IoT in Smart Grid: Energy Management Opportunities and Security Challenges

Motahareh Pourbehzadi, Taher Niknam, Abdollah Kavousi-Fard, Yasin Yilmaz

IoT in Smart Grid: Energy Management Opportunities and Security Challenges

Motahareh Pourbehzadi[1,2][0000-0002-9063-591X] Taher Niknam[1][0000-0001-7439-3183] Abdollah Kavousi-Fard[1][0000-0001-8316-5588] and Yasin Yilmaz[2][0000-0001-9445-5927]

[1] Department of Electrical Engineering, Shiraz University of Technology, Shiraz, Iran, 71557-13876
m.pourbehzadi@sutech.ac.ir; Niknam@sutech.ac.ir; Kavousi@sutech.ac.ir

[2] Department of Electrical Engineering, University of South Florida, Tampa, Florida, 33620
mpourbehzadi@mail.usf.edu; yasiny@usf.edu

Abstract. This study is focusing on presenting an online machine learning algorithm that benefits from sequential data of IoT devices in the smart grid. This method provides the smart grid operator with the historical data of generation units of a smart grid that is connected to the IEEE 33-bus test system. The proposed smart grid consists of two photovoltaic cells, two wind turbines, a microturbine, a fuel cell and an electric car the behaviour of which is considered similar to that of a storage unit. In the training phase, the optimized generation units' data is used to form a regressive model of every unit's behaviour. Afterwards, the model is used to predict the behaviour of every unit in the next 24 hours. The optimized operation data is used to solve the optimal power flow (OPF) problem. The output of OPF is useful in monitoring the stability of the smart grid, calculating power losses and locating possible faults. Moreover, the proposed framework benefits from the online discrepancy test (ODIT) method, which uses the data of the machine learning method to form a baseline for anomaly detection. The advantage of this method is that it minimizes false alarms and it eliminates false data in anomaly detection. The implementation of the proposed solution methodology has proven to be effective in regards with execution-time reduction and accuracy.

Keywords: Energy Management, IoT, Machine learning, Microgrid, Security.

1 Introduction

1.1 Background

Since the 21st century, the advancements in electronic communication technology have resolved most of the technical and economic limitations of the electric grid. This is the distinction between an electric grid and a smart grid. A smart grid is an electric grid that benefits from a communication infrastructure among its constituting units; i.e. smart meters, smart appliances and renewable energy resources [1]. Thus, finding the optimal energy dispatch of the generation units is a great matter of concern. Several studies have introduced different solution methodologies in this regard. It is a known fact that

meteorological phenomena i.e. wind speed and solar irradiation have a sequential pattern. Historical analysis of other smart grid components such as electric load and market price show that they also have sequential behavior. Therefore, machine learning algorithms have turned into a popular choice for predicting the behaviour of the aforementioned units/ aspects of the smart grid. Figure 1 present the increasing trend in the popularity of addressing IoT-related security issues in smart grids.

