4th International Conference on Knowledge-Based Engineering and Innovation (KBEI-2017)
Dec. 22th, 2017
(Iran University of Science and Technology) – Tehran, Iran

The Effect of Cyber Attacks on the Demand Dispatch Application and Identify Them by OPTICS

Farid Fathnia, Fatemeh Daburi Farimani, Froogh Fathnia, Mohammad Hossein Javidi Dasht Bayaz
Department of Electrical Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
Farid.fathnia@mail.um.ac.ir
Tel Number: +98-915-6848608

***Abstract*— With the growing trend of emerging technologies and the global concern for increasing greenhouse gas emissions from fossil fuels, the concept and implementation of smart grids over the past few years have been presented. According to the American National Technology and Energy National Laboratory, the intelligent network must have some features such as self-healing, energy efficiency, smart management, penetration of renewable energy sources, and so on. These features make the future power grid a highly complex network of cyber-physical aspects and propose some demanding requirements in the information infrastructure of the new generation power grids. Some of these requirements are 1- the rapid response to faults, errors and cyber-attacks 2- extensive information management 3- data security and 4- more efficient management of energy sources. The purpose of this paper is to examine and analysis the aforementioned features in the smart grid besides each other. In this regard, we will show the effects of cyber-attacks on smart meter' data as well as the losses that can influence the demand dispatch programs, and finally detect them based on the density-based OPTICS algorithm using LOF index. The proposed system is an off-grid network that consists of wind turbines, solar system, diesel generator and battery, and its customers which have some dispatchable and non-dispatchable loads that are connected by intelligent meters to the control center. In order to simulate the proposed method, the actual wind energy and solar energy data obtained from the NREL laboratory climate database are used. The results will show for two general modes that are Demand Dispatch program with and without cyber-attack to smart meters' data.**

Keywords—Cyber-Attack; Microgrid; OPTICS; Demand Dispatch; Anomaly Detection; Renewable Energy

I. INTRODUCTION

The current and future changes in distribution networks are such that the typical operating system seems to be incapable of answering the optimal response to network requirements. Some of these changes are as follows: 1- increasing the sensitivity of loads to price changes 2- increasing penetration of distributed renewable sources such as wind and solar 3- the presence of electric vehicles in the network, and 4- intelligent control processes in the operation of the network. There are two major challenges in this typical chosen operating approach. At first, from a design point of view, the random nature of production and energy consumption of these resources is a challenging problem in the current method of grid operation. If this approach of operation, changes, not only will not be considered as a challenge, but also will be optimally solved. In the current operation approach called generation dispatch (GD), for the purpose of balancing generation and consumption, the operation process is designed in which generation will follow the consumption of electrical loads. This overall approach can be somewhat modified and applied at the level of the distribution grid. In this regard, the general idea of the Demand Dispatch (DD) is raised to operate such resources. With regard to the expansion of power grid intelligence, for these sources, the reverse approach, that is, the following of dispatchable loads from generation, which is called Demand Dispatch, is suggested. Thus, the commonly used GD approach is limited to typical network loads and its concurrent and focused generic production, and DD is related to demanding dispatchable loads and variable and distributed network generation. Therefore, DD is complemented by an economical GD for optimal network utilization. This emerging operation approach has been addressed with the overall objectives of reducing operating costs, optimizing the use of available assets on the demand side and addressing the challenges posed by distribution networks [1].

Demand Dispatch approach was introduced for the first time in 2010 [2]. In this paper after defining the Demand Response (DR) concept and pointing to the advancement in communication and control technologies, it thinks the Demand Dispatch a new look of DR and expresses the differences between the two concepts and also some requirements of the Demand Dispatch program clearly. The simulation of smart charging in electric vehicles is presented as an example of Demand Dispatch program in this paper. In the reference [3], the influence of DD, and the use of Wind Power Forecasting (WPF) method on the expansion of the wind energy contribution in the smart grid has been investigated. Then, it calculates the various costs of operation (fuel, commissioning, etc.), load disconnection, reserve and wind production, the amount of generation of various power plants and the effect of using DD program in a number of scenarios. The details of the WPF method are given by the authors of this article in reference [4]. Then, using the WPF method, the modification of the planning

model in the unit commitment application (UC) in reference [5] is discussed. In [1], which is our main reference for simulation of this research, and its equations have been assisted, it consider a microgrid including wind turbines, solar cells, diesel generators, batteries and shiftable and non-shiftable loads. By examining the simulation results, including the dispatch command and the loading rate of diesel generator and storage, it is shown that the diesel and storage capacity required to support the uncertain generation of wind and solar will be reduced due to the participation of dispatchable loads.

