IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON IEEE POWER & ENERGY SOCIETY SECTION

Received 9 January 2023, accepted 19 January 2023, date of publication 25 January 2023, date of current version 3 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3239684

RESEARCH ARTICLE

Multi-Agent Distributed Deep Learning Algorithm to Detect Cyber-Attacks in Distance Relays

MEYSAM RAJAEE AND KAZEM MAZLUMI, (Member, IEEE)
Department of Electrical Engineering, Faculty of Engineering, University of Zanjan, Zanjan 45371-38111, Iran
Corresponding author: Meysam Rajaee (rajaeemeysamacademic@gmail.com)

ABSTRACT Distance relays are critical components in protection systems of power grids that can be attacked by cyber-attackers. Indeed, a cyber-attacker injects fake data into a distance relay to pretend a fault has happened, and the distance relay must be tripped. Thus, a new powerful approach, named Multi-Agent Distributed Deep Learning (MADDL) method is proposed to tackle cyber-attacks in distance relays. Unlike centralized methods, the protection system with several distance relays is mapped to a multi-agent distributed system by employing the graph theory, in which the distance relays are considered as the agents of the multi-agent system or the nodes of the considered graph. Each agent is only connected to the neighboring agents to exchange voltage and current data. Then, a deep neural network as a cyber-attack detection structure is assumed for each agent that utilizes the local voltage and current data and the received data from the neighboring agents to detect the attacks. Hence, the considered detection structures are tuned by employing train data, obtained by simulating the grid in different types of faults. Then, the tuned detection structures are evaluated by a test dataset, including data from the grid under various faults and the normal situation by injecting fake data as cyber-attacks. The developed method has been employed for three different case studies, including IEEE 6-bus, IEEE 14-bus, and IEEE 118-bus power grids. According to the simulation results, the proposed algorithm has succeeded in identifying more than 99.88% of faults and cyber-attacks.

INDEX TERMS Cyber-attack, distance relay, graph theory, multi-agent system, distributed system, deep neural network.

I. INTRODUCTION

Nowadays, power grids have changed from simple transfer networks into cyber physical platforms in which exchanging data plays a key role in these grids. Although a more dynamic power grid is being prepared due to high-speed communication services, the grids confront of serious security difficulties [1]. Regarding the security of smart grids, the National Institute of Standards and Technology (NIST) has introduced three essential principles, including confidentiality, integrity, and availability, which are vital for the management, operation, and protection systems, as well as the infrastructure of telecommunications [2]. On the other hand, one of the most important current problems related to the security of the power grid is cyber-attacks. Most cyber-attacks in grids are against three mentioned participles, which are described below:

- **Attacks against availability:** These attacks are usually carried out to prevent or delay the transmission of data [3], which are categorized under Denial of Services Attacks (DoS) [4].
- **Attacks against integrity:** These attacks are carried out to create deliberate changes or fake data in smart grids [5]. The main goal of these attacks is telemetered data, such as line flows, power injections, voltage and current measurements, and the data of switches and breakers, in smart grids, which can even lead to grid instability.
- **Attacks against confidentiality:** These attacks are also used to create unauthorized access by using fake identities [6]. In these attacks, the attacker gains access to an open-access field of MAC frame, threats as a healthy

The associate editor coordinating the review of this manuscript and approving it for publication was Qiang Li.

user and connects to other users and devices, and finally, sends fake information on the network [1].

Besides, substations are important infrastructure components in terms of security in power grids, which consist of critical assets. These critical assets include protection systems, circuit breakers, bus bars, transformers, etc. Although substations were limited in connecting with other components in the past, they currently easily exchange data due to technological advancements, such as developing the ethernet platforms, Intelligent Electronic Devices (IEDs), standardized protocols, and remote access controls. This communication progress in power grids has advantages, the most important of which include increasing the reliability in substations, needing less engineering efforts and costs, as well as reducing problems between different suppliers in power grids. However, with the presence of this technology, power grids confront new difficulties, the most important of which are security problems. Unfortunately, communication platforms have provided an opportunity for cyber-attacks on protection devices in power grids [7]. These cyber-attacks would lead to mis operations and malfunctions of protection systems, trip a relay mistakenly, and cascading outages or system collapse [8]. For example, consider an attacker who accesses the configuration of a distance relay and sets the setting of the relay for zone 1 to overreach to the next power line. The distance relay trips mistakenly and cut the line if a fault happens outside the zone distance of the relay [9]. Cyber-attacks in power grids even are able to lead to blackouts, causing irreparable damage, which proves the need of a reliable cyber security strategy in power grids, especially in substations.

