JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ADAPTIVE HIERARCHICAL CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE DISTRIBUTION SYSTEMS

(1) Mrs.Dr.SARADA

Associateprofessor

DepartmentofComputer Applications

Chadalwada ramanamma engineering colleage (Autonomous)

(2)Y.HEMALATHA

Student

D epartment of Computer Applications

chadalawadaramanamma engineering colleage

(Autonomous),Tirupati

Abstract:

Development of a cyber security strategy for the active distribution systems is challenging due to the inclusion of distributed renewable energy generations. This paper proposes an adaptive hierarchical cyber attack detection and localization framework for distributed active distribution systems via analyzing electrical waveforms. Cyber attack detection is based on a sequential deep learning model, via which even minor cyber attacks can be identified. The two-stage cyber attack localization algorithm first estimates the cyber attack sub-region, and then localize the specified cyber attack within the estimated sub-region. We propose a modified spectral clustering-based network partitioning method for the hierarchical cyber attack 'coarse' localization. Next, to further narrow down the cyber attack location, a normalized impact score based on waveform statistical metrics is proposed to obtain a 'fine' cyber attack location by characterizing different waveform properties. Finally, compared with classical and state-of-art methods, a comprehensive quantitative evaluation with two case studies shows promising estimation results of the proposed framework.

Keywords

Cyberattack Location awareness,Sensors,Adaptive systems,Adaptation models,Topology,Monitoring

1 .INTRODUCTION

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 cyber-device in fault or under attack will cause unusual 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 power grids 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 real-time

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. Rule-based data-driven analytics [23], signal property-based 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;

The remainder of this paper is organized as follows. In Section II, the cyber attack model of active distribution systems is discussed. In Section III, we describe the proposed approaches with the details of each key component, which are cyber attack detection, network partition and cyber attack localization. Experiments and evaluations can be found in Section IV. In the end, a conclusion is drawn in Section V.

2. LITERATURE SURVEY

2.1 DIFFERENT AUTHORS

Data-driven methods have been widely adopted for event localization in power electronics networks and active distribution systems. Rule-based data-driven analytics [23], signal property-based 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

2.2 DOMAIN DESCRIPTION

We propose a modified spectral clustering-based network partitioning method for the hierarchical cyber attack ‘coarse’ localization. Next, to further narrow down the cyber attack location, a normalized impact score based on waveform statistical metrics is proposed to obtain a ‘fine’ cyber attack location by characterizing different waveform properties. Finally, compared with classical and state-of-art methods, a comprehensive quantitative evaluation with two case studies shows promising estimation results of the proposed framework.

3. EXISTING SYSTEM

3.1 EXISTING SYSTEM:

Cyber and physical attacks threaten the security of distribution power grids. The emerging renewable energy sources such as photovoltaics (PVs)

introduce new potential vulnerabilities. Based on the electric waveform data measured by waveform sensors in the distribution power networks, in this article, an existing system develops a novel high-dimensional data-driven cyber physical attack detection and identification (HCADI) approach.

First, we analyze the cyber and physical attack impacts (including cyber attacks on the solar inverter causing unusual harmonics) on electric waveforms in the distribution power grids. Then, we construct a high-dimensional streaming data feature matrix based on signal analysis of multiple sensors in the network. Next, we propose a novel mechanism including leverage score-based attack detection and binary matrix factorization-based attack diagnosis. By leveraging the data structure and binary coding, our HCADI approach does not need the training stage for both detection and the root cause diagnosis, which is needed for machine learning/deep learning-based methods. To the best of our knowledge, it is the first attempt to use raw electrical waveform data to detect and identify the power electronics cyber/physical attacks in distribution power grids with PVs.

3.2 DISADVANTAGE OF EXISTINTG SYSTEM:

The system is not implemented Network Partition based on Modified Spectral Clustering. The system is not implemented Cyber Attack Localization within Sub-regions.