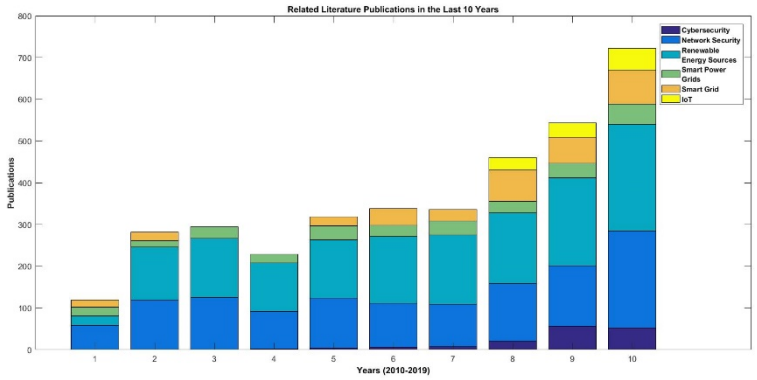

Fig. 1. Related Literature Publications in the Last 10 Years

A smart IoT-based grid is subject to various security challenges such as impersonation, eavesdropping, data tampering, availability and denial of service issues, etc. [2]. Since IoT devices are vulnerable to cyber-attacks the main problem that needs to be addressed is: "what if the IoT devices' data in the smart grid is hacked/ manipulated?" This justifies the existence of adversarial machine learning algorithms. If the manipulated data is not detected through a reliable and quick mechanism, the repercussions can inflict economic and technical cost to the smart grid. That is why addressing security issues in smart grids have been a popular topic in recent years. In [3] the authors used wide and deep convolutional neural networks to analyze the periodicity and non-periodicity in electrical energy consumption. The findings of this study have been used in anomaly detection (electricity theft) of a smart grid. In the study presented in [4] the availability of fine-grained time series data has been introduced as a game changer at the distribution systems level. This issue has prevented effective application of complex machine learning algorithms on grid operation. In this paper, the deep generative adversarial network (GAN) is introduced for learning the conditional probability distribution of real datasets. Article [5] presents adversarial machine learning, whereby models are fooled through malicious input, either for financial gain or to cause system disruption. This paper has presented simulation results that show the effect of adversarial machine learning on the operation of smart energy systems and has proposed directions for future research related to detection and defense mechanisms for such attacks. In [6] it is described that detecting False Data Injection (FDI) attacks by current bad data detection systems is impossible. Ergo, three various supervised learning techniques are presented, the accuracy of which are tested on the IEEE 14-bus, IEEE 57-bus and IEEE 118-bus test systems. The authors of [7] have proposed a new metric for the smart grid that is called the entropic state. This metric has two main purposes. First, it provides an indication of the grid's health on cycle-to-cycle basis. Second, it can be

used to detect FDI attacks. The idea of this paper comes from the mentality of addressing state estimation in smart grids and cognitive dynamic systems at the same time.

The aforementioned literature review along with other studies lead us to the conclusion that in regards to adversarial machine learning you can take two main approaches. 1) Designing a robust machine learning algorithm and 2) Detecting attacks and mitigating them. The latter provides us from benefiting current machine learning techniques and is the general approach that has been taken into account. In this study, a regressive model has been introduced to substitute the time-consuming and off-line optimization method that is widely used for energy management in smart grids. Afterwards, the output of this model is given to the OPF solver to gain the power loss and voltage diagram of the main network. The security of the proposed framework is guaranteed using the online discrepancy test (ODIT). The distinction of this method lies within the fact that it eliminates false data, thus avoiding adversarial machine learning while minimizing false alarms.

.

1.2 Contributions

The present study has major contributions in regards to optimized operation and the OPF of smart grids. The outline of the contributions can be mentioned as follows:

- Presenting an online machine learning regressive method to find the optimized energy dispatch of a microgrid
- Presenting a machine learning based method for addressing the OPF problem
- Avoiding adversarial machine learning using the ODIT

The rest of the paper is organized as follows. In section 2, the problem formulation is stated. Section 3 covers the solution framework implementation. Finally, the concluding remarks can be found in section 4.

2 Problem Formulation

This section presents the operation cost minimization formulation and its associated constraints. The formulation is valid for a 24-hour period and the proposed MG is consisted of a MT, a FC, two PVs, two WTs, a BAT and the main grid.

2.1 Cost Function

The cost function of the proposed MG is formulated as described in equation (1). Equations (1a-1j) express the detailed value of each term in equation (1):

$$F(X) = M(\sum_{t=1}^{T} \mathrm{Cost}) = \sum_{t=1}^{T} (Cost_{Winds}^{t} + Cost_{PVs}^{t} + Cost_{FC}^{t} + Cost_{MT}^{t} + Cost_{BAT}^{t} + Cost_{Grid}^{t}) \quad (1)$$

$$= M\Big(\sum_{t=1}^{T}\Big([\sum_{a=1}^{N_{WTs}} P_{WTs_a}^t \times Bid_{WTs_a}^t] + [\sum_{b=1}^{N_{PVs}} P_{PVs_b}^t \times Bid_{PVs_b}^t] +$$

