

## Identification scheme of false data injection attack based on deep learning algorithms for smart grids

Marwah Ezzulddin Merza<sup>1</sup>, Shamil H. Hussein<sup>2</sup>, Qutaiba I. Ali<sup>3</sup>

<sup>1</sup>Department of Mechatronics Engineering, College of Engineering, University of Mosul, Mosul, Iraq

<sup>2</sup>Department of Electrical Engineering, College of Engineering, University of Mosul, Mosul, Iraq

<sup>3</sup>Department of Computer Engineering, College of Engineering, University of Mosul, Mosul, Iraq

### Article Info

#### Article history:

Received Aug 29, 2022

Revised Nov 17, 2022

Accepted Nov 21, 2022

#### Keywords:

AI techniques

Cyber security smart grid

False data injection

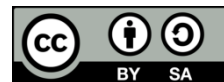
Smart grid

Threats and attacks

### ABSTRACT

This paper presents the artificial intelligence (AI) techniques based on the deep learning algorithms to diagnose false data injection (FDI) attacks to smart grids with the measurement data in real-time. The power and data flow between end-user consumers and all components of the advanced metering infrastructure (AMI) and supervisory control and data acquisition (SCADA) system in the SG is bidirectional flow by advanced communication networks. For all the advantages of the SG come with, they remain at risk to a series of many potential threats and ongoing attacks. The conditional-deep-belief-network (CDBN) architecture is employed to un-observable FDI attacks which pass the state-vector-estimator (SVE) mechanisms. The IEEE 118 bus, and IEEE 300 bus power system have been used to evaluate our detection scheme. Finally, the suggested CDBN scheme is compared with other detection such as artificial neural network (ANN) and support vector machine (SVM). It is observed that the simulation result shows that suggested detection methods can attain a high accuracy of unobservable FDI attacks.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Shamil H. Hussein

Department of Electrical Engineering, College of Engineering, University of Mosul

Mosul, 41002, Iraq

Email: shamil\_alnajjar84@uomosul.edu.iq

## 1. INTRODUCTION

The Distribution systems of traditional electric grid used to convey produced energy from centralized plants to customers by high voltage transmission lines. This grids have many defect, including the disability to involve various sources, green energy, costly assets, and time consumption of demand response, greenhouse emission, and blackouts [1]. It is shown that these issues of system cannot be addressed with conventional grid. Therefore, the smart grid is used to solve the issues as mentioned above, then the SG enables manage and distributed power flow and information by two-way direction by using Information and communications technologies (ICT) [2]. Smart grid has flexibility via distributed generation, reliability via self-healing, and efficiency through load balancing and use intelligent devices [3]. The SG can be combination of renewable energy resources such as solar cell photovoltaic and wind and have many major components are household appliances, renewable energy resources, smart meter and devices, and utility centers [4]. The communications networks in smart grids are the core network, wide area network (WAN), neighborhood area network (NAN), and local area network (HAN) that implemented in real time control in order to realize reliability. A core network is used for long distance based on fiber optic cables and have two standards, OpenADR and IEEE 2030.5 power assets [5]. High performance of WANs can be realized by using the long term evolution LTE networks. Neighborhood ZigBee network is used to receive state of data from WAN net and delivered to residential building and consumers. ZigBee is a low power dissipation and connect smart meters to the

networks based on IEEE 802.15.4 bus. WiMAX, 3G/LTE technologies are used for communication and combine the house appliances to smart meters [6].

There are many paper published that presented general problems about cyber-security in infrastructure of SG. Rawat and Bajracharya [7] presented a study of the challenges and Vulnerabilities existing in SG cyber security. They classified attacks based on the LAN, NAN, and WAN networks. The authors studied the impact of each threats and attacks on the data security, confidentiality of the data for customers by using encryption techniques such like AES, integrity of the system and data flow between users and SCADA system, and availability of advanced metering infrastructure (AMI) devices for users.

Sakhnini *et al.* [8] analyze three different techniques of the supervised learning such as three types of feature selection (FS) techniques that are implemented on the IEEE 14, 57, and 118 bus system for estimation of fluctuation. The IEEE buses systems has been implemented to test and detect false data injection (FDI) attacks by using supervised learning algorithm. High performance have been obtained for detection via integration the learning algorithm with heuristic FS methods.

In this study, some notable recent attacks, threats, and the security vulnerabilities are described against infrastructures of the SG. This paper presents the AI techniques based on the deep learning algorithms to diagnose FDI attacks to smart grids with the measurement data in real-time. The performance of the suggested detection method has been inspected through the effect of the following points: first of all, the amount of compromised data samples, the level of the noise produced from the environment. The CDBN architecture is employed to un-observable FDI attacks which pass the SVE mechanisms. Finally, the threshold level for SVE suggested. Afterward, evaluating our proposed detection against the artificial neural network (ANN) and support vector machine (SVM).

