECHNOLOGY

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 5, May 2023

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

A Machine Learning Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids

Mrs. K. Sudha Devi[1], M. Praveena[2]

Associate professor, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India[1]

M.E CSE IInd Year, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India [2]

ABSTRACT : Because they are more susceptible to a variety of cyber attacks, cyber-physical systems (cpss) play a crucial role in power system security today. Due to the increasing use of direct current micro grids (dc-mgs) in a variety of electrical engineering applications, such as the generation of renewable power and the distribution of electricity, power system of public transportation, and subway electric network, detection of cyber attacks on dc-mgs has become a crucial issue. In order to improve the cyber-security of electrical systems, a novel method for diagnosing potential false data injection attacks (fdia) in dc-mgs was presented in this study. Consequently, a novel wavelet transform (wt) and singular value decomposition (svd) method based on deep machine learning was proposed to diagnose cyber attacks in dc-mg and identify the fdia to der unit. Furthermore, this paper presents a created specific troupe profound learning (dl) move toward utilizing the dark wolf streamlining (gwo) calculation to distinguish the fdia in dc-mg. A dc-mg was operated and controlled without fdias in the paper's first stage to gather sufficient data within normal performance for the dl network's training. The diagnosis datasets for cyber-attack and load variation schemes were considered to have load changing in the information generation process.

KEYWORDS: resent, cyber attacks, direct current micro grid (dc-mg), and false data injection attacks

I. INTRODUCTION

(SIs) with advanced cyber-infrastructure, a novel method for diagnosing potential false data injection attacks (FDIA) in DC-MGs was presented in this study. Since SIs with advanced cyber-infrastructure are extremely susceptible to cyber-attacks, greater attention must be paid to their cyber-security. By manipulating measurements, false data injection attacks (FDIAs) can result in SE solutions that are incorrect or affect the performance of the central control system. There is plausible that ordinary assault identification strategies don't distinguish numerous digital assaults; Consequently, system operation may impede. Cyber attacks that target DC-SE are the primary focus of research; however, because Smart-Islands (SIs) with advanced cyber-infrastructure are extremely vulnerable to cyber-attacks, increasing attention must be paid to their cyber-security due to the increased use of AC SIs. Misleading information infusion assaults (FDIAs) by controlling estimations might cause wrong state assessment (SE) arrangements or impede the focal control framework execution. There is a possibility that traditional methods of attack detection do not catch many cyber attacks; consequently, system operation may impede. Cyber attacks that target DC-SE are the primary focus of research; However, cyber-attack detection in AC systems is becoming increasingly important as AC SIs become more widely used. In this regard, this paper proposes a novel signal processing-based method for detecting the injection of any false data into AC-SE. The temporal and spatial data correlations of the state vectors may deviate from their normal operation in response to malicious data injection. The proposed recognition technique depends on breaking down transiently successive framework states by means of wavelet particular entropy (WSE). In this technique, to change particular worth frameworks and wavelet changes' definite coefficients, exchanging surface in light of sliding mode regulator are deteriorated; The expected entropy values are then calculated using the stochastic process. For the purpose of detecting cyberattacks, indicators are characterized by the WSE in terms of switching level of current and voltage. In order to identify cyberattacks involving a variety of false data injections, including amplitude and vector deviation signals, the proposed detection strategy is utilized in a number of case studies. The simulation results confirm the proposed FDIA detection method's high performance. This location technique's critical trademark is its capacity in quick identification (10 ms from the assault commencement); In addition, the accuracy that this method can achieve is greater than 96.5 percent.

From one perspective, these innovations carry imperativeness to the power framework by upgrading framework dependability, empowering quicker controls, and working with far reaching association of dispersed energy assets (DERs). Power systems, on the other hand, are susceptible to cyber attacks because they are heavily dependent on information and communications technologies. By and by, digital assaults related with DC MICROGRIDS estimations can be ordered into six sorts refusal of-administration assault, actual assault, Man-in-the-center (MITM) assault, bundle examination, vindictive code infusion, and information mocking. Data spoofing and MITM both fall under the category of data integrity attacks. This paper's main concern is also the vulnerability of telemetered data, such as power injections, line flows, voltage measurements from DC microgrids, and breaker and switch status information.