$$[\sum_{c=1}^{N_{FC}} u_c^t \times P_{FC_c}^t \times Bid_{FC_c}^t + SU_{FC_c} \times u_c^t \times (1-u_c^{t-1}) + SD_{FC_c} \times u_c^{t-1} \times (1-u_c^t)] +$$

$$[\sum_{d=1}^{N_{MT}} u_d^t \times P_{MT_d}^t \times Bid_{MT_d}^t + SU_{MT_d} \times u_d^t \times (1-u_d^{t-1}) + SD_{MT_d} \times u_d^{t-1} \times (1-u_d^t)] +$$

$$[\sum_{e=1}^{N_{Bat}} Max(u_e^t, 0) \times P_{BAT_e}^t \times Bid_{BAT_e}^t] + P_{Grid}^t \times Bid_{Grid}^t)\Big)$$

$$X = [P_g, U_g]_{1\times n} \tag{1a}$$

$$n = [2 \times (N_{MT} + N_{FC}) + N_{BAT} + 1] \tag{1b}$$

$$P_g = [P_{Grid}, P_{BAT}, P_{FC}, P_{MT}] \tag{1c}$$

$$U_g = [U_{FC}, U_{MT}] \tag{1d}$$

$$P_{Grid} = [P_{Grid}^1, \dots, P_{Grid}^T] \qquad T \in \{1, \dots, 24\} \tag{1e}$$

$$P_{BAT} = [P_{BAT_1}, \dots, P_{BAT_e}]$$
$$P_{BAT_e} = [P_{BAT_e}^1, \dots, P_{BAT_e}^T] \qquad e \in \{1, \dots, N_{BAT}\} \tag{1f}$$

$$P_{FC} = [P_{FC_1}, \dots, P_{FC_c}]$$
$$P_{FC_c} = [P_{FC_c}^1, \dots, P_{FC_c}^T] \qquad c \in \{1, \dots, N_{FC}\} \tag{1g}$$

$$P_{MT} = [P_{MT_1}, \dots, P_{MT_d}]$$
$$P_{MT_d} = [P_{MT_d}^1, \dots, P_{MT_d}^T] \qquad d \in \{1, \dots, N_{MT}\} \tag{1h}$$

$$U_g = [u_{c_1}^1, u_{c_1}^2, \dots, u_{c_1}^T, \dots, u_{c_{N_{FC}}}^1, \dots, u_{c_{N_{FC}}}^T, u_{d_1}^1, u_{d_1}^2, \dots, u_{d_1}^T, \dots, u_{d_{N_{MT}}}^1, \dots, u_{d_{N_{MT}}}^T] \in \{0,1\} \tag{1i}$$

$$U_E = [u_{e_1}^1, u_{e_1}^2, \dots, u_{e_1}^T, \dots, u_{e_{N_{BAT}}}^1, \dots, u_{e_{N_{BAT}}}^T] \in \{-1,0,1\} \tag{1j}$$

2.2 Constraints

Considering the above formulation, X denotes the decision variables' vector, which is mainly consisted of two elements. The first element is that is constituted from the grid, battery, fuel cell and micro turbine's power. Note that since the renewable energy sources are not dispatchable; meaning that the main aim is to benefit their output power the most, they are not being considered as decision variables. The next element of the

decision variable vector is Ug specifying the ON/OFF status of the fuel cell and micro turbine. One of the other coefficients in (1) is Uet, defining the battery charge status. This variable is equal to -1, when the battery is discharging and it equals 1 during the charging process. In order to demonstrate the battery state when the battery is neither being charged nor discharged, Uet equals zero. Note that the term SU/SD denotes the startup/shutdown cost of the MT or FC depending on the index. Also here, "a" denotes number of WTs, "b" is for number of PVs, "c" denotes number of FCs, "d" is for MTs and "e" stands for BAT numerator.