The attack tree in substations demonstrates in Fig. 1. Regarding the attack tree, all cyber-attacks can be divided into two parts, including the attacks that happen on-site and with remote access. According to this figure, a distance relay can be attacked with both an inside attack or a remote access attack. An attacker can inject false data for measured voltage and current samples from inside of a substation. In addition, the communication network of a substation can be accessed by an attacker from an external network by a remote connection. Changing the setting of a distance relay is another scenario that is considered in the attack tree. Consequently, cyber-attacks in distance relays are possible.

In the following, some of the most important research in the cyber-attack field related to the power system and protection systems in the power grid will be studied. Firstly, cyber-attacks issue in power systems is introduced in 2011 [10], which became a serious challenge and a myriad research has been proposed so far. The necessity for reliable cyber-physical security in power systems was demonstrated by the Ukrainian power system cyber-attack [11], [12] and other real cyber-attacks. In recent research, the infrastructure of communication systems in power grids with respecting the cyber security is analyzed in [13]. In [14], the cyber security related to electric vehicle charging ecosystems is introduced and the impact of the growing the number of electric vehicles

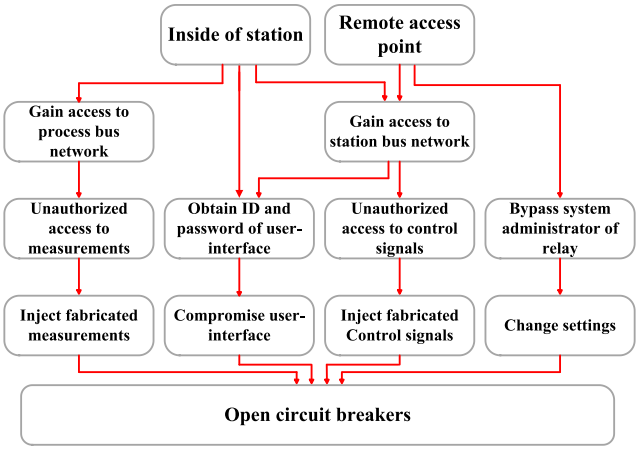

FIGURE 1. The cyber-attack tree.

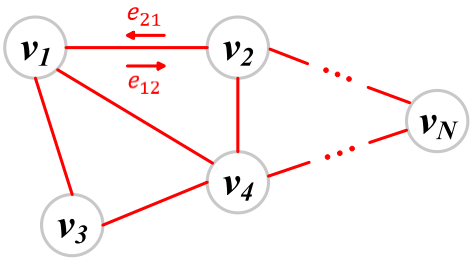

FIGURE 2. A direct graph.

on power grids is studied. Besides, a comprehensive integrated framework of modeling, simulation, and analysis of cyber-attacks is investigated in [15], which is finally reported various types of cyber-attack detection in power grids. In [16], a blueprint of reducing cyber security threats approach is introduced, trained technical personnel, evaluated the cyber-attack impacts, and tested the proposed approach. Another cyber security approach for integration systems of electric power systems and renewable energy sources is proposed in [17], which is developed a new deep reinforcement learning method. Moreover, a practical method for the vulnerability assessment of smart power grids is presented in [18].

In [19], a new platform is presented for the risk analysis of the protection aspect of the United States power grid in order to increase the cyber security of the grid. In addition, a new cyber security protection method is introduced in [20], which leads to identifying the most important components of power grid security. In [7], a new method is proposed to detect and tackle cyber-attacks on substations in power grids. In this regard, a new platform is introduced to collaborate the protection devices against cyber-attacks. Also, in [21] both energy losses and energy conservation are employed to develop a new false data injection in power system which has been cyber-attacked.

In this paper, a novel Multi-Agent Distributed Deep Learning (MADDL) method is proposed to tackle cyber-attacks on distance relays in power grids, regardless the configuration

of the power grid [22]. It is considered that an attacker has succeeded in injecting false data by one of the methods discussed above, and the proposed algorithm is going to detect the real voltage and current for each distance relay in the grid. In this regard, a power grid with some distance relays is assumed as a multi-agent system in which the distance relays are the agent of the considered system. Then, the graph theory is employed to model the power system with several distance relays as a multi-agent system in which the distance relays and related measurement transformers are supposed as the nodes of the graph or the agents of the multi-agent system. These agents can exchange data with their neighbors and estimate the real voltage and current by using both local voltage and current measurements and receiving voltage and current data from neighboring agents. It is worth mentioning that the connections in the multi-agent system are considered between the close agents geographically to each other to reduce connection costs. Then, the consensus control approach is employed to determine the true values for the voltage and current of each agent. In this respect, a deep neural network for each agent is utilized to estimate the true values by using all available data. In other words, a detector or estimator structure, including a deep neural network, is supposed to estimate the local voltage and current of the agent. Firstly, the deep neural networks of the agents should be trained. Thus, the grid should be considered in various situations, including the normal situation or under different faults. Consider a grid with n distance relays has m lines. All voltage and current data of n distance relays for different types of faults in different locations of each line are collected, for example, different types of faults for the m lines by 10% interval. Then, the considered deep neural networks for the agents are trained by the collected data. Finally, the trained detector structure is evaluated by new data that some data has changed as a cyber-attack.

