Darwish, Mohamed M.F.; Elsisi, Mahmoud; Fouda, Mostafa M.; Mansour, Diaa Eldin A.; Lehtonen, Matti

Emerging applications of IoT and cybersecurity for electrical power systems

Published in:
IET Generation Transmission and Distribution

DOI:
10.1049/gtd2.13012

Published: 01/10/2023

Document Version
Publisher's PDF, also known as Version of record

Received: 28 September 2023 | Accepted: 29 September 2023

DOI: 10.1049/gtd2.13012

IET Generation, Transmission & Distribution

The Institution of Engineering and Technology WILEY

GUEST EDITORIAL

Emerging applications of IoT and cybersecurity for electrical power systems

1 | INTRODUCTION

With the growth of Internet of Things (IoT) techniques, applications have become smarter, and linked gadgets allow them to be used in many parts of power systems. Meanwhile, cybersecurity is used to improve an application's intelligence and capabilities, especially with the growing size of collected data. Further, the robustness of cybersecurity infrastructure can protect the risk of cyberattacks and facing systems from hackers. This fast-rising trend of IoT and cybersecurity has begun to grow worldwide, especially for power system applications. It is therefore worthwhile to present a comprehensive overview of the current actions and trends involving relative regulations and reservations towards power systems. In this regard, many academics have been drawn to the area of power systems, which have been explored using both Artificial Intelligence (AI) techniques and machine learning (ML) techniques, as well as IoT methodologies. Accordingly, this Special Issue seeks to encourage researchers to showcase cutting-edge research results in the field of promising applications of IoT and cybersecurity based on AI and ML techniques for power systems.

This Special Issue contains a collection of high-quality research that focuses on important topics and offers valuable insights into modern electric power and energy sectors which are the implementation of IoT and Cybersecurity into numerous applications of electrical power systems.

2 | PAPERS IN THE SPECIAL ISSUE

In this Special Issue, the Guest Editors have acknowledged a total of 17 papers which have all been sent to peer-review. Of these 17 papers, 8 have been accepted. These 8 papers were of a very good quality and have contributed to the success of the Special Issue; otherwise,9 papers have been rejected or referred to other journals. The papers address the following key areas:

'***Applications of IoT and digital twin in electrical power systems: A comprehensive survey***': This research paper reviews the applications of the Internet of Things (IoT) and digital twin technology in electrical power systems. It begins by discussing the generalized IoT value chain, followed by the terminology of smart grid, with clarifying the role of IoT-systems and the digital twin structure within the Smart Grid. A comparison between different short-range and long-range transports is presented. The paper then discusses the use of IoT and digital twin technology for effective energy management with applications in smart homes, smart buildings, smart grids, smart industries (Industry 4.0), smart transportation, and smart cities. Additionally, the paper explores the use of IoT and digital twin technology for condition monitoring and diagnosis (CMD) in electrical power systems. Three different cases are presented for CMD, that is, CMD of power transformers, CMD of electrical grids, and CMD of substations. IoT and digital twin applications are also highlighted in power electronic systems. Finally, the paper discusses the challenges and opportunities of applying IoT and digital twin technology to electrical power systems and provides recommendations for future research.

'***A rapid state estimation method for calculating transmission capacity despite cyber security concerns***': This research paper simulates cyberattacks in DIgSILENT for energy management and state estimation. Assuming hackers have adequate information to alter input data, they can alter the power market and the available transmission capability (ATC). Detection programs may fail if false information is coordinated in the presence of error information. The minimum number of network measurements before the state estimation program converges is 54% of the total measurements. In the new method, weighted least squares improve the state estimation speed. The new method can also improve the speed of ATC. In addition to identifying the cyberattack, the algorithm in the present paper can be used to identify the target of the attack. It also uses complete and correct information and even incorrect measurements to report state estimator errors. The paper shows that ATC values follow the inverse pattern of load and loss. A real sample network is presented at the end of the paper to test the suggested method.

'***Optimal power flow-based reactive power control in smart distribution network using real-time cyber-physical co-simulation framework***': This research paper aims to mitigate voltage violations by using optimal power flow (OPF)-based reactive power control (RPC) in a real-time cyber-physical co-simulation (CPCS) framework with multiple smart converters (SCs) in a realistic DN. The OPF-based RPC is achieved by performing the CPCS framework developed in this study.