The main constraints that are associated with the proposed MG optimized operation are analyzed in this section. The most important constraint in this problem is the power balance constraint as described below:

- **Power/Load Balance Constraint**

The load and supply balance equation is considered as the major constraint that must be fulfilled. This constraint is formulated as equation (2):

$$\sum_{a=1}^{N_{WTs}} P_{WTs_a}^t + \sum_{b=1}^{N_{PVs}} P_{PVs_b}^t + \sum_{c=1}^{N_{FC}} u_c^t \times P_{FC_c}^t + \sum_{d=1}^{N_{MT}} u_d^t \times P_{MT_d}^t + \sum_{e=1}^{N_{Bat}} Max(u_e^t, 0) \times P_{BAT_e}^t + P_{Grid}^t = \sum_{f=1}^{N_{LOAD}} P_{Load}^t - \sum_{e=1}^{N_{Bat}} Min(u_e^t, 0) \times P_{BAT_e}^t \quad (2)$$

- **Battery Constraint**

The utilization of energy storage systems in the proposed MG leads to some constraints that are mainly associated with the batteries' state of charge (WtBAT), the charge/discharge rate (Pch/dch), their corresponding boundaries and the batteries' efficiency (η). These constraints are described in equations (3-8):

$$W_{BAT}^t = W_{BAT}^{t-1} + \eta_{ch} \times P_{ch}^t \times time - \frac{1}{\eta_{dch}} \times P_{dch}^t \times time \quad (3)$$

$$W_{BAT_{e,\min}} \leq W_{BAT_e}^t \leq W_{BAT_{e,\max}} \quad (4)$$

$$P_{ch}^t \leq P_{ch,\max} \quad (5)$$

$$P_{dch}^t \leq P_{dch,\max} \quad (6)$$

$$P_{ch}^{t} = Max(u_{e}^{t}, 0) \times P_{BAT_e}^{t} \tag{7}$$

$$P_{dch}^{t} = -Min(u_{e}^{t}, 0) \times P_{BAT_e}^{t} \tag{8}$$

The limitations on the maximum and minimum levels of output powers of the fuel cell, the micro turbine, the grid and the battery must be taken into account, as described in equations (9)-(12).

$$u_{c}^{t} \times P_{FC_{c,min}}^{t} \leq P_{FC_c}^{t} \leq u_{c}^{t} \times P_{FC_{c,max}}^{t} \tag{9}$$

$$u_{d}^{t} \times P_{MT_{d,min}}^{t} \leq P_{FC_c}^{t} \leq u_{d}^{t} \times P_{MT_{d,max}}^{t} \tag{10}$$

$$P_{Grid,min}^{t} \leq P_{Grid} \leq P_{Grid,max}^{t} \tag{11}$$

$$u_{e}^{t} \times P_{BAT_{e,min}}^{t} \leq P_{BAT_e}^{t} \leq u_{e}^{t} \times P_{BAT_{e,max}}^{t} \tag{12}$$

3 Solution Implementation

3.1 Machine learning substitution for optimization algorithm

Classical operation of microgrids is usually performed via solving the optimal dispatch of the system whilst considering the constraints explained in section 2. Figure 2 illustrates the traditional chronology of microgrid operation.

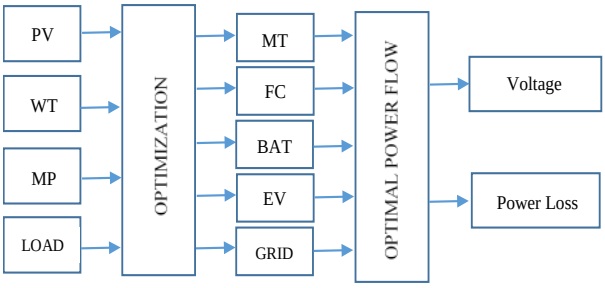

Fig. 2. Traditional microgrid operation

In this study, we have utilized the output of a solution methodology called the bird mating optimization (BMO) algorithm. The fundamental of this algorithm is based on the mating of birds. Male or female birds choose their elite mate or mates based on a series of preferences. This mating behaviour is scored in a descending order and it will be considered as the fitness function of the algorithm of the initial population. Detailed description of the BMO algorithm can be found in [8]. After implementing the BMO algorithm on the proposed microgrid and analyzing the results, it came to the authors' attention that the temporal behaviour of different units can be considered as training data for a regression-based supervised machine learining algorithm. Therefore, the optimization section in figure 2 was substituted with the machine learning algorithm.