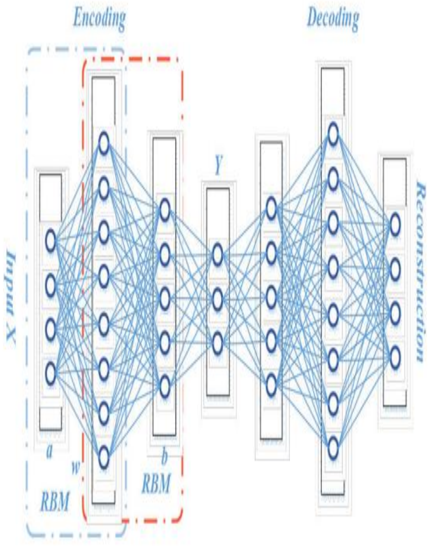
In circumstances where the principal lattice and power usage are far separated, as far off islands and isolated correspondence stop, it isn't financially productive or is essentially difficult to supply power by transmission lines. In such instances, it is best to use a microgrid (MG) that incorporates renewable energy resources like wind turbines, photovoltaic, and fuel cells to provide power in the islanding mode. The MG distributed generation units are in charge of voltage, frequency, and current control, fault protection, and cyber-attack detection in such a smart island (SI). In an islanding, SI is an effective method for combining renewable energy resources, storage devices, and new electronic loads that can operate independently of the utility grid. Additionally, the nature of the operating units at AC paradigm led to a brilliant performance boost. In addition, the distributed control philosophy is a cost-effective option because it can easily accommodate a lower volume of data transformation without requiring a significant amount of traffic to counteract the intensive communication.

II. PRE-TRAINING OF THE DAE

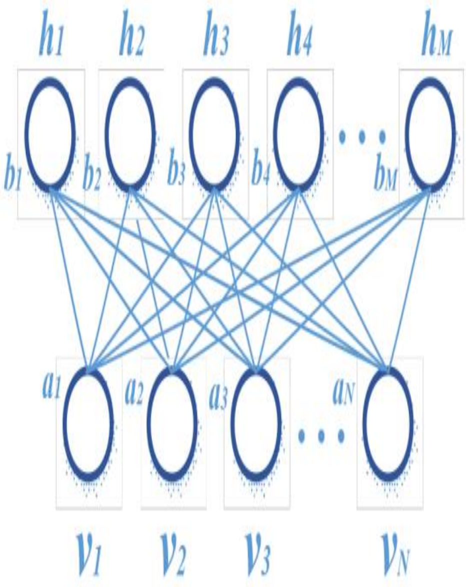
Diverse RBM stacks make up the DAE, a deep learning network. In order to transmit learning outcomes layer by layer, the DAE treats each RBM output as a new input to a higher level RBM. In order to set the parameters, multiple copies of each hidden layer are used. Encoding and decoding are the two steps in the DAE network's construction. The input X is first converted in the encoding function to build a series of details for subsequent layer-by-layer conversions, and the intricate details are added in higher layers. Ultimately, the code Y is gotten by the encoding capability.

In a similar fashion, the decoding function produces the renovation of X, X, and iteratively returns the code Y to the primary input. The mechanisms for encoding and decoding, as depicted in Fig. 3, a random Markov type two-layer network with N visible modules vi = 0, 1 N and M hidden modules hj = 0, 1 M is present in the RBM. However, the RBM presents the energy pattern to the related energy of the common Structure modules.

DAE NETWORK FRAMEWORK



RBM FRAMEWORK



III. RELATED WORK

Because they are limited-scope power frameworks that are independent and controllable, micro grids can be used in both network-associated and islanded activities. They also play a significant role in increasing the versatility of basic power foundations. There are two primary types of microgrids: AC and DC. DC micro grids have recently received a lot of attention due to their flexibility for integrating DC nature power sources (like photovoltaic and battery energy storage systems) and their improved power delivery efficiency in comparison to AC micro grids.

Similar to AC micro grids, DC micro grids employ a hierarchical control structure with primary, secondary, and tertiary control levels. Primary control typically makes use of local droop controllers on DERs to maintain the stability of the micro grid voltage following islanding. The DC micro grid voltage guideline is uniquely managed by the auxiliary control after the essential control takes action, resulting in a slight drop in the micro grid voltage level. Tertiary control controls the optimal operation of the micro grid and the power flow between it and the upstream grid in the grid-connected mode. Legitimate voltage guideline while fulfilling the corresponding power dividing between DERs is of central significance as one of the essential control goals in DC miniature networks.

IV. PROPOSED SYSTEM

Based on the historical DC MICROGRIDS data obtained from both ends of the line, we propose a method to recover the missing or abnormal amplitude data in DC MICROGRIDS measurements (i.e. the active power, reactive power, positive sequence current, and voltage amplitude), which is independent of the transmission line parameters and the phase angle that may be influenced by synchronization in the proposed system.

The recovery method, which recovers the voltage amplitude, active power, reactive power, and current amplitude in order by utilizing historical amplitude data to calculate related recovery coefficients, is proposed after the model of data recovery has been established.

ADVANTAGES

These kinds of attacks can be carried out by adding a minor constant or a slope to the original data packet. This method is efficient and requires the least amount of effort from the attacker's perspective.

From a security standpoint, such attacks can cause the grid control/dispatch center to issue harmful commands by tampering with the measurement data of the power system and disrupting the normal dispatching operation of the power system.