The next major challenge is about privacy of customers' data transmitted to the control center. Since the onset of the smart grid, the risks and security threats have increased dramatically both inside and outside of the system and in this respect, intelligent metering data has steal control over other rivals. One of the uses of smart meters installed at the customers' site is to detect anomalies and analyze them. Because power distribution systems are subject to dangers, faults, failures and a lot of disturbances and abnormalities. Here we assumed that cyber-attackers can tamper the data of customers. Therefore, the detection of abnormalities and outlier data can be considered an effective way to maintain the security of the smart network, especially on the customers' side. There has been a lot of research in this area. Studies in this field is divided into 4 general categories [6]. 1- Consumption analysis 2- Destructive and security attacks 3- Fault Location 4. Detection of anomalies. In [7-8], machine learning methods are used to detect abnormalities. A review of the methods for analyzing consumption and intelligent data management is presented in [9].

The overall goal of this research is to model and implement the DD application at the level of a smart microgrid. Due to the lack of a specific structure for DD, At first we try to provide a simple model for this application and the problem of minimizing the cost of grid operation as an optimization problem, and it is applied on a hybrid off-grid system, consisting of wind turbines, solar panels, diesel generators and storage modules. Then, by creating a simulation of cyber-attacks in the consumer information, analyzing the effect on the DD program and showing the losses that could occur, is on the agenda. These losses will affect the overall cost. Then, in order to prevent this destructive attempt, we will try to implement a new method based on the data density to identify the anomaly created on the customer side of the smart meter data. For this purpose, the OPTICS (Ordering Points To Identify the Cluster Structure) method [10] is used and, by using the LOF (Local Outlier Factor) index [11], we will improve the performance of this algorithm. It is worth noting that all the modeling of Demand Dispatch program is inspired by the paper [1].

The rest of this paper is organized as follows: Section II talks about the modeling of the system. It is an off-grid microgrid system that consists of wind turbines, solar panels, batteries, diesel generators and shiftable and non-shiftable loads. In Section III, the problem-solving method will be expressed. In this section, both the DD program and the anomaly detection scheme in smart meter data will be presented. The results of the simulations will be shown in Section IV and finally Section V summarizes the contents.

II. SYSTEM MODELING

As shown in Fig. 1, the system is composed of wind turbines, solar panels, diesel generators and storage devices. The number of customers is 20. The loads of each customer are classified into two dispatchable and non-dispatchable categories. The consumer is assumed to plan for each of his controllable loads for the next day. Thus, the charging time of the desired load, instead of being used at the same moment as the connection to the outlet, declares to be acceptable on its own opinion within a given time limit. Here, the length of the time range is 6 hours, and the beginning of the range can only be at one of the hours: 24, 6, 12, and 18 P.M [1]. It should be noted that we have taken all dispatchable loads into one account. All of this delivery and receipt of scheduling and consumption intervals is assumed to be possible through the communication lines between the smart meters and the control center. Below is a modeling of the microgrid components. More detailed information about wind and photovoltaic systems and datasheets can be seen in reference [12]. Geographic information and weather conditions are also obtained from [12] which are related to NREL Laboratory. At the end we will model the customers and cyber attackers.

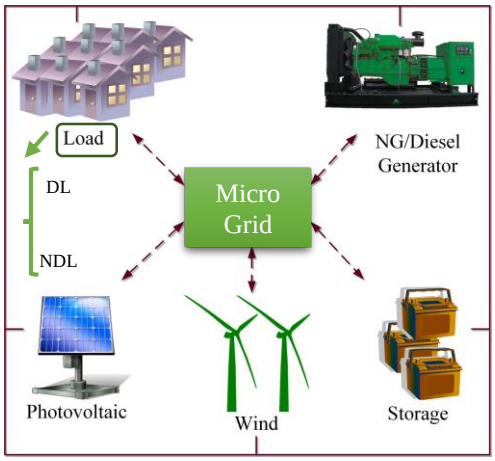

Figure 1 -Microgrid System with Dispatchable and Non-Dispatchable Loads

A. Photovoltaic Panel Modeling

$$P_{pv}(t) = Y_d \frac{I_G(t)}{I_S}\left[1 - \frac{K_P}{100}(T_C(t) - T_{STC})\right] \quad (1)$$

Where Y_d is derating factor due to dust accumulation (%), I_s is standard radiation (1 kWh/m2), K_p is Power temperature coefficient (%/◦C), and T_{STC} is cell temperature at standard test condition (STC) which is 25°C. The actual output power of photovoltaic panel is calculated by multiplying P_{pv} to nominal power of the panel [13].