4.PROPOSED SYSTEM

4.1 PROPOSED SYSTEM:

The system proposes 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.

4.2 ADVANTAGE OF PROPOSED SYSTEM:

In the proposed system, the cyber attack can be detected based on the deviation of the monitoring metrics from steady-state, which, in our study, is an anomaly detection problem. To efficiently locate the cyber attacks, the system proposes to first partition the active distribution systems into several subregions.

5.MODULE DISCRIPTION

5.1 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 Login, Train & Test Cyber Data Sets, View Cyber Datasets Trained Accuracy in Bar Chart, View Cyber Datasets Trained Accuracy Results, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Datasets, View Cyber Attack Type Ratio Results, View All Remote Users.

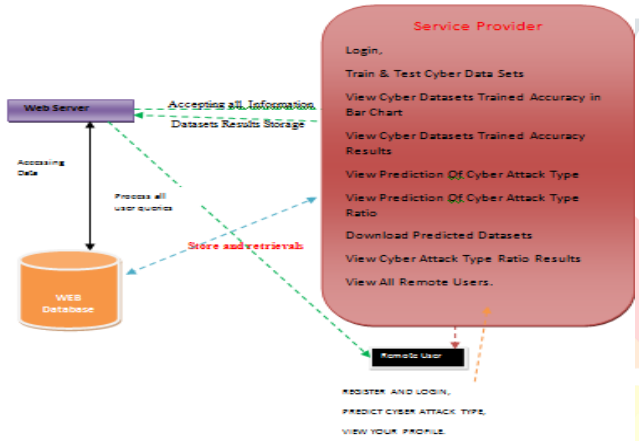
5.2 View and Authorize Users

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.

5.3 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 TYPE, VIEW YOUR PROFILE.

6. SYSTEM ARCHITECTURE:



7.CONCLUSION

In this paper, we proposed an adaptive hierarchical cyber attack localization approach for active distribution systems. Electric waveform signals obtained by WMU sensors are used to capture the abnormal features, which would be otherwise ignored. To improve the efficiency, we propose a modified spectral clustering method to first partition the whole large network into smaller 'coarse' sub-regions. Next, the accurate 'fine' cyber attack location can be determined by calculating and analyzing Impact Score of each sensor in the potential sub-region. Furthermore, we compare our method with other methods in each step in cyber attack detection, sub-graph clustering, and localization, respectively. The results from two representative distribution grids show that our method shows promising performances.

8.FUTURE ENHANCEMENT

Extensive experiments are utilized to evaluate the proposed approach performances with quantitative analytics

9.REFERENCES

I. Džafi´c, R. A. Jabr, S. Henselmeyer, and T. Đonlagi´c, "Fault location in distribution networks through graph marking," Transactions on Smart Grid, vol. 9, no. 2, pp. 1345–1353, 2016.

R. Bhargav, B. R. Bhalja, and C. P. Gupta, "Novel fault detection and localization algorithm for low voltage dc microgrid," Transactions on Industrial Informatics, 2019.

G. Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," Transactions on Automatic Control, vol. 65, no. 9, pp. 3919–3926, 2020.

F. Li, Y. Shi, A. Shinde, J. Ye, and W.-Z. Song, "Enhanced cyberphysical security in internet of things through energy auditing," Internet of Things Journal, vol. 6, no. 3, pp. 5224–5231, 2019.

A. J. Wilson, D. R. Reising, R. W. Hay, R. C. Johnson, A. A. Karrar, and T. D. Loveless, "Automated identification of electrical disturbance waveforms within an operational smart power grid," Transactions on Smart Grid, vol. 11, no. 5, pp. 4380–4389, 2020.

P. Dutta, A. Esmaeilian, and M. Kezunovic, "Transmission-line fault analysis using synchronized sampling," transactions on power delivery, vol. 29, no. 2, pp. 942–950, 2014.

