RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

False Data Injection Attacks (FDIA) detection by Deep Learning Techniques in Smart Grids: survey

Hesham Haider
Department of Computer Science
Amran University, Al-Razi University
Sana'a -Yemen
hesham_haider@yahoo.com

Al-Marhabi Zaid Ali
Department of Cybersecurity and networking
Al-Razi University
Sana'a -Yemen

Ayeda Al-Hmadi
Department of Cybersecurity and networking
Al-Razi University
Sana'a -Yemen

*Corresponding author
Al-Marhabi Zaid Ali
Marhabi2000@gmail.com

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

1. Abstract

Smart grids are becoming increasingly popular due to their ability to enhance energy efficiency and reduce costs. However, they also pose new challenges to the security of the grid. One of the main threats to smart grids is False Data Injection Attacks (FDIA), which can cause serious damage to the grid if not detected and prevented in a timely manner.

Deep learning techniques have shown great promise in detecting FDIA in smart grids due to their ability to automatically learn and detect patterns in large and complex datasets. In this research project, we review the existing deep learning techniques used to detect FDIA in smart grids. We provide an overview of the various deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders, that have been used to detect FDIA.

We also discuss the challenges and limitations of using deep learning techniques for FDIA detection in smart grids, such as the lack of large-scale datasets and the need for more explainable models. Finally, we propose future research directions in this field, such as the development of hybrid models combining deep learning with other techniques to improve the accuracy and efficiency of FDIA detection.

Key Word: *Smart grid, False Data Injection Attacks (FDIA), Deep Learning, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders.*

2. Introduction

The false data attack is recognized as a significant danger, capable of compromising the measurements of sensors in SG and attacking all layers of SG systems, thus bypassing traditional defense mechanisms [1]. For instance, a malicious actor can introduce false values into the state estimation process, resulting in catastrophic outcome. Defending against these attacks has become a significant issue, leading to the development of various detection methods in the past decade. However, most of these methods lack scalability and are not suitable for large-scale SG systems. Effective data analysis and anomaly detection techniques are necessary to handle the massive amount of energy data.

To effectively detect these attacks, deep learning (DL) techniques are increasingly seen as a viable solution due to their scalability. Given the numerous contributions to this area, we aim to conduct a comprehensive survey of the advances in false data detection using DL methods. We will first review previous surveys on this research topic and then highlight our contributions.

False data injection attacks pose a significant risk to the secure and reliable operation of the smart grid, and it is imperative to develop effective methods for detecting and mitigating such attacks. Deep learning, a subfield of artificial intelligence, has shown great promise in various applications, including anomaly detection and security. However, to the best of our knowledge, there have been limited studies exploring the use of deep learning in detecting false data injection attacks in the smart grid.

The main research contributions of this work are summarized as follows:

- It provides a comprehensive overview of the current state-of-the-art research in the field of false data injection attacks and deep learning-based solutions for their detection in smart grids.
- It provides a comparative analysis of different deep learning techniques and identify the strengths and weaknesses of each technique.
- It identifies research gaps in the field of deep learning for FDIA detection in smart grids and highlight areas where further research is needed and suggest future research directions.

2.1 Smart grid's network protocols

Several communication protocols are needed for distributed and diverse applications in the smart grid. The smart grid network architecture and each network's protocol are shown in Figure1.1. ZigBee and Z-wave technologies are used by household appliances in the home area network (HAN) [2]. Devices linked to the neighborhood area network (NAN) often do so via the

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

IEEE 802.11,and IEEE 802.16 , or IEEE 802.15.4 protocols. Several industrial protocols, particularly Distributed Networking Protocols like 3.0 (DNP3) and the (Modicon Communications Bus (ModBus)), are utilized in WAN or Wide Area Networks and supervisory control and data acquisition (SCADA) applications [3]. Protocol IEC 61850 is utilized in substation automation [4]. We will cover Modbus and DNP3 in this section together with two more popular but weak smart grid protocols [5] [6]. The IEC 61850 protocol, power line communication, Bluetooth, Z-Wave, Zigbee, 6LoWPAN, and WiMAX are all covered in full in [7] [8] [5].