## 2. SMART GRID ATTACKS AND CYBER-SECURITY PRINCIPLES

SG systems contains on many units such like, phasor measuring units (PMU), sectional control, power production, ICT technology, intelligent electronic devices (IEDs), smart meters and devices, remote terminal units, human-machine-interfaces (HMI), and protocol gateway [9]. SCADA system provides controller and observer of the electric grid units as a real time. The AMI is the combination the utility control units and smart devices. The power transmission lines of the SG can be implemented by using internet of things (IoT) technologies that leads to reduce cost of the transfer power and data from utilities to customer and vice versa. The SG support the environments by eliminate greenhouse carbon emissions and independent of the fossil fuels via using hybrid electric vehicles (HEV) [10].

The security required of the smart power grids are confidentiality-integrity-availability (CIA) triad. The institute-of-standards-and-technology (NIST) has identify three standard needed to preserve security of data in the SG, specifically CIA triad. In general, confidentiality protects reasonable boundaries on the access and disclosure of information. Integrity in SG means protecting against manipulation of the information of customers' bills. Availability is reliable access of consumers to private information of them [11]. The cyber-security issues are one of the impairment disadvantages of SG development. The problems of the SG cyber-security involve realize the security service CIA of the system and intelligent technology. The C\_I\_A triad is fundamental of protection of the energy management units. The aims of the SG Cyber-security must have reservation protect data with CIA service [12]. The wide-spread energy blackout to energy resources in smart grid has been getting up because of cyber-attacks. Therefore, the cyber-attacks for SG security have been categorized to three ways by CIA triad as shown in Table 1.

There are many cyber-attacks of smart-grids according to network layers. Network layers are application, transport, MAC, and physical layer. The attacks exist in application layer can penetrate system that has limited on many computing resources by flood attack. In addition to, the denial-of-service attack objective to destroy resources in system such as memory, CPU or bandwidth [13]. Spoofing attack are pernicious threat in MAC layer. The main aim of this attack in SG is phasor measurement units (PMU) by investment the item range in a layer framework, can deny forward dummy data to other devices [14]. Transport layer attacks such like TCP and UDP which cause flooding availability objective of users. Therefore, the base system cannot receive valid flow data. Man in-the middle (MITM) attack can pass during IP spoofing to deny connection. The most important prevention towards a MITM is using good encrypted algorithm. In this layer, an IDS system is efficient security solution for detect vulnerability exploits from attacker against computer and systems [15]. While in the physical layer, jamming attack is the important dangerous type that occurs in wireless networks.

The systematic approach is used to analyze the following types of attack. Figure 1 shows described of the system as a control center and smart grid [16]. The whole system contains control centers for SCADA, wide area measurement system (WAMS) technologies, inputs and relevant outputs.

Table 1. SG cyber attacks classification

Cyber_security objective	Attack type	Solution
Confidentiality	Eavesdropping, traffic analysis, unauthorized access, password pilfering, MITM, replay, masquerading, data Injection Attacks.	Authentication processes, and encryption.
Integrity	Tampering, replay, false data injection, spoofing, data modification, time synchronization, masquerading, load drop attacks.	Power fingerprinting technique, Volt-var control, trusted network connect, authenticity, and non-repudiation.
Availability	Jamming, denial of service (Dos), low-rate Dos, buffer overflow, teardrop, time synchronization, masquerading, MITM, spoofing attacks.	Traffic filtering, Big pipes, anomaly detection approaches and Applying air-gapped network.

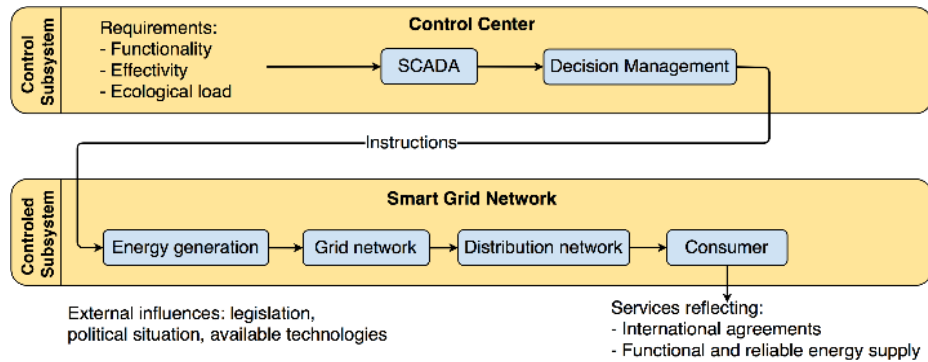


Figure 1. Smart grid systematic approach [16]

**2.1. NAN and HAN networks**

Advanced encryption standard counter (AES-CTR) algorithms is used to detection of some attacks exist in the HAN, WAN networks, such like Dos and spoofed annunciation packets. The communication is realized via ZigBee network technology. Utilize of the same keys on multiple access control list (ACL), tuning on an encryption value when the electricity is theft. This encryption algorithm detects MITM attack, MAC and point spoofing via radio spectrum congestion that exist in Wi-Fi topology. MITM attacks sending by using WiMAX network forge messages to server which increase end user's energy and jamming [17].

**2.2. SCADA systems**

SCADA serves as the backbone of several critical infrastructures. SCADA system provides controller and observer of the electric grid units as a real time. The AMI is the combination the utility control units and smart devices. As a result, it is critically important to analyse cyber risks associated with the industrial SCADA system. There are many vulnerabilities on the data networks of SCADA system, such as security problem in operating system, mistaken management, wrong security from account and password requirements to access, error in software of the hosting server by Dos threat, and finally configured firewall faulty that leads to insufficient network infrastructure security [18].