B. Wind Turbine Modeling

$$P(t) = \begin{cases} 0, & if\ v(t) < v_{ci}\ or\ v(t) > v_{co} \\ \frac{v^3(t) - v_{ci}^3}{v_r^3 - v_{ci}^3}, & if\ v(t) > v_{ci}\ and\ v(t) < v_r \\ 1, & if\ v(t) > v_r\ and\ v(t) < v_{co} \end{cases} (2)$$

Where V_{ci}, V_r and V_{co} are cut-in, rated and cut-out speeds of the wind turbine [13].

C. Diesel Generator and Battery Modeling

Modeling these components in the next section will be presented as an optimization constraint for the DD program.

D. Customer Modeling

As already mentioned, the number of customers is 20. Each customer has two non-dispatchable and dispatchable energy features. For non-dispatchable energy, these 20 values are generated by MATLAB by randomly adopting a probability distribution function with an average of 40 and a variance of 0.9. Also, the dispatchable power consumption is also calculated by the probability distribution function with the mean of 5 and the variance 0.8. The sum of the non-dispatchable energy consumptions in this deterministic scenario is 1506 KWh and this value for dispatchable energy is 102.75 KWh. For each 6-hour interval, these numbers are equal to 195, 750, 475, and 86 KWh. It is worth noting that the controllable load connection is automatically and remotely operated by the grid operator at the optimal time. As stated, the consumer will have to choose one of the time periods and wait for the auto-activation of his device within that time frame. In fact, the participation in the DD application in comparison of the other various consumption management programs is consumer beneficial issue, and there is no need for constant attention to the price of electricity and direct control by himself. In terms of energy costs, due to the goal of minimizing the cost by the operator, his device will be largely less costly.

E. Cyber-Attack Modeling

In the case of modeling cyberattacks, it is assumed that the first, thirteenth and eighteenth customers are assaulted, so that the attackers applied the FDI (False Data Injection) attack [14] on the data sent by these customers to the control center, which is a dispatchable and non-dispatchable energy consumption. This attack follows the Modification mode, which is one of the four common security threats available [14]. The basis of this attack is that it reduces the amount of dispatchable energy to the target customers, and instead reduces the difference from their non-dispatchable energy. Thus, the total amount of energy consumed by each subscriber remains constant. Increasing the dispatchable energy of each customer means that the number of home appliances that do not require immediate access to them and are more controllable is more, and thus makes it annoying for customers to not be able to use their essential equipment at a given moment. The disadvantages that occur in the overall cost of the grid operation are shown in Section 4.

Below, the modeling of the various components mentioned is depicted.