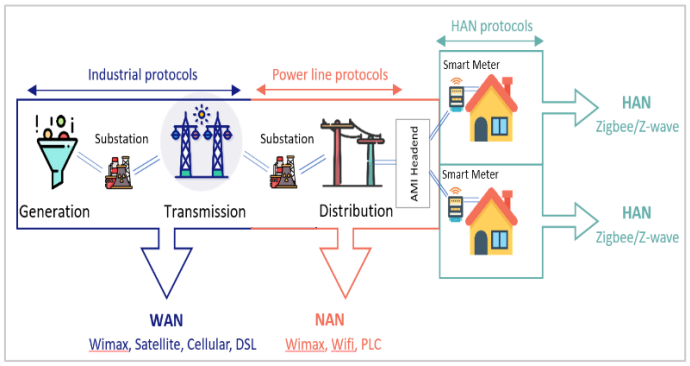

Fig. 1 Illustration of smart grid network architecture

2.2 Impact of FDIAs on Power Systems

On the power grid, FDIAs may have a major negative financial or physical effect.

1- Load Redistribution Attack: The Load Redistribution (LR) attack, which Yuan et al. propose targets the Security-Constrained Economic Dispatch (SCED) and may have an impact on the operation of the power grid, is a specific sort of FDIA [9]. By correctly redistributing the generation output, SCED helps the power system lower the overall cost of system operation. The system is forced into unfeasible operational states as a result of LR attacks, which cause the SCED to deliver inaccurate solutions based on corrupted state estimates. Furthermore, load shedding events that result from LR attacks have the potential to paralyze any quick corrective response [13], [10].

2- Energy Deceiving: Energy misleading assaults, a new FDIA variant that focuses on the energy distribution process' routing procedure, are studied by Liu et al. [11]. To determine the best path for energy to travel between grid nodes, the authors present a distributed energy routing scheme. An energy consumer or a producer, depending on the node, could exist. Using a measurement tool (like a smart meter), various nodes can be distinguished from one another. To share information like as measurements, requests, and demands, all nodes communicate with one another. The information transmitted between nodes is spoofed in order to carry out the energy-deceiving attack. The energy request and answer messages of the nodes contain malicious link-state information or

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

malicious energy information. By carrying out a successful attack, it is possible to introduce fraudulent messages regarding the demand and supply of energy to the power grid and alter the memory of a measuring device. The attack would lead to imbalances between supply and demand, according to the authors' analysis of the energy misleading attack's effects using the suggested methodology. The price of distributing electricity may consequently significantly rise.

3- Economic Attack: Xie et al. show how FDIAs have an impact on the energy market in terms of effects on economic operations [12]. Ex-post LMP values are used to produce the final settlement prices for real-time market prices, which are then based on the actual SCADA measurements. Therefore, the outcomes of the SE, and subsequently, the price of electric energy, can be impacted if an attacker can manipulate the system measurement data. To calculate the LMPs and present the attack as a convex optimization problem, the authors employ a linear form of Optimal Power Flow (OPF), DCOPF. Two instances, one for a single congested line and the other for three congested lines, are applied to the IEEE 14 bus system. The study demonstrates how FDIAs can be used by attackers to manipulate the ex-post market's nodal price and generate profits. In a subsequent study [13], the authors also investigate more plausible assault scenarios under threat models in which the attackers are only able to control a small number of sensors.

4.2 Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning

In [14], the authors propose a framework that utilizes deep learning to identify measurement irregularities resulting from FDI attacks. They employ both recurrent and convolutional neural networks to detect such attacks and their technique is able to identify hidden attacks by learning normal behavior from normal data. Their two-level detector, which is based on hybrid features, is reliable and can detect attacks even when the state vector estimator is not effective. The performance of the proposed algorithm is influenced by various parameters, which the authors discussed in detail. Additionally, they presented a thorough case study of the algorithm's performance on the IEEE 39-bus system.