I. Sadeghkhani, M. E. H. Golshan, A. Mehrizi-Sani, J. M. Guerrero, and A. Ketabi, "Transient monitoring function–based fault detection for inverter-interfaced microgrids," Transactions on Smart Grid, vol. 9, no. 3, pp. 2097–2107, 2016.

A. F. Bastos, S. Santoso, W. Freitas, and W. Xu, "Synchrowaveform measurement units and applications," in 2019 Power & Energy Society General Meeting (PESGM)., 2019, pp. 1–5.

Schweitzer Engineering Laboratories, Pullman, WA, USA., "SEL-T400L Time Domain Line Protection," https://selinc.com/ products/T400L/, Last Access: July 31, 2020.

Candura instruments, Oakville, ON, Canada., "iPSR intelligent Power System Recorder," https://www.candura.com/ products/ipsr.html, Last Access: July 31, 2020.

D. Borkowski, A. Wetula, and A. Bie´n, "Contactless measurement of substation busbars voltages and waveforms reconstruction using electric field sensors and artificial neural network," Transactions on Smart Grid, vol. 6, no. 3, pp. 1560–1569, 2014.

B. Gao, R. Torquato, W. Xu, and W. Freitas, "Waveform-based method for fast and accurate identification of subsynchronous resonance events," Transactions on Power Systems, vol. 34, no. 5, pp. 3626–3636, 2019.

F. Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Song, "Online distributed iot security monitoring with multidimensional streaming big data," Internet of Things Journal, vol. 7, no. 5, pp. 4387–4394, 2020.

F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W.-Z. Song, "System statistics learning-based iot security: Feasibility and suitability," Internet of Things Journal, vol. 6, no. 4, pp. 6396–6403, 2019. [15] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," Transactions on Power Electronics, vol. 36, no. 3, pp. 2495–2498, 2021.

A. Wang and J. Shi, "Holistic modeling and analysis of multistage manufacturing processes with sparse effective inputs and mixed profile outputs," IISE Transactions, vol. 53, no. 5, pp. 582–596, 2021.

J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639–4657, 2021.

F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," Journal of Emerging and Selected Topics in Power Electronics, Early Access.

J. Zhang, S. Sahoo, J. C.-H. Peng, and F. G. Blaabjerg, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," Transactions on Power Electronics, 2021, early access.

M. P. Tcheou, L. Lovisolo, M. V. Ribeiro, E. A. Da Silva, M. A. Rodrigues, J. M. Romano, and P. S. Diniz, "The compression of electric signal waveforms for smart grids: State of the art and future trends," Transactions on Smart Grid, vol. 5, no. 1, pp. 291–302, 2013.

Y.-C. Chang and T.-C. Huang, "An interactive smart grid communication approach for big data traffic," Computers & Electrical Engineering, vol. 67, pp. 170–181, 2018.

H. Maaß, H. K. Cakmak, F. Bach, R. Mikut, A. Harrabi, W. Süß, W. Jakob, K.-U. Stucky, U. G. Kühnapfel, and V. Hagenmeyer, "Data processing of high-rate low-voltage distribution grid recordings for smart grid monitoring and analysis," EURASIP Journal on Advances in Signal Processing, vol. 2015, no. 1, pp. 1–21, 2015.

X. Liang, S. A. Wallace, and D. Nguyen, "Rule-based data-driven analytics for wide-area fault detection using synchrophasor data," Transactions on Industry Applications, vol. 53, no. 3, pp. 1789–1798, 2016.

B. Wang, H. Wang, L. Zhang, D. Zhu, D. Lin, and S. Wan, "A datadriven method to detect and localize the single-phase grounding fault in distribution network based on synchronized phasor measurement," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, p. 195, 2019.

I. Niazazari and H. Livani, "A pmu-data-driven disruptive event classification
in distribution systems," Electric Power Systems Research, vol. 157, pp. 251–260, 2018.