Unlike conventional consensus approaches in multi-agent systems, the proposed algorithm has not any reference agent. Additionally, the proposed algorithm is developed as a distributed method due to some benefits, which are expressed below:

1) The calculations are divided and assigned to the agents. Hence, the speed of the algorithm will enhance.
2) Unlike centralized methods, the sensitivity of the connections in a distributed approach is low. In other words, the estimated voltage and current of an agent will be interrupted if the connection is interrupted. While the detection of real voltage and current signals in a distributed algorithm will not stop when a connection line is cut.
3) Although reducing the connections in MADDL algorithm is not proven, the speed of exchanging data will be increased by employing a distributed approach, since each agent is only connected to the neighbors. Whereas agents in a centralized method have to connect to a control center.

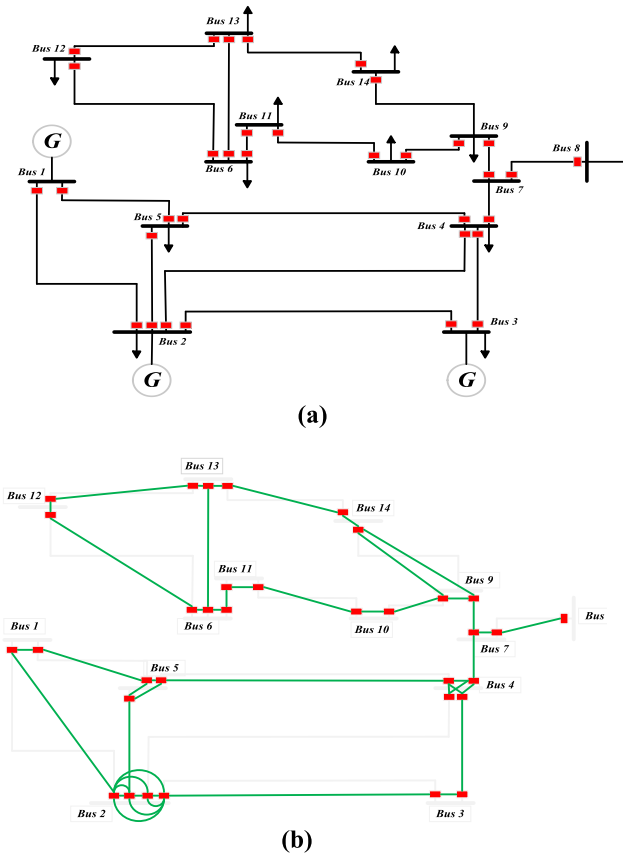

FIGURE 3. (a) the location of distance relays in the IEEE 14 bus power grid, and (b) the related algebraic graph with the distance relays as the nodes and their control connections as the edges.

4) Last but not least, distributed algorithms assist producer to protect the power system against cyber-attacks. Indeed, using a deep learning method based on a distributed multi-agent approach helps to propose a new powerful and practical method to tackle cyber-attacks in power grids.

The remainder of this research is organized as follows. Firstly, the proposed method is described in Section II. Simulation results of implementing the proposed method on standard power grids are analyzed in Section III. Ultimately, the conclusion is presented in Section IV.

II. METHODOLOGY

In this section, the proposed Multi-Agent Distributed Deep Learning (MADDL) algorithm is explained. Indeed, distance relays in a protection system of a power grid are supposed as the agents of a multi-agent system. These agents are connected to each other according to an equivalent graph, which the algebraic graph theory is introduced firstly. Besides, the proposed method is based on a distributed system in which the distance relays are the various parts of the distributed system. Hence, distributed systems are presented in the second subsection. Finally, the proposed method is described in the last subsection.

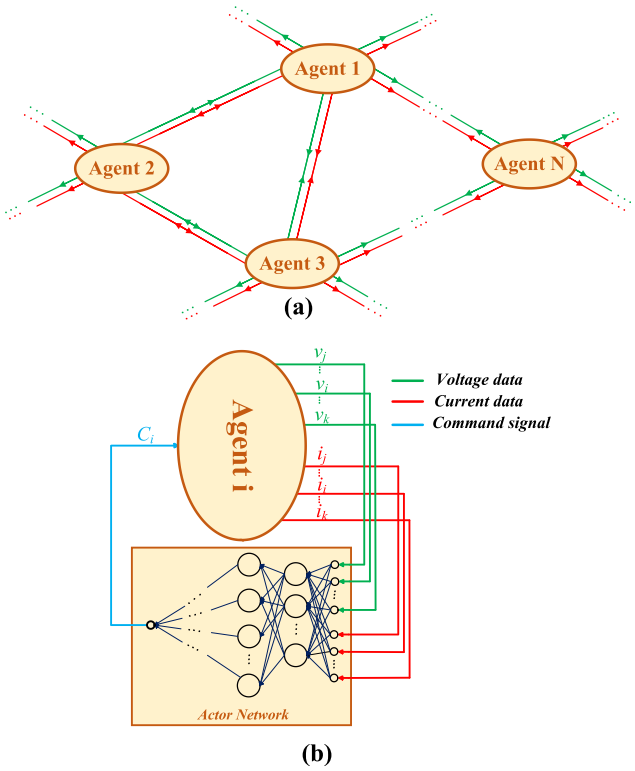

FIGURE 4. The proposed MADDL method, (a) a multi-agent system, (b) an agent of the multi-agent system with the attack detector system.