The CIGRE medium-voltage DN is considered a test system. Real-time optimization and signal processing are achieved by Python-based programs using a model-based toolchain of a real-time DN solver and simulator. Real-time simulation studies show that the proposed method is capable of handling uncertain voltage violations in real time.

'***A Novel detection and defense mechanism against false data injection attack in smart grid***': This research paper aims to develop a novel detection and recovery mechanism against false data injection attack (FDIA) in smart grid. Based on the established state space grid model derived from the three-phase sinusoidal voltage equations, an improved principal component analysis (PCA)-based detection method is proposed. By introducing the mathematical transformation principal method, the detection performance such as detection rate and false-positive rate can be improved. To keep the stable running of the power system, a genetic optimization algorithm-based linear quadratic regulator (LQR) defense method is developed. In addition, to improve the response performance to external attacks, an AI method named genetic optimization algorithm is introduced to optimize the robust performance of the proposed defense method. Finally, the simulation results on the IEEE 6-bus and 118-bus grid systems demonstrate the superiority of the proposed genetic algorithm optimization-based LQR defense method.

'***A security model for smart grid SCADA systems using stochastic neural network***': This research paper intends to design a new detection approach by integrating the optimization and classification models for smart grid SCADA security. In this framework, the min–max normalization is performed at first for noise removal and attribute arrangement. Here, the correlation estimation mechanism is mainly deployed to reduce the dimensionality of features by choosing the relevant features used for attack prediction. Moreover, the optimal features are selected by using the optimal solution provided by the Holistic Harris Hawks Optimization (H^3O). Finally, the Perceptron Stochastic Neural Network (PSNN) is utilized to categorize the normal and attacking data flow in the network with minimal processing time and complexity. By using the combination of the proposed H^3O-PSNN technique, the detection accuracy is improved up to 99% for all datasets used.

'***Increasing the resiliency of power systems in presence of GPS spoofing attacks: A data-driven deep-learning algorithm***': This research paper proposes a Deep-learning GPS-Spoofing Counteraction (DLGSC) algorithm, utilizing phasor measurement units (PMU) data for GPS spoofing attack (GSA) detection and PMU data correction. The algorithm incorporates a recurrent neural network (RNN) and a set of long short-term memory (LSTM) units separately, for signal correction after attack detection. Unlike existing methods that struggle with simultaneous attacks or they are static methods, DLGSC tackles these challenges by leveraging deep learning (DL) techniques. By selecting appropriate features for GSA detection, DLGSC achieves accurate results. The algorithm is evaluated on standard IEEE 14-bus and IEEE 39-bus power systems, and its performance is compared to statistical, dynamic, and DL methods in the literature. Additionally, an experimental setup is designed to validate the algorithm in a laboratory environment. Results demonstrate the easy-implementable DLGSC algorithm's satisfactory real-time performance in various scenarios, such as load variations and noise, achieving over 98% accuracy. Notably, DLGSC is a cable for detecting multiple GSAs on different PMUs.

'***Double-loop settlement monitoring system based on laser collimation***': This research paper proposes a double-loop monitoring system based on laser collimation. The system combines distributed computing, spot image processing, embedded computing, laser collimation technology etc., to design settlement monitoring equipment and corresponding software. Finally, the data processing is carried out by the double-loop calculation algorithm to obtain the sedimentation amount of the analyte. The test results show that the whole system can be intelligently and accurately monitored, and the monitoring accuracy can reach the millimetre level.

'***A new low-cost and low-power industrial Internet of Things infrastructure for effective integration of distributed and isolated systems with smart grids***': This research paper provides an Internet of Things (IoT) infrastructure solution based on a newly designed low-cost microcontroller-based IoT remote terminal unit (RTU) to integrate new, old, and conventional sites of existing grids with smart grids. The IoT RTU supports Wi-Fi communication and includes digital/analog inputs and outputs besides the advantage of serial data transmission standard RS-485 as an industrial field communication (IFC). The Modbus communication protocol is utilized as a serial industrial protocol that can be interfaced over the RS-485 standard. The advantage of having an IFC protocol integrated into the IoT infrastructure enables it to link any supported device and publish the required data to the cloud, besides the ability to add smart metering technologies, which allows Advanced Metering Infrastructure (AMI) in these areas. IoT-enabled SCADA system is integrated with the proposed IoT infrastructure for its advantages of remote monitoring and control. The proposed IoT infrastructure is characterized by proper data security and low power consumption. The IoT infrastructure is simulated with an existing real application for proof of concept, and the results are discussed for different case studies.