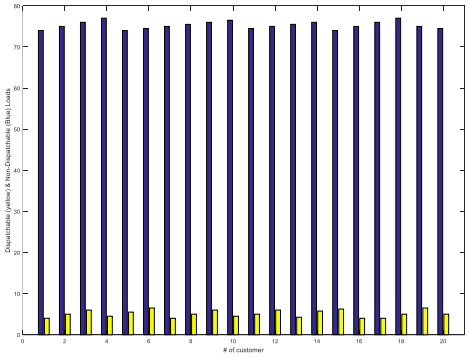

Figure 2 -Modeling Customers' Loads in Normal Mode

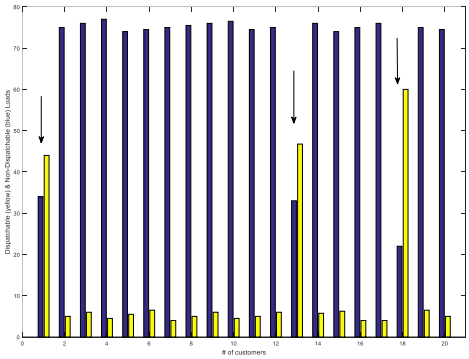

Figure 3 -Modeling Customers' Loads in Attack Mode

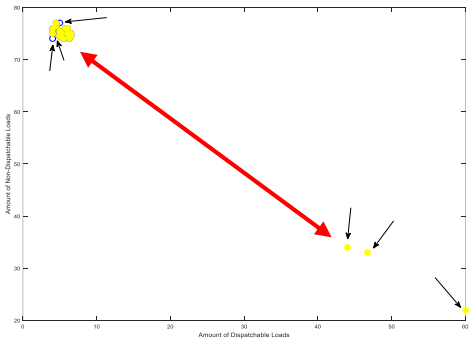

Figure 4 -2-D Plot of Customers' Consumption in Attack Mode

In Figures 2 and 3, respectively, the bar graph of dispatchable and non-dispatchable uses for every 20 consumers,

in normal mode and in the event of a cyber-attack, is presented. As can be seen, in Figure 3, the attacker changes the information of the 3 customers mentioned before. For this the dispatchable load data will be increased and non-dispatchable load data will be reduced with the same value to make identifying the attack with more difficulty. In Figure 4, each point represents the information of a customer, drawn in the 2-dimensional space in the coordinate axis. The vertical axis refers to the non-dispatchable load and the horizontal axis to the dispatchable load of each customer. The two normal and attack modes are shown, respectively, with an empty blue circle and a yellow solid circle.

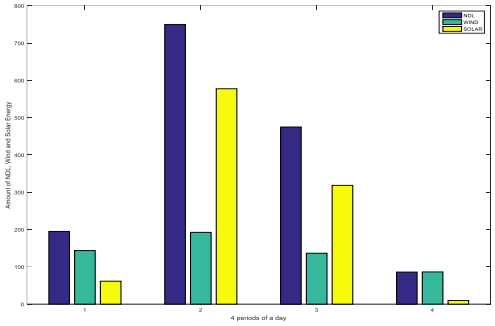

Figure 5 -Comparing Wind and Solar Energy with Non-Dispatchable Loads

In Fig. 5, the values of wind energy and solar energy, along with the amount of non-dispatchable (NDL) loads, are depicted in the four desired periods of the day. As can be seen, in some intervals, the energy produced by renewable sources is greater than the energy of non-dispatchable loads.

III. SOLVING PROCEDURE

In this section, first, the formulation of the DD application and then the anomaly detection algorithm are presented.

A. Demand Dispatch Formulation

The objective function of the operator's view is to minimize the cost of operation in accordance with equation 3 [1]. In this regard, the first sentence relates to the cost of diesel generator generation over a full day. The second sentence of the objective function, the Energy Not Supplied (ENS) cost, and lack of power at the first time interval of the next day is due to a shortage of stored energy at the end of the current day. In mathematical terms, the second sentence is the final cost of the planning period, which is intended to coordinate sequential planning periods. Other minor operating costs are discounted in comparison to diesel fuel costs. In this regard, $E_{Di,\,i}$ is the total amount of energy that diesel generator should produce on the basis of the command received from the operator, in the first interval. The cost of operating diesel in $/KWh, is shown with C_{Di}. C_{NS} the cost of non-supplied loads at the beginning of next day is due to low storage costs at the end of the current day. The coefficient represents the probability that the load will not be loaded, the high values of that will increase the amount of charge in the storage, at the end of the day. $E^*_{St,imax}$ Coefficient is the maximum amount of rechargeable storage capacity at the end of the current day [1].

$$O.F.: \quad Min \sum_{i=1}^{i_{max}} E_{Di,i} C_{Di} + \alpha E^*_{St,imax} C_{NS} \tag{3}$$

$$E_{Di,i} + E_{pv,i} + E_{W,i} - E_{st,i} - E_{DL,i} - E_{NDL,i} = 0 \tag{4}$$

$$\sum_{i=1}^{i\ max} E_{DL,i} = E_{DL,max} \tag{5}$$

$$E_{Di,min} \le E_{Di,i} \le E_{Di,max} \tag{6}$$

$$E^*_{St,i} = E^*_{St,i-1} - E_{St,i} \tag{7}$$

$$0 \le E^*_{St,i} \le E_{St,max} \tag{8}$$

$$-(E_{St,max} - E^*_{St,i-1}) \le E_{St,i} \le E^*_{St,i-1} \tag{9}$$

Equations 4 to 9 show the constraints of optimization problem. The balance of production and consumption is considered in accordance with equation 4. The total energy of dispatchable loads should be equal to the maximum energy of dispatchable loads during the day. This point is presented in equation 5. The maximum and minimum limits of power generated by diesel generator are considered in equation 6. Equation 7 is responsible for updating the amount of initial charge storage per interval. Equation 8 states that the rechargeable capacity at the beginning of the minimum interval can be zero. Equation 9 shows the permitted range of the amount of storage control command [1].