4.3 Cyber-Secure Hybrid Electric Load Forecasting Model

The proposed deep learning framework AE-CLSTM in [15] combines the Autoencoder (AE), and Convolutional Neural Network (CNN), with Long Short-Term Memory (LSTM) models to reliably anticipate electric demand in power grids across time spans ranging from an hour to a week. The suggested model's architecture is meant to be able to quickly pre-process and extract characteristics from data, and then forecast electric load in the ultra-short-term and short-term time horizons. The AE-CLSTM technique, a unique hybrid model of deep learning applications, is used in this work. Each of the models listed is detailed in depth, as is their

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

mathematical modeling.

The paper [15] proposes a hybrid deep learning model, called AE-CLSTM, for electric load forecasting in ultra-short-term and short-term time horizons, which integrates the capabilities of autoencoder (AE), convolutional neural network (CNN), and long short-term memory (LSTM) models. The AE-CLSTM architecture comprises an AE network for data pre-processing and de-noising, a CNN model for feature extraction and behavioral pattern identification, and an LSTM model for training and forecasting. The performance of the AE-CLSTM model is compared against conventional CNN and LSTM models in terms of load forecasting in Tabriz, Iran, based on meteorological variables and historical information for the years 2017 and 2018. The experimental results for ultra-short-term and short-term load forecasting in all four seasons of 2019 demonstrate the superior performance of the proposed model. Furthermore, the model is shown to be resilient to cyber-attacks, specifically a False Data Injection Attack (FDIA), which is modeled as a scaling attack on air temperature parameters in all four seasons of 2019. The results in this case reveal the AE-CLSTM model's ability to reduce the effects of FDIA and data reconstruction accurately, emphasizing its practicality and security in power system forecasting applications.

4.4 Deep learning-based identification of false data injection attacks on modern smart grids

The proposed anomaly detection approach in [16] was built based on the error covariance matrix after the nonlinear deep learning model was used to anticipate the estimated operating states of the power network.

To define crucial grid functions like load forecasting and economical load dispatch etc, operators at the control center use state estimation techniques [17].

A significant increase in cyberattacks has been observed, creating extremely vulnerable conditions, as a result of the widespread approval of IIOT devices within current power networks. The real-time detection of FDIA in the smart grid in conjunction with an effective projected operating state forecasting is thus the main emphasis of the current research. Compared to other SOA techniques, the robust, nonlinear LSTM structure exhibits a better forecasting horizon. Comparing the nonlinear LSTM structure to MLP, SVM, and ARIMA, there is also a superior improvement of the performance metrics. Since the computational efficiency of the proposed nonlinear LSTM model (i.e., the time required for testing and training) is in the range of μs, which is significantly less than the SCADA sampling period, it can be successfully applied in real-time. Future implementation of the suggested detection approach will be possible under smart grid contingency situations with a tighter bound on the detection benchmark, increasing the likelihood of FDIA discovery.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

4.5 Deep Learning Techniques for Detecting of False Data Injection Attacks(FDIA) in Smart-Grid ystems: Benchmarking

False data injection (FDI) attacks are a critical security issue that have the potential to significantly raise the cost of energy distribution [18]. The majority of current research is focused on FDI defenses for traditional power networks. However, a deep learning system has been developed to detect FDI threats in smart grids. This approach detects FDI assaults in real time via spatial-temporal correlations between grid components.

The goal of FDIA is to deceive the system operator into accepting a compromised state estimate $\hat{x} = x + c$ as a genuine estimate, where $c \neq 0$ is the power system state deviation. They created a new data-driven technique for detecting FDIA in a SCADA system. It is expressed as a multilabel classification problem that assesses if each meter measurement is compromised.

Here in [31] they designed a BDD-CNN architecture as a multilabel classifier and framed the FDIA locational detection problem as a multilabel classification problem. The standard BDD detector, which also filters out low-quality data, is used to assess the real-time measurement data quality. The CNN captures the FDIA's co-occurrence dependence and inconsistent behavior. The approach is cost-effective because it is based on the existing BDD, requires no modifications to the current BDD system, and is model-free because the architecture is independent of any anticipated attack model. Additionally, the detection process takes only a few hundred microseconds on a typical home computer. They also conducted extensive simulations in the IEEE 118-bus power systems to demonstrate its feasibility.