3 | CONCLUSIONS

These papers contribute to the body of knowledge surrounding the implementation of IoT and Cybersecurity into numerous applications of electrical power systems, such as electrical smart grids, substations, power electronic systems, power transformers, SCADA systems, DNs, and transmission capacity, which can improve any application's intelligence and capabilities, especially with the growing size of collected data. Further, the robustness of IoT and cybersecurity infrastructure can protect the risk of cyberattacks and facing systems against hackers. Notably, each paper carries unique perspectives and methodologies, showcasing the diversity of methodologies implemented to tackle the technical challenges associated with the implementation of IoT and cybersecurity for electrical power systems.

AUTHOR CONTRIBUTIONS

Mohamed Darwish: Conceptualization; Data curation; Investigation; Methodology; Writing original draft. Mahmoud Elsisi: Conceptualization; Data curation; Resources; Writing original draft. Mostafa Fouda: Conceptualization; Data curation; Supervision; Validation; Writing review & editing. Diaa-Eldin Mansour: Methodology; Resources; Supervision; Validation; Writing review & editing. Matti Lehtonen: Supervision; Validation; Visualization; Writing review & editing.

ACKNOWLEDGEMENTS

The Guest Editors spread their gratitude to all the authors who submitted their research papers to this Special Issue. Many thanks go to the reviewers for their valuable contributions and constructive feedback that helped us make the final decisions. The peer-review process ensured that the selected papers met the highest standards of quality and significance. Lastly, the Guest Editors would like to express their special thanks and, genuine, sincere appreciation and gratitude to the Editors-in-Chief, the Special Issues Editor, and the Editorial Office for their support throughout this mission.

GUEST EDITOR BIOGRAPHIES

Mohamed M. F. Darwish (Senior Member, IEEE) was born in Cairo, Egypt. He received the B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering from the Faculty of Engineering at Shoubra, Benha University, Cairo, in May 2011, June 2014, and January 2018, respectively. From 2016 to 2017, he joined as a Ph.D. student with the Department of Electrical Engineering and Automation (EEA), Aalto University, Finland, and Prof. M. Lehtonen's Group. Since January 2023, he has been working as an Associate Professor with the Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University. He was also a Postdoctoral Researcher with the Department of EEA, School of Electrical Engineering, Aalto University. He has co-authored several international IEEE journals and conferences. His research interests include high voltage, cable insulation, fault diagnosis, polymer nanocomposites, nano-fluids, partial discharge, DGA, renewables, applied machine learning, IoT, and Industry 4.0. He received the Best Ph.D. thesis prize that serves industrial life and society all over the Benha University Staff for the academic year (2018–2019). Moreover, in the academic year (2021–2022), he got the Benha University Encouragement Award in the field of Engineering Sciences and Technology. Since 2021, he has been a Topic Editor in *Catalysts* (MDPI) Journal, also becomes a Guest Editor for several special issues. Further, in 2022, he has been nominated as a young editorial board member of *Applied Energy* Journal. Besides, being a Subject Editor and Associate Editor in *IET Generation, Transmission & Distribution*, and *Frontiers in Energy Research* Journals. In addition, Editor of the *Electric Power Components and Systems* Journal. Finally, in 2023, he has been promoted to Associate Editor in *High Voltage* Journal.

Mahmoud Elsisi (Senior Member, IEEE) was born in Cairo, Egypt, in 1989. He received his B.Sc., M.Sc., and Ph.D. degrees in 2011, 2014, and 2017, respectively from the Electrical Engineering Department, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt. Since 2022, he has worked as an Associate Professor at the Electrical Engineering Department, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt. Also, he is currently an Associate Professor with the National Kaohsiung University of Science and Technology, Taiwan. His research activity includes studying the power system dynamics: stability and control, artificial intelligence techniques, fault diagnosis, renewables, robotics, Industry 4.0, the IoT, and applied machine learning. Since 2021, he becomes a Guest Editor for the special issue in the *Electronics* (MDPI) Journal. Besides, in 2022, he has assigned as a Topic Editor in *Frontiers in Energy Research* Journal.