**2.3. Advanced metering infrastructure attack**

Un-authorized data access and modification, stealing data, physical harm to the tools, malicious software and devices insertion, data integrity blocking, and data leaks via person. These risks threatened to AMI devices that found in the SG systems. For example, of the communication attacks, FEMTO cell attack to GPRS service, physical attacks require access to the metering device to measure power consumption, and over-voltage attack to metering device and thus destroy the electronic circuits. The connection between the metering devices and communication infrastructure will disable through damage of the antenna which is a type of attack called mechanical damage [19].

**2.4. IP spoofing attacks**

IP-address-spoofing is the practice of faking the data in the source IP-header, typically using random number, in order to conceal the identity of the sender or conduct a mirrored D.DoS attack. There is a great attack on the IP networks on both versions of IPv4 and IPv6. The use of IPsec in IPv6 is only recommended, making its security very similar to the IPv4.

### 3. ARTIFICIAL INTELLIGENCE TECHNIQUES IN SG

There are many take place countermeasures to detect and prevent the cyber-attacks, such as encryption algorithm, VPN, Firewall, antivirus software, IDS, and access control. From a security management viewpoint, the countermeasures must hood risk estimate of resources at behind attack, exchange and manage of secret key, and vulnerability reporting [20]. Different security strategies to defense solution through AI, machine-learning (ML), certificate authenticity (CA), and proactive real-time IPS-IDS. These methods provide adaptability, flexible, and patient security technology. The secure framework is required to the following: authenticity and access control of the system, detection and countermeasures procedures, cryptographic functions at every node in grid, and Security of network protocols in MAC layer.

The AI technique that used in the SG are aggregate of multi data about operation of the SG by using combining AMI, control systems, and communication. This technique can be classified to fuzzy systems and artificial neural networks ANN [21]. ML learning is a part of the AI and just a way to perform AI systems [22]. The AI may be learned by supervised, unsupervised, and reinforcement learning methods that can be overcome the limitations with better performance has been realized [23]. The artificial ANN techniques allows the detection rate and time of threats, attacks and state its clean solution [24].

#### 3.1. Load forecasting attacks

The load forecast (LF) is the most important factor in the operation of any power system. System operator and utilities use forecast models using input features like historical loads and weather forecasts to help with commitment and dispatch decisions. As the forecasting techniques become more sophisticated, however, they also become more vulnerable to cybersecurity threats. In order to solve the LF issues are used the deep learning (DL) algorithm based on convolutional neural networks CNN, wavelet neural network WNN, and ANN schemes [25].

#### 3.2. Power grid stability assessments

The power grid stability assessment represents the reliability and security of the power system and it is containing many evolutional of stability, such as transient, frequency, small signal, and voltage. The stability meaning the ability of the power system to stay at an equilibrium operation state after a perturbation. AI methods are used to analysis these assessments that have been applied on power grid because of the development of PMU [26].

#### 3.3. Fault detection FD

The FD of the transmission lines in the energy plants which use long short-term memory (LSTM) networks and state estimation matrix (x). LSTM uses RNNs model in smart grid. FD represent the most one challenge for the progress of the micro-grid, that sitting an efficient energy for the integration of distributed power resource and can be used k-nearest neighbor (KNN) algorithm to prevent FD attack [27].

#### 3.4. Smart grid security

The SGs are exposed to many issues of security because of the complexity of SG system and the weakness of communication technologies. The cyber-attack of the network is causing failures in the operation and power supply, synchronization loss with complete electricity theft. The FDI and distributed Dos are attacks to SG networks [28]. To prevention and detection of these threats must be improve the overall security. Many approaches have been used the state of the art intelligent technology. ANN and SVE were used previously to detect FDI. Table 2. brief some intelligent techniques for SG security.

FDI attacks on the secure data integrity that threat to the SCADA system. Despite, smart grid improved the specific of controlled of infrastructure through ICT and intelligent devices. FDI increases the rate of electricity theft by the state estimator measured data of the load profiles in real time. To diagnosis the habit merit of the FDI and measurement data, the deep learning technique is used to detect FDI attack [29]. For the sake of maintaining the efficiency of the power grid, the system state estimation is used that measured the voltage buses, power flow bus, and load profile by the remote transducers units is shown in Figure 2. Thus these measured values are sent to a SCADA system which analysis data and resend to the unit called remote terminal units (RTUs) to make the operation system is more reliable [30].

$$\text{Let } z = [z_1 \ z_2 \ z_3 \ \dots \ z_m]^T \in R^m \quad (1)$$

$$\text{Let } x = [x_1 \ x_2 \ x_3 \ \dots \ x_n]^T \in R^n \quad (2)$$

$$\text{Let } e = [e_1 \ e_2 \ e_3 \ \dots \ e_m]^T \in R^m \quad (3)$$

Where  $z$ : measurement vector.  $x$ : state vector.  $e$ : measurement error vector. The observation model in the d.c power flow, where the  $(H)$  is the Jacobian state matrix of the power system.