In particular, they showed that DLLD can perform locational detection for the entire bus system under a variety of noise and attack conditions. They further demonstrated that the presence-detection accuracy can be improved further by using a multilabel classification formulation, with the resulting presence-detection accuracy outperforming the state-of-the-art benchmarks.

4.6 Deep learning for online AC False Data Injection Attack detection in smart grids: An approach using LSTM-Autoencoder

The power system is a vital Cyber-Physical system that is susceptible to such assaults. This research [19] provides a new approach for identifying False Data Injection Attacks (FDIA) in the power system. While the current FDIA detection algorithms mostly target DC state estimates, this research suggests a phased AC FDIA that targets load shedding and generation rescheduling. Variational mode decomposition (VMD) is used in the proposed technique to extract the spatial and spectral characteristics of the modes decomposed from the estimated states, and an LSTM-Autoencoder is trained to learn the temporal correlations between the multi-dimensional feature vectors. An LR classifier is trained to determine whether an error deviation vector is anomalous based on the reconstructed error deviation

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

vectors derived from the feature vectors generated and refined through an LSTM Autoencoder. Simulation exercises carried out within customized environments featuring IEEE 14/118 bus systems. Accordingly, the mechanism may attain sufficient levels of attack detection precision.

In [19], a cutting-edge method is suggested to identify an AC FDIA that attempts to trigger load shedding and scheduling. The method is based on signal processing where the estimated state is divided into several modes using VMD, and the spatial and spectral properties are extracted from them. The authors trained an LSTM-Autoencoder model to learn the temporal correlations between the feature vectors using the feature vectors obtained from the "normal" estimated states. The deviation vectors of the reconstruction errors are calculated and updated using the experimental dataset and the trained LSTM-Autoencoder. The LR classifier can distinguish FDIA from events that occur during typical system operation based on the labeled deviation vectors. The effectiveness of the proposed mechanism is first evaluated through simulations, and the number of deconstructed modes is counted. Next, the authors investigated how the structure of the LSTM-Autoencoder affects the effectiveness of detection.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Table 1 paper evaluation

Paper	Author	Year	Algorithm	Performance	Strengths
Paper 1 [14]	Xiangyu Niu et al.	2019	Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks	Accuracy: above 90%. Weakness: When attacking power is low, we observe that the system's precision is low. Additionally, early construction of the electricity network was necessary for this mechanism to perform well.	High detection accuracy may be attained for a variety of circumstances using the two-level detection approach that is being offered. When is high, the suggested detection system can identify assaults by random FDI with an accuracy of above 90%.
Paper 2 [15]	Ying Zhang et al.	2020	AAE-based semi-supervised	Accuracy: 96.25% on 13-bus System and **97.85% on 123-bus system** **Weakness:** For prospective FDIAs that are not thoroughly examined and are not labeled in the training step, the suggested algorithms exhibit some weaknesses.	The suggested technique has a detection error of 2.15% in the 123-bus system and 3.75% in the 13-bus system when utilized to detect the attacked metering data. Additionally, in the 13-bus and 123-bus systems, the suggested method's average computation time is 9.30 and 14.81 milliseconds, respectively. Due to the effective integration of autoencoders with GAN, as demonstrated in the simulation results, better detection accuracy may be achieved. For example, the S3VM-based method performs worse than the suggested approach, with a detection accuracy of less than 80%. The proposed technique, however, obtains a high detection accuracy of up to 95%.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Table 1 paper evaluation