A. ALGEBRAIC GRAPH THEORY

Consider a direct graph, illustrated in Fig. 2, which is specified by $G = (V, E)$ and includes N nodes, demonstrated by $V = \{v_1, v_2, \ldots, v_N\}$, and the edges are shown as a set, $E = \{e_{ij}\} \in V \times V$. In set E, $e_{ij} = 0$ if there is no connection from the ith node to the jth node, and $e_{ij} > 0$ if a connection is established from the ith node to the jth node. Consequently, the in-neighbors and out-neighbors' concepts are easily defined. In-neighbors and out-neighbors for the ith node are indicated by (1) and (2), in turn.

$$N_i^{in} = \{j | e_{ji} > 0\}, \quad i = 1, 2, \ldots, N \tag{1}$$

$$N_i^{out} = \{j | e_{ij} > 0\}, \quad i = 1, 2, \ldots, N \tag{2}$$

In this graph, the value of e_{ij} in weighted graphs shows the weight from the ith node to the jth node. While in unweighted graphs, e_{ij} can be 1 or 0.

Distance relays of a power grid can be easily mapped to a direct graph in which the distance relays and the connections among them are considered as the nodes and the edges of the relevant graph, respectively. Thus, the nodes are assumed as the agents of a multi-agent system where the connections among the agents to exchange data are specified by the equivalent graph.

B. DISTRIBUTED SYSTEMS

Distributed systems usually are known as systems that include several separate components. These components can easily exchange messages or signals. In other words, a collection of autonomous computing components, seen as a unified system, is a distributed system. Thus, two main features of a distributed system can be expressed as follows [23]:

1) Distributed systems are collections of various separated components that can behave separately or depend on the other. This definition defines a component as either a hardware device or software.
2) In a distributed system, users confront a single system with unit goals. Therefore, components must collaborate.

Moreover, in computer science and engineering applications, distributed systems are systems with several parts that are geographically separated [23]. In power systems, distance relays work separately, while they are synchronized. Indeed, distance relays in the proposed method only are collaborated with neighbors, considered as components of a distributed system. Hence, according to graph theory, a power system with several distance relays can be mapped to a graph. In this graph, distance relays are the nodes and the control connections between them are considered as the edges. Each node connects only to its neighbors to reduce connection costs and also have more convenient cooperation. Besides, the defined distributed system is considered as a multi-agent system and the consensus control approach is employed to optimize the performance of the distance relays, which are the agents of the multi-agent system. In the next subsection, the proposed method is introduced in detail.

C. MULTI-AGENT DISTRIBUTED DEEP LEARNING METHOD

The proposed method, named Multi-Agent Distributed Deep Learning (MADDL) method, is introduced in this subsection to detect cyber-attacks in distance relays. A new proposed multi-agent distributed system is introduced in this paper in order to model the protection system of a power system. In the proposed method, a corresponding graph is assumed for the protection system that distance relays of the protection system are the nodes. The connections between the agents of the considered multi-agent system are optimized to minimize the connection costs. Moreover, a new policy is selected for the classification of the power grid's situations. In fact, the voltages and currents, measured by the neighboring agents, have been affected when a fault have happened in a line. Thus, the inputs of the classifier in each agent are the local and neighboring voltages and currents. Finally, a deep neural network is employed to provide a fast classifier that can classify with a huge number of data, received from neighboring agents.

Consider the distance relays in the IEEE 14-bus grid, illustrated in Fig. 3(a) in which the distance relays are highlighted in red color. Moreover, the corresponding graph is shown in Fig. 3(b) where the relays and the control connections among them are supposed as the nodes and edges of the graph, respectively. Considering more connections helps the algorithm to detect cyber-attacks more appropriately.

However, more connections impose more costs on the detection system.