$$z = Hx + e \tag{4}$$

By using minimum mean square error that is the statistical criteria. The state estimated ( $\hat{x}$ ) can be calculated by (5), where  $(\Lambda)$ : it is a diagonal state of the system.

$$\hat{x} = (H^T \Lambda H)^{-1} H^T \Lambda z \tag{5}$$

The FDI attackers have the ability of detect a finite number of state load profiles and also have the information of the Jacobian Matrix  $H$  of the system. The observation model of these FDI can be described with additive attack called the state vector ( $a$ ).

$$\hat{z}_a = Hx + a + e \tag{6}$$

Table 2. Intelligent approaches of security for SG networks

Objects	Mechanism
Intrusion detection	Reinforcement learning (RL)
Detect malicious voltage control	ANN
Attack detection	KNN, SVM
Survey	Data-driven approach

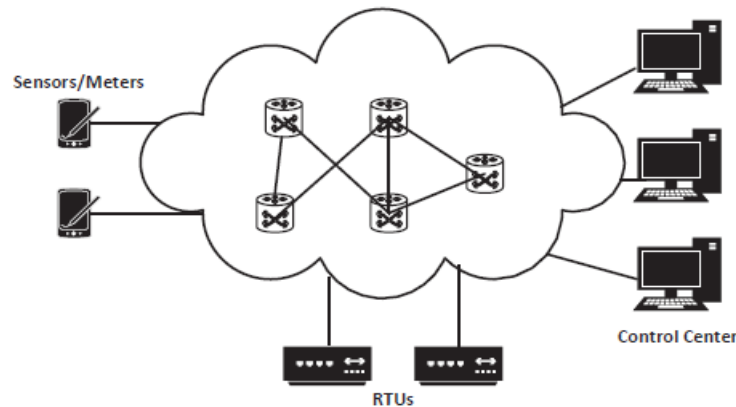


Figure 2. Communication structure of RTU sensors and control systems

Real-time mechanisms for detect FDI attack consist of a SVE-unit and deep learning based identification (DLBI) schemes as shown in Figure 3. The measurement data quality should be adjusted by SVM unit as a real-time by finding the  $\ell_2$ -Norm as described in (6). The calculation result  $\eta$ , from this (6) with a pre-determined threshold level ( $\tau$ ). The SVE record attacks alarm, if  $(\eta) > \tau$ , the estimated data is penetrated information.

$$\begin{aligned} \eta = \|\hat{z} - H\hat{x}\|_2 > \tau & \text{Attack alarm is reported.} \\ \eta = \|\hat{z} - H\hat{x}\|_2 \leq \tau & \text{No attack is reported} \end{aligned} \tag{7}$$

Where  $\|\cdot\|_2$ , denotes  $\ell_2$ -norm operation. If ( $\tau$ ) is very low, the state SVE system is reduced the false alert on the FDI Detection. While if ( $\tau$ ) is very high, SVE unit potency will be increased the treatment loads of the DLBI unit.

The perverse control  $\hat{z}_a$  that cannot be disclosed by SVE unit because of the availability of the FDI attack to threat. Therefore, the DLBI was used to detect the un-observable FDI attacks which consists of two fundamental mechanisms in parallel based on (7). Modify the conditional-deep-belief-network (CDBN) architecture via the training procedure. Diagnosis of FDI by using real time updating of the currently CDBN. DLBI scheme assigned with label  $l=1$ , when the FDI attacks is existence at collect of the data measurements. While it is assigned with label  $l=0$ , when no FDI occurrences. Otherwise, this vector is kept un-labeled.

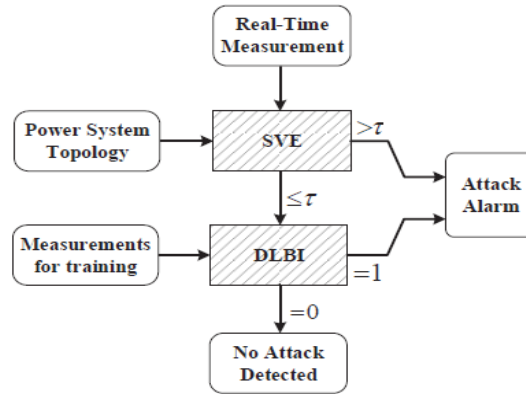


Figure 3. FDI attacks detecting by using deep learning on real-time

**4. IDENTIFICATION SCHEME BASED ON DEEP LEARNING ALGORITHMS**

The electricity theft through FDI intrusion and specify the model by the following approaches of the attackers: i) they have information about structure of the system; ii) they are capable of corrupting the state measurement data such as load profiles; iii) they have understanding of the SVE mechanism without the threshold level, and iv) stealing electricity and modification of the measurement data.

In general, the widely used to detect FDI attacks is the SVE. Therefore, the third assumption above is the threat model is reasonable. The optimization model, such the sequential-quadratic-programming (SQP) algorithms is used to fix and prevent FDI attacks as described in [31]. This algorithm transfers the bases of the main issue to sub-problem QP and accomplish the solved through numerical iteration. Then the sub-problems are solved by the SQP methods that represent a sequence of optimization.