Paper	Author	Year	Algorithm	Performance	Strengths
Paper 3 [13]	Arash Moradzadeh et al.	2022	AE-CLSTM technique (Autoencoder (AE), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) models)	Accuracy: above 97%	the proposed mechanisms shows AE-CLSTM model outperformed traditional CNN and LSTM models in terms of performance, and the FDIA attack was executed as a scaling assault on air temperature parameters during all four seasons of 2019. The proposed AE-CLSTM model was able to remove the impacts of the FDIA assault and rebuild the data by depending on the intelligent structure since the attack was modeled in a way that by retaining the average data, it lowered and raised the air temperature parameters by 5%.
Paper 4 [17]	Debottam Mukherjee et al.	2022	Nonlinear Long Short-Term Memory (LSTM) model	Accuracy: higher than 95% **Weakness:** demonstrates the least accurate identification of the models tested compared to the others, however FDIA recognition is still easily accomplished. Further evidence suggests that SVM, as compared to the nonlinear MLP and ARIMA, requires a longer testing period as well as a longer training period to identify FDIA well.	Since nonlinear LSTM models are computationally efficient and can be successfully executed in real-time, proposed LSTM model detects the presence of FDIA with a probability of 95% for an attack. The detection strategy can also be implemented under contingency scenarios of the smart grid with a stricter bound over the detection benchmark.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Table 1 paper evaluation

Paper	Author	Year	Algorithm	Performance	Strengths
Paper 5 [18]	Lukumba Phiri et al.	2023	BDD-CNN architecture	The accuracy of the recommended detection method surpasses that of the DLBI and SVM algorithms, and that of these algorithms declines as the noise level rises.	The architecture of the mechanism is cost-friendly in that it is built on the existing BDD, requiring no modification of the current BDD system, and model-free in that it depends on no assumed attack model. Additionally, the mechanism's detection process can be completed on a home computer in just a few hundred microseconds. Additionally, it was demonstrated that, in varied noise and attack situations, DLLD can carry out locational detection for the whole bus system.
Paper 6 [19]	Liqun Yang et al.	2021	LSTM-Autoencoder	Accuracy: 94.56% **Weakness:** The location detecting system has various flaws.	The proposed mechanism is model-free since the design is unrelated to any presumptive attack model, is built on the existing BDD, and doesn't call for alterations to the BDD system. Furthermore, on a typical home computer, the detection procedure is completed in a matter of hundred microseconds.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Table 1 paper evaluation

Paper	Author	Year	Algorithm	Performance	Strengths
Paper 7 [4]	Shuoyao Wang et al.	2020	Deep Learning based Locational Detection architecture (DLLD). The DLLD architecture concatenates a convolutional neural network (**CNN**) with a standard bad data detector (**BDD**).	DLLD (Deep Learning for Large-scale Detection) achieves a high F1-Score of 99.37% and a RACC of 93.2%. **Weakness:** suggested a reconstruction error distribution-based method for anomaly identification, however this approach has a high incidence of false alarms and necessitates setting a threshold.	The proposed DLLD approach proposed a detection mechanism that is resistant to environmental noise and resilient to malfunctioning buses. The detection performance of the proposed method is superior to that of ARMA and RNN-Autoencoder, and the proposed mechanism can archive the best performance with an AUC of 0.9464. This demonstrates the superior effectiveness of our detection strategy.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Table 1 paper evaluation

Paper	Author	Year	Algorithm	Performance	Strengths
Paper 8 [16]	Adel Tabakhpour et al.	2019	A Multi-Layer Perceptron (MLP)	Accuracy: between 91.80% and 99.87% **Weakness:** unable to launch a real-time assault.	While 20% of them lack errors, the majority contains inconsistent, arbitrary-generated falsehoods (80%). To effectively train models, trains each of the 10,000 sets equally, allocating around 70% for actual model refinement, approximately 15% for quality control, and nearly 15% reserved exclusively for assessment. By leveraging the strong connection among remaining factors in our situation, PCA enables us to significantly reduce the dimensionality of our model (more than 90%) while keeping comparable efficacy. Reducing the number of training epochs from 118 to 44 also applies Principal Component Analysis (PCA) to the identical Multi-Layer Perceptron (MLP).