B. Anomaly Detection Algorithm

Statistical and distance-based outlier detection both depend on the overall or global distribution of the given set of data points. However, data are usually not uniformly distributed. These methods encounter difficulties when analyzing data with rather different density distributions. This brings us to use density-based methods to detect anomalies. For this we use the OPTICS (Ordering Points To Identify the Clustering Structure) algorithm introduced in [10]. The innovation of this research is the use of this method in the discussion of the problem of detecting anomalies of smart meter data, which is being discussed for the first time, and also covers the weaknesses of other density-based methods. Also, in this paper, the number of input parameters of this method, which is in general 2 items, is reduced to 1 in order to reduce the complexity of the problem. To improve the efficiency of the methodology, we use the index called LOF (Local Outlier Factor), Which is actually a factor in detecting the unusual nature of the data in the density-based methods, and will do this based on the score given to it [11].

1) Core- Distance

Let p be an object from a database D, let ε be a distance value, let $N_\varepsilon(p)$ be the ε-neighborhood of p, let $MinPts$ be a natural number and let $MinPts - distance(p)$ be the distance from p to its $MinPts$' neighbor [10]. Then the core-distance of p is defined as $core - distance_{\varepsilon,MinPts} =$

$$\begin{cases} UNDEFIEND, & if\ Card\big(N_\varepsilon(p)\big) < MinPts \\ MinPts - distance(p), & otherwise \end{cases} \quad (10)$$

Where Card(N) denotes the cardinality of the set N which indicates the neighboring point of interest given ε [10].

2) Reachability-Distance

Let p and o be objects from a database D, let $N_\varepsilon(p)$ be the ε-neighborhood of o, and let $MinPts$ be a natural number [10]. Then the reachability-distance of p with respect to o is defined as $reachability - distance_{\varepsilon,MinPts}(p,o) =$

$$\begin{cases} UNDEFINED, & if\ |N_\varepsilon(o)| < MinPts \\ \max\big(core - distance(o), distance(o,p)\big), & otherwise \end{cases} \quad (11)$$

3) K-Distance

The k-distance of an object p is the maximal distance that p gets from its k-nearest neighbors. This distance is denoted as k -distance (p). It is defined as the distance $d(p,o)$ between p and an object $o \in D$, such that for at least k objects, $ó \in D$ it holds that $d\big(p, ó \le d(p,o)\big)$ [10].

4) K-Distance Neighborhood

The k-distance neighborhood of an object p is denoted $N_k(p)$. By setting k to $MinPts$, we get $N_{MinPts}(p)$. It contains the $MinPts$-nearest neighbors of p. That is, it contains every object whose distance is not greater than the $MinPts$-distance of p [10].

5) Local Reachability Density

The local reachability density (lrd) of p is the inverse of the average reachability density based on the $MinPts$-nearest neighbors of p. It is defined as [11]:

$$lrd_{MinPts}(p) = \frac{|N_{MinPts}(p)|}{\sum_{o \in N_{MinPts}(p)} reachability - distance_{MinPts}(p,o)} \quad (12)$$

6) Local Outlier Factor

The local outlier factor (LOF) of p captures the degree to which we call p an outlier. It is defined as [11]:

$$LOF_{MinPts}(p) = \frac{\sum_{o \in N_{MinPts}(p)} \frac{lrd_{MinPts}(o)}{lrd_{MinPts}(p)}}{|N_{MinPts}(p)|} \quad (13)$$

IV. RESULTS

The capacity of different microgrid components and other parameters of the problem are presented in Table 1. Simulation of the whole article was done by MATLAB software. The results of the simulation of the linear optimization problem are presented in two scenarios.