Mapping the above graph to a multi-agent system provides an opportunity to employ the advantages of these system models and apply the consensus control approach to optimize the estimation in this system. Hence, the distance relays are considered as the agents of a multi-agent system in which the relations between the agents are the shown edges. In the proposed method, the calculation of the cyber-attack detection in each agent is assigned to themselves. In this regard, each agent receives the measured voltages and currents of the neighbors' agents. Then, the collected voltage and current signals, in addition to the local measured voltage and current, are used to detect the cyber-attack. In other words, when a fault happens in a power grid, most of the neighbor distance relays can sense the effect of the fault. Nevertheless, in cyber-attacks, the attacker can only inject fake data to one or in a worst case, a limit number of distance relays. Therefore, a cyber-attack is detected by analyzing the voltage and current signals of all the neighboring distance relays. In this respect, a deep neural network is employed for each agent to analyze the received data. Hence, a distributed method based on a multi-agent system will be proposed for the distributed plant in order to detect cyber-attacks in distance relays.

Firstly, the agents and their connections for the distance relays in the power grid should be specified so that each agent has enough number of connections. Then, a detection structure, including a data receiver from the connected agents, the local voltage and current measurement system, and a deep neural network for analyzing the data, should be considered for each agent. The deep neural networks of the agents must be tuned by the train data. In this regard, the voltage and current data of the power grid are collected in both the normal operation of the system and under various faults. In the fault situation, different types of faults, including symmetrical and asymmetric single-phase and three-phase faults, and for different locations in the power grid are assumed and their voltage and current data are collected. Then, the neural networks will be trained by the collected data. Finally, the trained networks should be evaluated. Hence, different data are employed to evaluate the cyber-attacks detection system for detecting faults in the power grid correctly. Moreover, some data for distance relays in normal situation are replaced by fault sample data to analyze the performance of the detection system against cyber-attacks. Fig. 4 indicates the proposed method. The agents are only connected with the neighbors, and as shown in Fig. 4(a), they are able to exchange both voltage and current data, demonstrated by $v_j, \ldots, v_i, \ldots, v_k$ and $i_j, \ldots, i_i, \ldots, i_k$, respectively. In the considered multi-agent system, it is assumed that the ith agent is only connected to a limit number of neighbor's agents, from the jth agent to the kth agent. In each agent, the received voltage and current data, as well as the local measured voltage and current, are utilized as the input of a deep recurrent neural network, shown in Fig. 4(b). The estimation of the system situation, which is an appropriate command signal for the distance relay, is the output of the deep neural network, shown by C_i for the ith agent.

An Artificial Neural Network (ANN) models the information process in humans' brains, establishing a non-linear model to present more appropriate behavior of real-world strategies [24]. Consider a simple feedforward neural network with the input and output layers and some hidden layers. The output of the jth node in the ith layer can be expressed as below:

$$y_j = f\left(\sum_{k=1}^{n} w_{kj} y_k - \theta_j\right) \tag{3}$$

where y_j and f (.) are the output and the activation function of the neuron, respectively, $w_{kj} \forall\, k = 1, 2, \ldots, n$ are the weights between the jth neuron and the neuron in the previous layer, $y_k \forall\, k = 1, 2, \ldots, n$ are the output of the neurons in the previous layer, and θ_j is the jth neuron's bias. The weights are adjusted to minimize the output error expressed in (4).

$$e = (y_d - y_{real})^2 \tag{4}$$

where y_d and y_{real} are the desired and real output of the neural network. Regarding the presented error, the weights are updated as:

$$w_{kj} \leftarrow w_{kj} - \gamma \frac{\partial e}{\partial w_{kj}} \tag{5}$$

In (5), γ shows the learning rate.

In a Recurrent Neural Network (RNN) a neural sequence model is considered, which is mostly utilized for time series data [25]. Indeed, an RNN used the current inputs and previous output. Thus, it can remember previous inputs and uses them to generate current output. Hence, the output value of the jth node in the ith layer can be calculated as follows:

$$y_j^{(t)} = f\left(\sum_{k=1}^{n} w_{kj} y_k^{(t)} + \sum_{f=1}^{m} w_{fj} h_f^{(t-1)} - \theta_j\right) \tag{6}$$

In this equation, t represents sample time, w_{fj} and $h_f^{(t-1)}$ are the weights between the jth neuron and the output layer and the output layer values in the $(t-1)$th time step. The other parameters have already been introduced.

III. RESULT AND DISCUSSION

In this section, the proposed algorithm is evaluated using different case studies. In addition, the performance of the algorithm is examined in terms of some aspects. Hence, the robustness of the algorithm against disconnecting some connections and the change of the algorithm's speed by expanding the power system will be studied.