As mentioned above, DLBI unit is progressed to detect the penetrated data which passed SVE mechanism. It is connected the deep-belief-network (DBN) structure with conditional Gaussian bernoulli restricted boltzmann machines (CGBRBM) which is capable of responding to the input value in real time. CDBN uses the 1<sup>st</sup> hidden layer and for stages k-1, where k is the number of hidden layers of CDBN as shown in Figure 4. To perfect detection of the FDI, the output unit shows whether or not FDI attacks have compromised the data.

The unsupervised training process of the CDBN structure is described by energy function as follows by (8): where  $(v_j)$  is the  $j^{\text{th}}$  component of the visible-vector,  $(h_i)$  is the  $i^{\text{th}}$  elements of the hidden-unit's vector,  $(w_{ij})$  is the  $ij^{\text{th}}$  elements of the weight-matrix between the visible-units and hidden-units, and  $d_i$  and  $c_j$  stand for the  $i^{\text{th}}$  and  $j^{\text{th}}$  elements of the weight matrix between the visible units and hidden units.

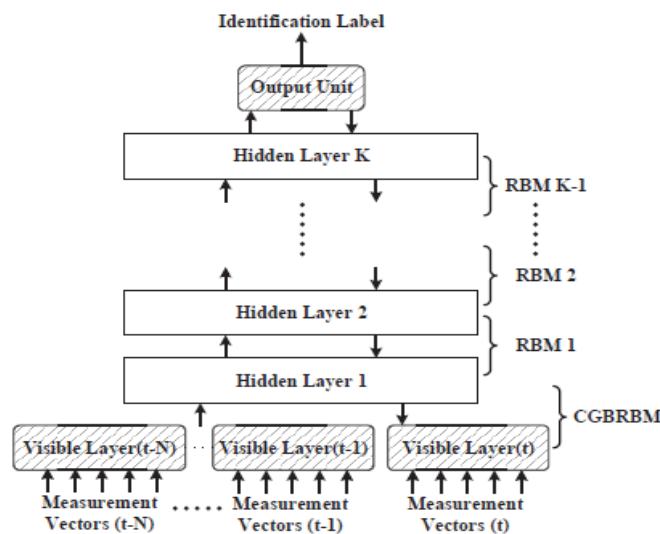


Figure 4. Design of the CDBN architecture

$$E(v, h) = -\sum_{i=1}^n \sum_{j=1}^m w_{ij} h_i v_j - \sum_{j=1}^m c_j v_j - \sum_{i=1}^n d_i h_i \tag{8}$$

While the structure of the CGBRBM designed for our CDBN architecture has (N + 1) visible layers and one hidden layer is illustrated in Figure 5. The energy-function of the CGBRBMs is reported as a (9): when n is the number of the visible-windows, and ( $\sigma_j$ ) is the standard deviation of the  $j^{th}$  parts of the visible-vectors.

$$E(v_t \dots v_{t-N}, h) = -\sum_i \sum_j w_{ij} h_i \frac{v_j}{\sigma_j^2} - \sum_i d_i h_i + \sum_j \frac{(v_j - c_j)^2}{2\sigma_j^2} \tag{9}$$

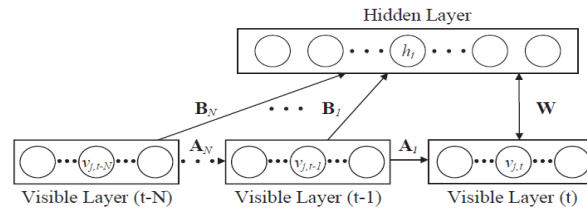


Figure 5. The CGBRBM structure for our suggested CDBN unit

In this paper, the performance of our detection mechanism has been illustrated by using IEEE 118 bus system as shown in Figure 6 and detailed in [32]. The IEEE 300 bus power-system, which is described in [33], is a larger-scale test system that we use to assess the scalability of our work. Use load profiles that were obtained from the real world for our approach, a specific portion of which are certified to contain contaminated data. In the DLBI scheme, to have enough labeled compromised information for training the CDBN structure. The data obtained must be extend from the world by using several analyses and techniques such as fourier transform, main component analysis, and create more vulnerable data that have same pattern with those from the out-world. Finally, we obtain enough compromised load profiles to effectively implement our DLBI scheme by integrating real data with artificially generated data. It is reasonable to assume that just a few load profiles can be corrupted by FDI attacks. Therefore, we assume that FDI attacks in IEEE 118 and IEEE 300 buses respectively, can corrupt up to 64 and 231 loads. Figure 7 illustrates a typical load profile for a one-day.

To analyze the evaluation of our real-time technique for the FDI Attack. Case study has been taken for the effect of the many keys on the detection-accuracy such like, the numbers of load-profiles, level of the environment noise, and the threshold ( $\tau$ ) value of SVE unit. We also compare the performance of DLBI schemes with an ANN based and a SVM respectively to demonstrate the effectiveness of CDBN structure. From the case study showed that the accuracy of CDBN scheme with different hidden layers was unobservable and described in the Table 3.