Mostafa M. Fouda (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Idaho State University, ID, USA. He also holds the position of a Full Professor with Benha University, Egypt. He has worked as an Assistant Professor at Tohoku University, Japan. He was a Postdoctoral Research Associate with Tennessee Technological University, TN, USA. He has been engaged in research on cybersecurity, communication networks, wireless mobile communications, smart healthcare, smart grids, AI, blockchain, and the IoT. He has published more than 70 papers in prestigious peer-reviewed journals and conferences. He received the prestigious 1st place award during his graduation from the Faculty of Engineering at Shoubra, Benha University, in 2002. He has served as the Symposium/the Track Chair of the IEEE VTC2021-Fall Conference. He has also served as the Workshops Chair, the Session Chair, a Technical Program Committee (TPC) Member, and a Designated Reviewer in leading international conferences, such as IEEE GLOBECOM, ICC, PIMRC, ICCVE, IWCMC, and 5G World Forum. He also served as a Guest Editor of some special issues of several top-ranked journals, such as IEEE Wireless Communications (WCM) and IEEE Internet of Things Magazine (IoTM). He also serves as a Referee for some renowned IEEE journals and magazines, such as IEEE Communications Surveys and Tutorials, IEEE Wireless Communications, IEEE Wireless, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Smart

Grid, IEEE Access, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, and IEEE Network. He is an Editor of IEEE Transactions on Vehicular Technology (TVT) and an Associate Editor of IEEE Access Journals.

Diaa-Eldin A. Mansour (S'06-M'10-SM'17) was born in Tanta, Egypt in 1978. He received the B.Sc. and M.Sc. degrees in electrical engineering from Tanta University, Tanta, Egypt, in 2000 and 2004, respectively, and the Ph.D. degree in electrical engineering from Nagoya University, Nagoya, Japan, in 2010. Since 2000, he has been with the Department of Electrical Power and Machines Engineering, Faculty of Engineering, Tanta University, Egypt, and currently, he is working as a Full Professor with the Electrical Power Engineering Department, Egypt-Japan University of Science and Technology (E-JUST), Egypt. From 2010, he was a foreign researcher for three months at EcoTopia Science Institute, Nagoya University, Nagoya, Japan. His research interests are high voltage engineering, condition monitoring, the IoT, diagnosis of electrical power equipment, nanodielectrics, and applied superconductivity. He received the best presentation award two times from IEE of Japan in 2008 and 2009, Prof. Khalifa's Prize from the Egyptian Academy of Scientific Research and Technology in 2013, Tanta University Encouragement Award in 2016, and Egypt-State Encouragement Award in the field of Engineering Sciences in 2018. Recently, he has been listed among the world's top 2% scientists by Stanford University in the USA, three times in 2020, 2021, and 2022. Further, he is an Associate Editor of *Alexandria Engineering Journal*.

Matti Lehtonen received the master's and Licentiate degrees in electrical engineering from Helsinki University of Technology, Finland, in 1984 and 1989, respectively, and the Doctor of Technology degree from Tampere University of Technology, Finland, in 1992. He was with VTT Energy, Espoo, Finland, from 1987 to 2003, and since 1999 has been a Full Professor and Head of power systems and high voltage engineering groups at Aalto University, Espoo, Finland. His research interests include power system planning and assets management, power system protection including earth fault problems, harmonic related issues, high voltage systems, power cable insulation, and polymer nanocomposites. He is an Editor and Special Issue Editor of *IET Generation, Transmission & Distribution* and an Associate Editor of *Electric Power Systems Research* Journal.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Mohamed M. F. Darwish
Mahmoud Elsisi
Mostafa M. Fouda
Diaa-Eldin A. Mansour
Matti Lehtonen

ORCID

Mohamed M. F. Darwish https://orcid.org/0000-0001-9782-8813
Mostafa M. Fouda https://orcid.org/0000-0003-1790-8640
Diaa-Eldin A. Mansour https://orcid.org/0000-0002-3894-4299
Matti Lehtonen https://orcid.org/0000-0002-9979-7333