5. Conclusion

Smart grid networks attack is increasing day by day confronting the expansion of the use of these networks, and the objective of these attacks is to destroy or reduce the efficiency of these networks. Here in this paper we focused on the most important strongest research's which published in the resent five years (and this is what is done in all research In scientific papers published in the largest international journals), as there is no need to review all the research but its better to focus is only on recently published scientific papers, which were published in highly peer-reviewed journals with a high impact factors.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Our paper focused on the research's that provided highly efficient techniques in confronting these attacks. In our paper, we reviewed the most important techniques that these researches presented, the most important advantages of the research, and some of the shortcomings from our point of view. In the table above, a comprehensive summary was made of the most important things mentioned in those papers, including: The most important scientific contribution of this research is summarizing and criticizing that research in a scientific and useful way for the reader, and this in itself is considered an important scientific contribution.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

6. References

[1] Y. Q. L. Cui, L. Gao, G. Xie and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," *Journal of Network and Computer Applications*, vol. 170, p. 102808, 2020.

[2] M. A. Faisal, Z. Aung, J. R. Williams and A. Sanchez, "Data-streambased intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Systems Journal*, Vols. 9, no. 1, p. 31–44, 2015.

[3] R. Radvanovsky and J. Brodsky, Handbook of SCADA/control systems security, CRC Press, 2013.

[4] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57 no. 5, p. 1344–1371, 2013.

[5] V. C. G. e. al., "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, Vols. 7, no. 4, p. 529–539, Nov. 2011.

[6] M. Bristow, "ModScan: a SCADA Modbus network scanner," *in DefCon-16 Conf.*, Vols. Las Vegas, NV, 2008.

[7] A. Usman and S. H. Shami, "Evolution of communication technologies for smart grid applications," *Renewable and Sustainable Energy Reviews*, vol. 19, p. 191–199, 2013.

[8] A. Mahmood, N. Javaid and S. Razzaq, "A review of wireless communications for smart grid," *Renewable and Sustainable Energy Reviews*, vol. 41, p. 248–260, Jan. 2015.

[9] Y. Yuan, Z. Li and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, p. 382–390, 2011.

[10] M. A. Rahman, E. Al-Shaer and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," *in Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on. IEEE*, p. 649–659, 2014.

[11] J. Lin, W. Yu, X. Yang, G. Xu and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," *in Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems. IEEE Computer Society*, p. 183–192, 2012.

[12] L. Xie, Y. Mo and B. Sinopoli, "False data injection attacks in electricity markets," *in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE*, p. 226–231, 2010.

[13] --, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, p. 659–666, 2011.

[14] X. Niu, J. Li, J. Sun and K. Tomsovic, "Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning," *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA*, pp. 1-6, 2019.

[15] A. Moradzadeh, Mostafa Mohammadpourfard, Charalambos Konstantinou, Istemihan Genc, Taesic Kim and Behnam Mohammadi-Ivatloo, "Electric load forecasting under False Data Injection Attacks using deep learning," *Energy Reports*, vol. 8, pp. 9933-9945, 2022.

[16] D. Mukherjee, Samrat Chakraborty, Almoataz Y. Abdelaziz and Adel El-Shahat, "Deep learning-based identification of false data injection attacks on modern smart grids," *Energy Reports*, vol. 8, pp. 919-930, 2022.

[17] A. Ali and Exposito Antonio G, "Power system state estimation: Theory and implementation," *CRC Press;*, 2004.

[18] L. Phiri and Simon Tembo, "Detection of False Data Injection Attacks in Smart-Grid Systems: Benchmarking Deep Learning Techniques," *Journal of Electrical Electronics Engineering*, vol. 2, no. 1, pp. 41-49, 2023.

[19] L. Yang, You Zhai and Zhoujun Li, "Deep learning for online AC False Data Injection Attack detection in smart grids: An approach using LSTM-Autoencoder," *Journal of*

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Network and Computer Applications, vol. 139, 2021.

[20] X. Niu, J. Li, J. Sun and K. Tomsovic, "Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning," *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, *Washington, DC, USA*, pp. 1-6, 2019.

[21] S. Wang, S. Bi and Y. -J. A. Zhang, "Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach," *in IEEE Internet of Things*, vol. 7, no. 9, pp. 8218-8227, 2020.