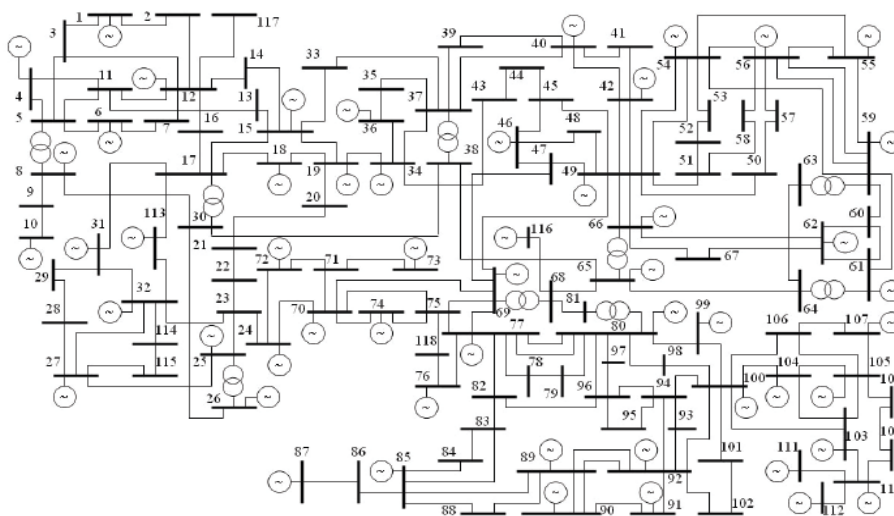


Figure 6. IEEE 118 bus power test system [32]

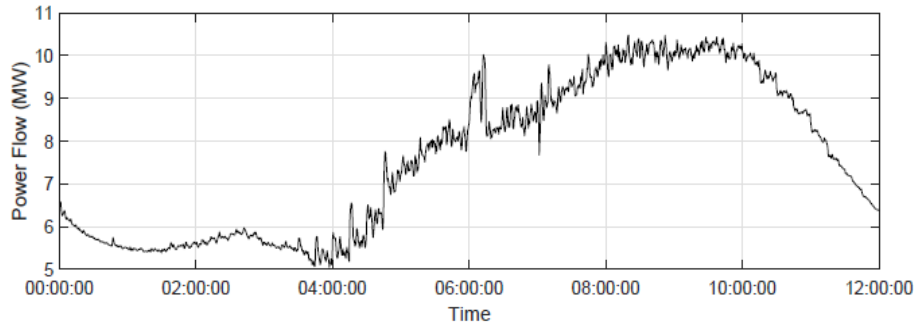


Figure 7. IEEE 118 bus power test system [32]

Table 3. Different elements of the hidden-layers of the FDI CDBNs unobservable attacks with the accuracy detecting

Number of buses	Accuracy (%)		
	3 hidden layers	4 hidden layers	5 hidden layers
32	94	94.6	95.6
40	96.2	96.6	96.7
48	96.6	96.9	97
56	97.9	98	97.9
64	97.7	98	98

As a clear from table the accuracy increases with increase the numbers of hidden layer of the CDBNs unit. Therefore, the CDBN have five hidden layers to achieve a good detection accuracy [31]. To investigate how the number of arrangement load profile, noise in the data-acquisition, and threshold of SVE detection affects the effectiveness of our detection method. Firstly, Figure 8 shows the accuracy attained by our technique with the ANN and SVM schemes. The CDBN-based deep learning algorithms acquire the highest accuracy via the three methods. Next, we take effect of the noise on the data acquired by assuming both the number of the load-profile and threshold are constants.

Figure 9 illustrated relationship between the noise and accuracy, as cleared from this figure, when the noise level increases, the accuracy of the three structures is decreased by assuming the loads and  $\tau$  are 64 and 10 respectively. As mentioned above, the attackers are aware of SVE's threshold. As a result, when the SVE detection threshold rises, the Attack will rise the value of fake data, potentially leading to a greater disparity in the forms of compromised and real data. We can see that when  $\tau \leq 10$ , the CDBN design can recognize the assault with an accuracy of more than 90% compared to ANN and SVM systems.

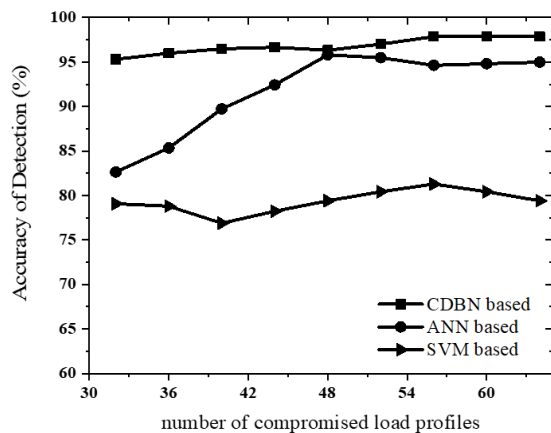


Figure 8. The accuracy of detecting unobservable FDI Attack with different numbers of the loads