The protection systems of power grids consist of several distance relays. A data exchanging system is considered in the proposed method in which the distance relays can receive the voltage and current data from other neighboring distance relays that are geographically close to the distance relay. Therefore, firstly, the equivalent graph determine which distance relays can exchange data with each other. Then, the

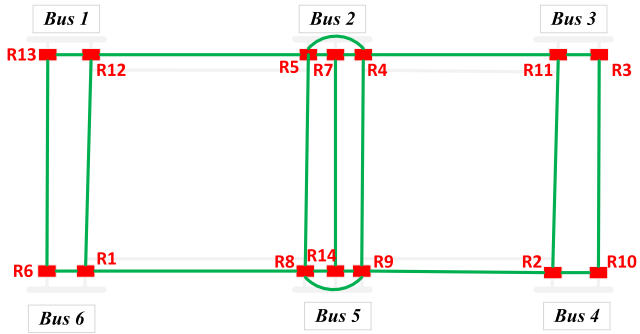

FIGURE 5. The equivalent graph for the protection system of the IEEE 6-bus power grid.

received current and voltage data and the local data measurement in each agent are utilized in the protection structure. Hence, the trained deep neural network for each agent excepts current and voltage data (received and measurements) to calculate the output, including normal, fault, or cyber-attack situations.

A. THE PROPOSED METHOD'S RESULTS FOR THREE CASE STUDIES

In this subsection, three grids, including the IEEE 6-bus, IEEE 14-bus, and IEEE 118-bus power grids as small, medium, and large power systems, respectively, are considered, and the proposed method of detecting cyber-attacks is tested on them. Consequently, all three power grids are put in both various faults and cyber-attacks situations, and the accuracy of the proposed cyber-attack detector for both fault and attack detections will be separately reported. It should be noted that each reported accuracy is the average of 20 repetitions of the estimation process by the proposed algorithm.

B. CASE STUDY I: IEEE 6-BUS POWER GRID

In the first case study, the IEEE 6-bus power system is supposed to evaluate the introduced MADDL method. In this regard, the equivalent graph for the IEEE 6-bus protection system with several distance relays are demonstrated in Fig. 5. In this figure, the agents and the connections among them are shown in red and green color, respectively.

According to Fig. 5, each agent (each relay) has a detection structure that illustrates in Fig. 4(b). The considered detection structure uses current and voltage data from the neighboring agents, as well as the local current and voltage measurements. For example, the neighboring agents for the 5^{th} agent, which is the 5^{th} relay (R_5), are the 4^{th}(R_4), 7^{th}(R_7), and 12^{th} (R_{12}) agents, which means the measured voltages and currents by the measurements in these relays, and the measured local voltage and current in the relay are used as the input of the considered detection structure for the 5^{th} agent. Hence, firstly, the train data for symmetrical and asymmetric various types of faults, including single line-to-ground, three phase line-to-ground, three phase line-to-line, and two-phase line-to-line faults, are collected by simulating the power grid in different situations. In these simulations, the location of fault is placed in different positions of the 7 available lines of the IEEE 6-bus grid by 10% interval. Hence, 505 different datasets are provided by simulating the supposed power grid in different situation of faults, which is prepared by 9(fault location in each line) × 7(number of lines) × 2(symmetrical and asymmetric faults) × 4(types of faults) + 1(normal state). Additionally, the algorithm needs some other data to evaluate. Thus, the mentioned simulation is repeated for different location of faults, by 5% interval in lines, which leads to 1065 sample data to test the trained detector. An attacker is willing to change the data to pretend that a fault has happened. Therefore, to simulate the cyber-attack situation for the proposed algorithm, the voltages and currents of some distance relays in the normal situation is replaced by the fault values of the same distance relays. Consequently, these data, including data in the both fault and cyber-attacks situations are utilized to evaluate the trained MADDL algorithm. The simulation results are expressed in TABLE 1.

TABLE 1. The obtained results for the IEEE 6-bus grid.

Accuracy / Dataset	Fault detection	Cyber-attack detection	Overall detection
Train dataset	%99.9433	%99.9284	%99.9401
Test dataset	%99.9207	%99.9005	%99.9186

Indeed, more than %99.91 of the test data is correctly detected. Looking at the results, the correct faults and cyber-attacks detection near the 4th and 6th buses are meaningfully detected more than others due to more neighboring agents in the multi-agent system. For instance, about %99.98 and %99.96 of the faults and cyber-attacks in the lines between the 1st and 6th buses and 4th and 6th buses are correctly detected, whereas only %99.85 of the faults and cyber-attacks in the lines between the 2nd and 5th buses are estimated correctly. In addition, the correct detections near the buses in each line are also more than the fault and cyber-attack detections that happen in the middle of the lines. In this regard, approximately %99.94 of the detections in the first and last 30% of the lines were correct. While only nearly %99.90 of the faults and cyber-attacks located from 30% to 70% of the lines are detected correctly.

C. CASE STUDY II: IEEE 14-BUS POWER GRID

As shown in Fig. 3(a), the IEEE 14-bus power grid includes 14 buses and 20 lines. Moreover, the corresponding algebraic graph is demonstrated in Fig. 3(b) in which the nodes (or agents) and edges (or connections) of the graph (or the multi-agent system) are highlighted in red and green color, respectively. The proposed method is employed for the considered power grid. In order to prepare train date, the simulation should be repeated for 1441 times, which is obtained by 9(fault location in each line) × 20(number of lines) × 2(symmetrical and asymmetric faults) × 4(types of faults) + 1(normal state). The algorithm is tuned by the train data and

TABLE 2. The obtained results for the IEEE 14-bus grid.