V. SYSTEM ARCHITECTURE

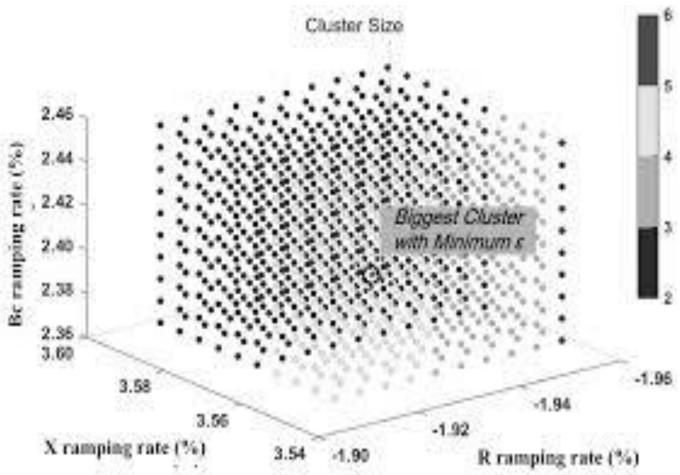


Fig.1.1 System Architecture

IMPLEMENTATION

The project's implementation phase is where the theoretical design becomes a functional system. This is the last and significant stage in the framework life cycle It is really the most common way of changing over the new framework into a functional one.

TESTING

The project's implementation phase is where the theoretical design becomes a functional system. This is the last and significant stage in the framework life cycle It is really the most common way of changing over the new framework into a functional one.

UNIT TESTING

The set of tests performed by a single programmer prior to the unit's integration into a larger system is known as unit testing. Tests are performed on the module interface to guarantee that data properly enters and exits the program unit. The local data structure is looked at to make sure that temporarily stored data stays the same at every step of an algorithm's execution. The module is tested under boundary conditions to ensure that it functions properly within limits imposed to limit or restrict processing.

BLOCK BOX TESTING

Black-box testing is a method of software testing that looks at an application's functionality without looking inside to see how it works or how it was built. Virtually every level of software testing can be tested using this method.

VI. CONCLUSION

A novel framework for the detection, identification, and data recovery of data integrity attacks against DC MICROGRIDS measurements is presented in this paper. Contrasted with existing methodologies, the proposed one has four significant benefits: 1) capable of providing bad data recovery solutions that maintain the data consistency, 2) effective for simultaneous attacks on multiple channels, 3) sensitive and robust to small attacking signals, which are difficult to detect with existing bad data detection methods, and 4) independent of system topological changes and therefore adaptive and effective for changing system configurations. As a result, the proposed framework can be used in a wide range of situations.

REFERENCES

[1]C. Beasley, X. Zhong, J. Deng, etc., “A Survey of Electric Power Synchrophasor Network Cyber Security,” 5th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Istanbul, Turkey, 2014.

[2]K. Chatterjee, V. Padmini and S. A. Khaparde, “Review of Cyber Attacks on Power System Operations,”2017 IEEE Region 10 Symposium (TENSYMP), Cochin, 2017, pp. 1-6.

[3]A. Abur, and A. G. Exposito, Power System State Estimation: Theory and Implementation. CRC Press, 2004.

[4]Y. Liu, P. Ning, and M. Reiter, “False Data Injection Attacks against State Estimation in Electric Power Grids,” ACM Transactions on Information and System Security, vol. 14, no. 1, Article 13, May 2011.

[5]J. Chen, and A. Abur, “Placement of DC MICROGRIDSs to Enable Bad Data Detection in State Estimation,” IEEE Trans. Power Syst., vol. 21, no. 4, pp. 1608–1615, Nov. 2006.

[6]G. B. Denegri, M. Invernizzi, and F. Milano, “A Security Oriented Approach to DC MICROGRIDS Positioning for Advanced Monitoring of a Transmission Grid,” Inter. Conf. Power System Technology, vol. 2, pp. 798-803, 2002.

[7]Q. Yang, D. An, etc., “On Optimal DC MICROGRIDS Placement-based Defense against Data Integrity Attacks in Smart Grid,” IEEE Trans. Information Forensics and Security, vol. 12, no. 7, July 2017.

[8]G. Dan, and H. Sandberg, “Stealth Attacks and Protection Schemes for State Estimators in Power Systems,” in Proc. IEEE Int. Conf. Smart Grid Commun., pp. 214–219, 2010.

[9]M. Jamei, E. Stewart, etc., “Micro Synchrophasor-based Intrusion Detection in Automated Distribution Systems: Toward Critical Infrastructure Security,” IEEE Internet Computing, vol. 20, no. 5, pp. 18-27, Oct. 2016.

[10]A. Mazloomzadeh, O. A. Mohammed, and S. Zonouzsaman, “Empirical Development of a Trusted Sensing Base for Power System Infrastructures,” IEEE Trans. Smart Grid, vol. 7, no. 5, Sep. 2015.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com