The distribution of various constituting units of the microgrid on the IEEE 33-bus test system is illustrated in figure 3.

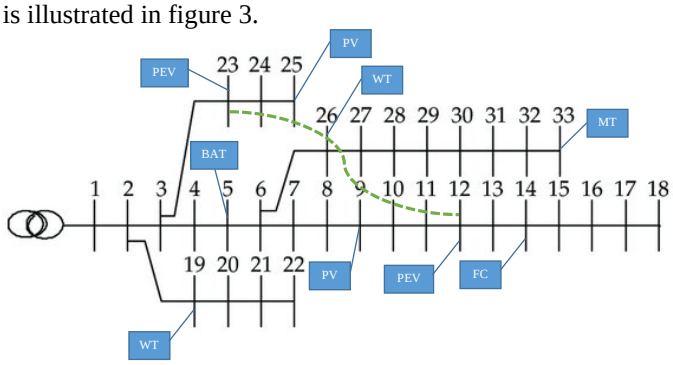

Fig. 3. Proposed microgrid topography

Considering the constraints of buses and lines in figure 3, it is obligatory that the OPF problem be solved for the IEEE 33-bus test system. Note that the dotted line illustrates the traveling path of the electric vehicle. Similar to the observations of the BMO algorithm, the OPF output has a temporal response as well. Ergo, the output data can be used to train another supervised machine learning algorithm to substitute the OPF calculations. It must be noted that the main motive for such substitutions lies within the fact that the traditional methods have two main deficiencies: 1) their performance is dependent on the initial population and 2) The computational complexity of these solutions is very high.

3.2 Online Discrepancy Test

It is a known fact that IoT devices are vulnerable to cyber attacks. The main question is: how can we avoid the manipulated data in machine learning? two main approaches can be taken: 1) Designing a robust machine learning algorithm and 2) Detecting attacks and mitigating them. The latter provides us from benefiting current machine learning techniques and is the general approach that has been taken into account. In this study, a regressive model has been introduced to substitute the time-consuming and offline optimization method that is widely used for energy management in smart grids. Afterwards, the output of this model is given to the OPF solver to gain the power loss and voltage diagram of the main network. The security of the proposed framework is guaranteed using the online discrepancy test (ODIT). Detailed description of the ODIT can be found in [9]. The distinction of this method lies within the fact that it eliminates false data, thus avoiding adversarial machine learning while minimizing false alarms. The final scheme of the proposed operational framework is illustrated in figure 4.