Accuracy / Dataset	Fault detection	Cyber-attack detection	Overall detection
Train dataset	%99.9182	%99.8902	%99.9141
Test dataset	%99.8863	%99.8637	%99.8811

TABLE 3. The obtained results for the IEEE 118-bus grid.

Accuracy / Dataset	Fault detection	Cyber-attack detection	Overall detection
Train dataset	%99.9614	%99.9488	%99.9595
Test dataset	%99.9560	%99.9418	%99.9523

TABLE 4. The average time required to estimate the situation for different dataset of three case studies.

Case study	Dataset	Time required (sec)
Case study I	Train dataset	1.264E-03
	Test dataset	1.259 E-03
Case study II	Train dataset	1.267E-03
	Test dataset	1.266E-03
Case study III	Train dataset	1.311E-03
	Test dataset	1.307E-03

evaluated by the test data, which are collected from both faults (%5 intervals) and cyber-attacks (injecting fake data into the normal situation) situations. TABLE 2 indicates the detection accuracy for both train and test datasets.

In this case, about %99.88 of faults and cyber-attacks are correctly estimated, and the distribution of the correct detections are similar to the IEEE 6-bus case study.

D. CASE STUDY III: IEEE 118-BUS POWER GRID

In the second case study, the proposed algorithm is used for the IEEE 118-bus grid and the obtained results will be analyzed. According to the previous argument, 118 buses and 186 lines of this grid leads to 13,393 different sets for train data, which is obtained by 9(fault location in each line) $\times$ 186(number of lines) $\times$ 2(symmetrical and asymmetric faults) $\times$ 4(types of faults) $+$ 1(normal state). Moreover, 28,273 sets are available in the test dataset. Similar results to the previous case studies are presented in TABLE 2.

E. THE SPEED OF THE ALGORITHM FOR DIFFERENT PROTECTION SYSTEMS

In this subsection, the speed of the proposed cyber-attack detection structure is examined. In this regard, the time required by each agent to estimate the situation for all three different case studies will be studied. In fact, it is expected that the time required by each agent does not increase as the grid expands due to the fact that each agent only connects to the neighbors. TABLE 4 illustrates the time average for the agents of three case studies when the estimation process has been repeated 20 times for each case study.

Independent of the largeness of the power grid, each agent only connects to a limit number of agents that are close geographically. Therefore, according to the results in TABLE 4, the time required does not grow by increasing the number of grid's bus from 6 to 14 and finally to 118 busses.

TABLE 5. The accuracy of the proposed detection structure for three case studies when 5% of connections are disconnected.

Case study	Dataset	Accuracy		
		Fault detection	Cyber-attack detection	Overall detection
Case study I	Train dataset	%99.9273	%99.9201	%99.9259
	Test dataset	%99.9191	%99.8907	%99.9135
Case study II	Train dataset	%99.9155	%99.8942	%99.9112
	Test dataset	%99.8820	%99.8546	%99.8788
Case study III	Train dataset	%99.9469	%99.9407	%99.9450
	Test dataset	%99.9535	%99.9399	%99.9501

F. ALGORITHM ROBUSTNESS AGAINST INTERRUPTION OF CONNECTIONS

Regarding the robustness of the proposed method against disconnecting the connections between agents of the multi-agent system, the estimation processes in Section III-A are repeated in this subsection. Indeed, it is possible to interrupt some connections of the considered multi-agent system in practice. Hence, approximately 5% of all connections in three different case studies are randomly selected to disconnect and the proposed algorithm is going to estimate the correct commands for the distance relays. TABLE 5 demonstrates the accuracy of the estimations by the proposed method when 5% of all connections are interrupted. It should be noted that the estimation process is repeated for 20 times and the average of the results are reported.

Looking the reported results in Section III, the minimum accuracy of detecting cyber-attacks and various faults in these three case studies is more than 99.88% for the test datasets, which proves the high performance of the proposed algorithm. Moreover, by comparing the three case studies, the time required of each agent to estimate the command signal does not increase by expanding the power grid. In this respect, the average time of each agent in 20 times of repeating the simulations for three case studies are equal to 0.0012, 0.0012, and 0.0013 seconds for Case study I, Case study II, and Case study III, in turn. Hence, the independence of the algorithm speed from the grid size as one of the most important advantages of the proposed algorithm is proven by the simulation results. Finally, the robustness of the algorithm against disconnection has been demonstrated so that the estimation accuracy has not changed significantly.