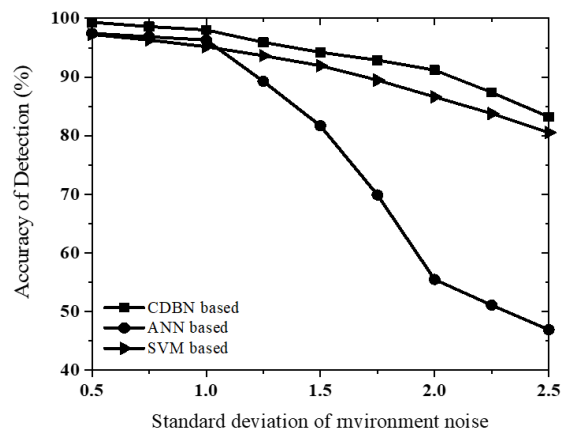


Figure 9. The accuracy of unobservable FDI attacks with different standards deviation of environment noise



## 5. CONCLUSION

The utilization of smart grids is predictable to increase in the future, especially with the rising demand for electricity. In order to respond with these requirements, perfect security has to be realized and implemented. Cyber security is some most important main problems for SG applications which involve data acquisition from intelligent meters. This paper presents the artificial intelligence (AI) techniques based on the deep Learning algorithms to diagnose FDI attacks to smart grids with the measurement data in real-time. The CDBN architecture is employed to un-observable FDI attacks which pass the SVE mechanisms. The IEEE 118 bus, and IEEE 300 bus power system have been used to evaluate our detection scheme. The suggested CDBN scheme is compared with other detection such as ANN and SVM. It is observed that the simulation result shows that our detection method can attain a high accuracy of unobservable FDI attacks.




## REFERENCES

- [1] H. Farooq, W. Ali, and I. A. Sajjad, "Smart grids and smart metering," in *The 4Ds of Energy Transition*, Wiley, 2022, pp. 357–379.
- [2] J. Sanusi, O. Oghenewogaga, B. B. Adetokun, and A. M. Abba, "The impact of communication technologies on the smart grid," in *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, Apr. 2022, pp. 1–5, doi: 10.1109/NIGERCON54645.2022.9803162.
- [3] S. S. Refaat and A. Mohamed, "Smart management system for improving the reliability and availability of substations in smart grid with distributed generation," *The Journal of Engineering*, vol. 2019, no. 17, pp. 4236–4240, Jun. 2019, doi: 10.1049/joe.2018.8215.
- [4] I. Worighi, A. Maach, A. Hafid, O. Hegazy, and J. V. Mierlo, "Integrating renewable energy in smart grid system: Architecture, virtualization and analysis," *Sustainable Energy, Grids and Networks*, vol. 18, p. 100226, Jun. 2019, doi: 10.1016/j.segan.2019.100226.
- [5] N. Raza, M. Q. Akbar, A. A. Soofi, and S. Akbar, "Study of smart grid communication network architectures and technologies," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 19–29, 2019, doi: 10.4236/jcc.2019.73003.
- [6] S. H. Hussein, S. W. Luhab, M. T. Yaseen, and M. Jasim, "Study and design of class f power amplifier for mobile applications," *Journal of Engineering Science and Technology*, vol. 16, no. 5, pp. 3822–3834, 2021.
- [7] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: status, challenges and perspectives," in *SoutheastCon 2015*, Apr. 2015, pp. 1–6, doi: 10.1109/SECON.2015.7132891.
- [8] J. Sakhini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, Aug. 2019, pp. 108–112, doi: 10.1109/SEGE.2019.8859946.
- [9] A. E. L. Rivas and T. Abrão, "Faults in smart grid systems: monitoring, detection and classification," *Electric Power Systems Research*, vol. 189, p. 106602, Dec. 2020, doi: 10.1016/j.epsr.2020.106602.
- [10] S. R. Mugunthan and T. Vijayakumar, "Review on IoT based smart grid architecture implementations," *Journal of Electrical Engineering and Automation*, vol. 01, no. 01, pp. 12–20, Sep. 2019, doi: 10.36548/jeea.2019.1.002.
- [11] A. Mohammed and G. George, "Vulnerabilities and strategies of cybersecurity in smart grid-evaluation and review," in *2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE)*, Mar. 2022, pp. 1–6, doi: 10.1109/SGRE53517.2022.9774038.
- [12] K. Y. Chai and M. F. Zolkipli, "Review on confidentiality, integrity and availability in information security," *Journal of ICT In Education*, vol. 8, no. 2, pp. 34–42, Jul. 2021, doi: 10.37134/jictie.vol8.2.4.2021.
- [13] M. Pilz *et al.*, "Security attacks on smart grid scheduling and their defences: a game-theoretic approach," *International Journal of Information Security*, vol. 19, no. 4, pp. 427–443, Aug. 2020, doi: 10.1007/s10207-019-00460-z.
- [14] I. Alsmadi and F. Mira, "IoT security threats analysis based on components, layers and devices," *American Journal of Science & Engineering*, vol. 1, no. 1, pp. 1–10, Jun. 2019, doi: 10.15864/ajse.1101.
- [15] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239–247, 2021, doi: 10.1016/j.procs.2021.05.025.
- [16] B. Rossi and S. Chren, "Smart grids data analysis: a systematic mapping study," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3619–3639, Jun. 2020, doi: 10.1109/TII.2019.2954098.
- [17] A. A. Ismael, A. T. Younis, E. A. Abdo, and S. H. Hussein, "Improvement of non-linear power amplifier performance using doherty technique," *Journal of Engineering Science and Technology*, vol. 16, no. 6, pp. 4481–4493, 2021.
- [18] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Computers & Security*, vol. 84, pp. 225–238, Jul. 2019, doi: 10.1016/j.cose.2019.03.007.
- [19] F. Holik and J. Horalek, "Security principles of smart grid networks," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, no. 1–4, pp. 41–45, 2018.
- [20] A. Kumar and G. Somani, "Security infrastructure for cyber attack targeted networks and services," in *Recent Advancements in ICT Infrastructure and Applications. Studies in Infrastructure and Control*, Singapore: Springer, 2022, pp. 209–229.
- [21] S. H. Husain and A. I. Khuder, "Hardware realization of artificial neural networks using analogue devices," *AL-Rafdain Engineering Journal (AREJ)*, vol. 21, no. 1, pp. 77–87, Feb. 2013, doi: 10.33899/rengj.2013.67355.
- [22] E. Foruzan, L.-K. Soh, and S. Asgarpoor, "Reinforcement learning approach for optimal distributed energy management in a microgrid," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5749–5758, Sep. 2018, doi: 10.1109/TPWRS.2018.2823641.
- [23] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: a review," *Electronics*, vol. 9, no. 6, p. 1030, Jun. 2020, doi: 10.3390/electronics9061030.
- [24] A. Almalq and G. Edwards, "A review of deep learning methods applied on load forecasting," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Dec. 2017, pp. 511–516, doi: 10.1109/ICMLA.2017.0-110.
- [25] A. Estesari and R. Rajabi, "Single residential load forecasting using deep learning and image encoding techniques," *Electronics*, vol. 9, no. 1, p. 68, Jan. 2020, doi: 10.3390/electronics9010068.
- [26] S. You *et al.*, "A review on artificial intelligence for grid stability assessment," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Nov. 2020, pp. 1–6, doi: 10.1109/SmartGridComm47815.2020.9302990.