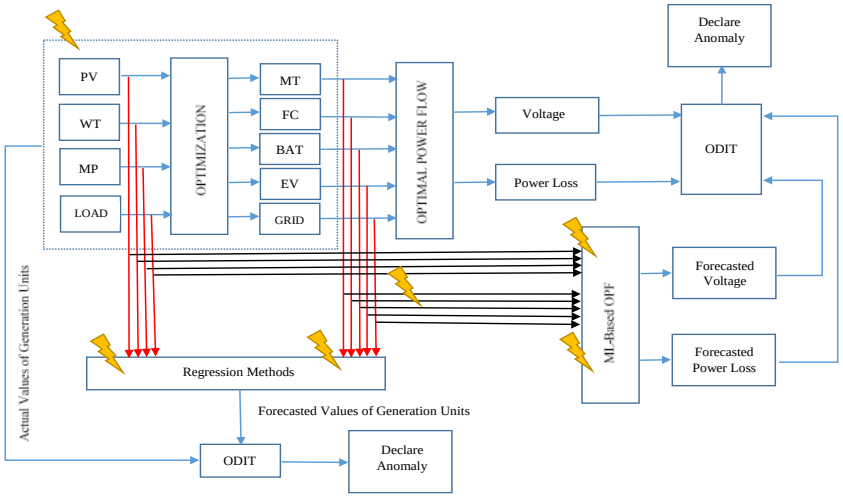

Fig. 4. Final operation scheme of the proposed ML-based framework

There are two important factors in regards to the final scheme of the system as illustrated in figure 4. 1) Both the optimization and OPF sections have substituted via regression methods. 2) The ODIT is used to declare any possible anomalies. The yellow surge signs in figure 4 show the possible parts of the scheme that can be subject to cyber attacks. The attack can occur in the optimization or OPF section, which supplies the training data for the regression method or it can occur on the system after the machine learning substitution. In either case, the ODIT's strategy is to get constant feedbacks from the actual values and the forecasted values and make a decision on the existence of anomalous activities using a cumulative criterion [9].

4 Conclusion

With the emergence and development of telecommunication technologies, a new generation of electric grid has been born; i.e. "the smart grid". Smart grids have facilitated several energy management limitations of classic grids. In this regard, two main points must be taken into consideration:

- The repetitive patterns of renewable energy resources such as solar irradiation and wind speed can be modeled using a regressive machine learning technique. Furthermore, other aspects that form the energy management of smart grid have a sequential pattern. For example the energy price and load demand are lower in the beginning and at the end of the day while they both have peaks sometime around noon. This justifies the usage of machine learning algorithms as a substitute for current off-line meta-heuristic algorithms that require high number of iterations to converge to the global optimal operation point.

- The security aspects of machine learning- based models in IoT systems. If the machine learning algorithm is fooled with false or manipulated data, then the final output of the computations will be false. This can lead to serious financial or even life-threatening consequences. In order to address this issue it is necessary to provide an anomaly detection method that is both quick and reliable.

Finally, The findings of this work can be summarized as follows:

We presented an online machine learning algorithm to substitute the optimized operation and optimized power flow of a smart grid. The benefits of using machine learning algorithms in energy management of smart grids can be reflected in addressing computational complexities in: 1)Time: Reducing the operation time and anomaly detection time. 2)Space: Real-life systems are large-scaled and solving the optimization problem for a grid-connected smart grid is mathematically complex.

We introduced an online anomaly detection method to detect and mitigate cyber attacks to IoT devices in smart grid so that: 1) the false alarms are minimized. 2) The false data is eliminated.

References

1. Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R.M. and Srivastava, G., 2019. Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet of Things*, p.100111.
2. Bekara, C., 2014. Security issues and challenges for the IoT-based smart grid. Procedia Computer Science, 34, pp.532-537.
3. Zheng, Z., Yang, Y., Niu, X., Dai, H.N. and Zhou, Y., 2017. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Transactions on Industrial Informatics, 14(4), pp.1606-1615.
4. Zhang, C., Kuppannagari, S.R., Kannan, R. and Prasanna, V.K., 2018, October. Generative adversarial network for synthetic time series data generation in smart grids. In 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 1-6). IEEE.
5. Bor, M., Marnerides, A., Molineux, A., Wattam, S. and Roedig, U., 2019. Adversarial Machine Learning in Smart Energy Systems.
6. Sakhnini, J., Karimipour, H. and Dehghantanha, A., 2019. Smart Grid Cyber Attacks Detection using Supervised Learning and Heuristic Feature Selection. arXiv preprint arXiv:1907.03313.
7. Oozeer, M.I. and Haykin, S., 2019. Cognitive Dynamic System for Control and Cyber-Attack Detection in Smart Grid. IEEE Access, 7, pp.78320-78335.
8. Askarzadeh, A., 2013. Parameter estimation of fuel cell polarization curve using BMO algorithm. International Journal of Hydrogen Energy, 38(35), pp.15405-15413.
9. Mozaffari, M. and Yilmaz, Y., 2019, October. Online Anomaly Detection in Multivariate Settings. In *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)* (pp. 1-6). IEEE.