IV. CONCLUSION

Cyber-attacks in protection systems of power grids have become a critical problem, especially in the last decade. In this regard, some methods have been proposed so far,

whereas a practical and powerful method is still needed due to the weaknesses of the previous approaches. Thus, a new method, called Multi-Agent Distributed Deep Learning (MADDL) method, is proposed to tackle cyber-attacks in distance relays on power grids. Firstly, a communication network is established among the distance relays of a power system so that each relay is only connected to the neighboring distance relays. By mapping the introduced network to a multi-agent system, the relays and the communications among them are the agents and connections of the multi-agent system, in turn, which is also considered as a distributed system. Finally, cyber-attacks are estimated by analyzing the voltages and currents of the neighboring agents and local measurements. The calculation of the cyber-attack detections and creating the appropriate command signal for the distance relay for each agent is assigned to themselves. Besides, a deep neural network is employed to analyzed the collected voltage and current data. The proposed algorithm is utilized for three different case studies to detect cyber-attacks, faults, and normal situations on the power systems. The detection accuracy of cyber-attacks in these case studies were more than %99.88, which is demonstrated the high-performance of the proposed MADDL method. Although the need of the algorithm to data for tuning and a bit difficult implementation of the algorithm, the proposed algorithm has high quality performance in detecting the cyber-attacks and easily compatible with the expanding of power grids.

REFERENCES

[1] K. Chatterjee, V. Padmini, and S. Khaparde, "Review of cyber attacks on power system operations," in *Proc. IEEE Region Symp. (TENSYMP)*, Jul. 2017, pp. 1–6.

[2] G. Arnold, D. Wollman, G. FitzPatrick, D. Prochaska, D. Holmberg, D. Su, A. Hefner, Jr., N. Golmie, T. Brewer, M. Bello, and P. Boynton, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," Special Publication (NIST SP), National Inst. Standards Technol., Gaithersburg, MD, USA, 2010.

[3] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan. 2006.

[4] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[5] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–6.

[6] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2011.

[7] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2018.

[8] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout–root causes and dynamics of recent major blackouts," *IEEE Power Energy Mag.*, vol. 4, no. 5, pp. 22–29, Sep. 2006.

[9] Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541–2552, Jul. 2018.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.

[11] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[12] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," in *Proc. Electr. Inf. Sharing Anal. Center (E-ISAC)*, vol. 388, 2016, pp. 1–29.

[13] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021.

[14] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[15] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[16] M. Henze, L. Bader, J. Filter, O. Lamberts, S. Ofner, and D. van der Velde, "Cybersecurity research and training for power distribution grids—A blueprint," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 2097–2099.

[17] X. Liu, J. Ospina, and C. Konstantinou, "Deep reinforcement learning for cybersecurity assessment of wind integrated power systems," *IEEE Access*, vol. 8, pp. 208378–208394, 2020.

[18] T. N. Nguyen, B.-H. Liu, N. P. Nguyen, and J.-T. Chou, "Cyber security of smart grid: Attacks and defenses," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[19] S. S. Baggott and J. R. Santos, "A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid," *Risk Anal.*, vol. 40, no. 9, pp. 1744–1761, 2020.

[20] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures," *Int. J. Crit. Infrastruct. Protection*, vol. 18, pp. 20–33, Sep. 2017.

[21] X. Fu, G. Chen, and D. Yang, "Local false data injection attack theory considering isolation physical-protection in power systems," *IEEE Access*, vol. 8, pp. 103285–103290, 2020.

[22] X. Fu, Q. Guo, and H. Sun, "Statistical machine learning model for stochastic optimal planning of distribution networks considering a dynamic correlation and dimension reduction," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 2904–2917, Jul. 2020.

[23] L. Kleinrock, "Distributed systems," *Commun. ACM*, vol. 28, no. 11, pp. 1200–1213, 1985.

[24] M. T. Hagan, H. B. Demuth, and M. Beale, *Neural Network Design*. Boston, MA, USA: PWS, 1997.

[25] D. Yogatama, C. Dyer, W. Ling, and P. Blunsom, "Generative and discriminative text classification with recurrent neural networks," 2017, *arXiv:1703.01898*.

MEYSAM RAJAEE was born in Zanjan, Iran, in 1991. He received the B.Sc. degree in electrical engineering from the University of Zanjan, in 2013, and the M.Sc. degree from the Amirkabir University of Technology, Tehran, in 2016. He is currently pursuing the Ph.D. degree with the University of Zanjan. His research interests include power system protection and high voltage technology.

KAZEM MAZLUMI (Member, IEEE) was born in Tehran, Iran, in 1976. He received the B.Sc. degree in electrical engineering from the Amirkabir University of Technology, Tehran, in 2000, the M.Sc. degree from the Sharif University of Technology, Tehran, in 2003, and the Ph.D. degree from the Amirkabir University of Technology, in 2009. He is currently an Associate Professor with the University of Zanjan, Zanjan, Iran. His research interests include power system protection, power system transients, and smart power grids.