- [27] D. Kaur, R. Kumar, N. Kumar, and M. Guizani, "Smart grid energy management using RNN-LSTM: a deep learning-based approach," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013850.
- [28] S. Mavale, J. Katade, N. Dunbray, S. Nimje, and B. Patil, "Review of cyber-attacks on smart grid system," in *Proceedings of Third International Conference on Communication, Computing and Electronics Systems . Lecture Notes in Electrical Engineering*, Singapore: Springer, 2022, pp. 639–653.
- [29] M. Ahmed and A.-S. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, p. 4, Dec. 2020, doi: 10.1186/s40294-020-00070-w.
- [30] S. Oshnoei and M. Aghamohammadi, "Detection and mitigation of coordinate false data injection attacks in frequency control of power grids," in *2021 11th Smart Grid Conference (SGC)*, Dec. 2021, pp. 1–5, doi: 10.1109/SGC54087.2021.9664078.
- [31] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.
- [32] S. Blumsack, *Network topologies and transmission investment under electric-industry restructuring*. Carnegie Mellon University, 2006.
- [33] P. Hines, S. Blumsack, E. C. Sanchez, and C. Barrows, "The topological and electrical structure of power grids," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–10, doi: 10.1109/HICSS.2010.398.

## BIOGRAPHIES OF AUTHORS






**Marwah Ezzulddin Merza**    was born in 1986 in Mosul, Iraq, she received the B.Sc. degree from the University of Ninevah, Electronic Engineering Department in 2007. She finished her M.Sc. in Electronics from Mosul University, Iraq in 2012. His research interest in Intelligent Systems. She is now an Assist. lecturer in Mechatronics Engineering Department in Mosul university, Iraq. She can be contacted at email: mialabasy@uomosul.edu.iq.



**Shamil H. Hussein**    was born in 1984 in Mosul, Iraq, he received the B.Sc degree from the University of Mosul, Electrical Engineering Department at Electronic and Communication. He finished his MS.c in Electronics from Mosul University, Iraq in 2012. His research interest in Microelectronic, IC Design, RF power amplifier design, and Intelligent Systems. He is now a lecturer in Electrical Engineering Department in Mosul university, Iraq. He can be contacted at email: shamil\_alnajjar84@uomosul.edu.iq.



**Prof. Dr. Qutaiba I. Ali**    was born in Mosul City, Iraq on 1974. He received the BS and MS degrees from the Department of Electrical Engineering, University of Mosul, Iraq, in 1996 and 1999, respectively. He received his Ph.D degree (with honor) from the Computer Engineering Department, University of Mosul, Iraq, in 2006. Since 2000, he has been with the Department of Computer Engineering, Mosul University, Mosul, Iraq, where he is currently a full professor. His research interests include computer networks analysis and design, embedded network devices, and network security. He instructed many topics (for post and undergraduate stage) in computer engineering field during the last 20 years and has more than 93 different publications in world class indexed journals and conferences. He acquires many awards and appreciations form different parties for excellent teaching and extra scientific research efforts. Also, he was invited to join many respectable scientific organizations such as IEEE, IENG ASTF, WASET and many others. He was participating as technical committee member in more than 55 IEEE international conferences joined the TPC 10 scientific international journals. He can be contacted at email: qutaibaali@uomosul.edu.iq.