Table 1 -Input Parameters

Parameters	Values
$E_{Di,max}$	60 KWh
$E_{DL,max}$	102.75 KWh
$E_{St,max}$	40 KWh
$E^*_{St,0}$	20 KWh
α	0.5
C_{NS}	2 $/KWh
C_{Di}	0.25 $/KWh

1) Normal Mode

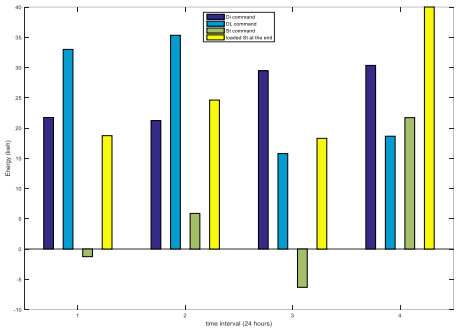

Figure 6 -Microgrid Components' Control Command in Normal Mode

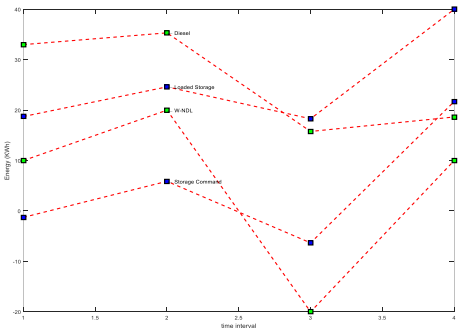

Figure 7 -Microgrid Components' Control Command in Normal Mode

In Figures 6 and 7, the optimal command of diesel generator operation, dispatchable loads and storage device is shown. It is worth noting the yellow bar graph in each interval, indicates the level of energy stored in the battery. As predicted, in the third period due to lack of wind and solar power to support non-dispatchable loads, the diesel generator is in the huge loaded level and the storage is also being discharged. In the second interval, the storage is being charged. The reason for this is the high non-dispatchable loads at this time.

Table 2-Normal Mode Features

Ratio of maximum storage loading command to nominal capacity	Ratio of maximum diesel loading command to nominal capacity	Total operation cost
55%	56%	25.562 $

From Table 2 we find that the most storage loading command is about 55% of its nominal capacity. In the case of diesel generator, it is about 56% of its nominal capacity. This means that with the DD application, the need for storage and the diesel generator has been reduced to support the stochastic production of a microgrid renewable sources.

2) Attack Mode

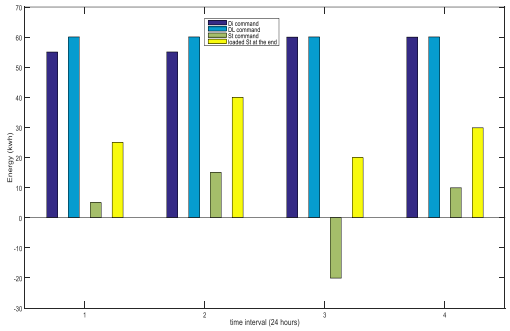

Figure 8 -Microgrid Components' Control Command in Attack Mode

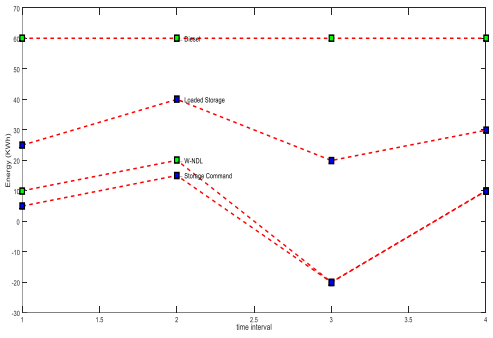

Figure 9 -Microgrid Components' Control Command in Attack Mode

The information in this scenario is presented in Table 3. This table shows that despite the fact that the storage loading command has been reduced to its nominal capacity, the diesel generator is at its maximum at all four intervals, which in turn requires a high operating cost, which results in a much higher overall cost of operation. And, as previously mentioned, it reduces the welfare of customers due to scheduling change. It is therefore necessary to identify these anomalies caused by cyber-attackers.

Table 3-Attack Mode Features

Ratio of maximum storage loading command to nominal capacity	Ratio of maximum diesel loading command to nominal capacity	Total operation cost
37.5%	100%	67.656 $

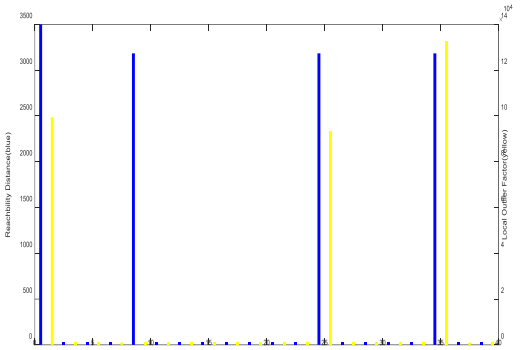

Figure 10 -LOF vs. RD for Customers

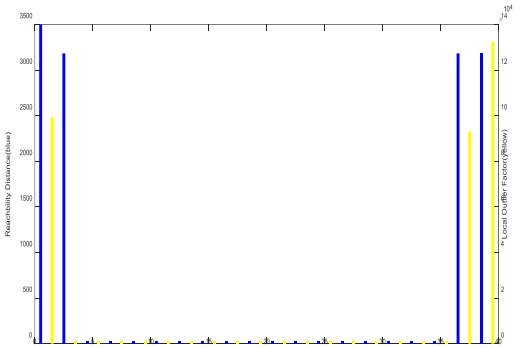

Figure 11 -LOF vs. RD for Customers when Ordering

As shown in Fig. 10, the algorithm was able to detect three attacked customers; the first, thirteenth, and eighteen by calculating the LOF index for all of them. This diagnosis is shown by the yellow bar chart. The blue bars also refer to the quantity of reachability distance for each customer. It can be seen that for all the attacked customers, this index is also very large and determines them, but for the fifth customer it also takes a large amount, which is because the mentioned point in the two-dimensional space of Fig. 4 (Red Arrow), is far from the first point, the algorithm has been initiated. Since the first point is one of the attacked points, this point also has a large amount of LOF, but in general, the algorithm's starting point takes a big value of reachability distance to form a cluster structure, which is the goal of the OPTICS method. Therefore, consideration of both indicators alone is not acceptable. A point is considered to be abnormal, since both indicators are much larger in size than other points. Be careful here that the only input parameter is

Minpts, and the rational choice of this number helps in the process of better identifying abnormalities.

In Fig. 11, these two indicators are also plotted for customers in the decreasing and incremental trend of reachability distance. This is due to implement the structure and the valley shape of this curve. As can be seen, the attacked customers are located at the end of this graph, and if the first attacked customer was not the starting point of the algorithm, it would definitely be at the end of the graph too.

V. CONCLUSION

In this paper, the purpose of the study is to analyze the impact of cyber-attacks on load management programs in the smart grid, and tried to finally identify these abnormalities by providing a model based on the density of available data in the 2-D space, and finally reducing the harmful economic consequences, and social repercussions for these attacks on both sides of the consumer and network management. For this purpose, an off-grid microgrid was used. This microgrid includes solar panels, wind turbines, storage, diesel generator, and customers' loads are divided into two groups of dispatchable and non-dispatchable loads. Then, using the Demand Dispatch (DD) algorithm, the linear optimization problem was solved in both normal condition and the attack condition, and to avoid losses caused by attackers, the improved OPTICS algorithm by the LOF index, is presented. The results indicate that this method can be effective if the input parameter of this algorithm is selected correctly. All simulations of this article are done by MATLAB software.

In order to continue this research, we need to provide a more detailed and comprehensive model of the DD application. Anomaly detection algorithm should be performed in different scenarios and the microgrid should be connected to the main grid for realistic conditions and including electricity market.

REFERENCES

[1] F. Daburi Farimani and H. Rajabi Mashhadi, "Effect of Demand Dispatch on Operation of Smart Hybrid Energy Systems," Power System Coneferance (PSC), 2013.

[2] A. Brooks, E. Lu, D, Reicher, C. Spirakis, and B. Weihl, 'Demand Dispatch," IEEE Magazine on Power and Energy, vol. 8, no. 3, May 2010.

[3] A. Botterud, Z. Zhi, W. Jianhui, J. Sumaili, H. Keko, j. Mendes, R.J. Bessa, and V. Miranda, "Demadn Dispatch and Probabalistic Wind Power Forecasting in Unit Commitment and Economic Dispatch: A Case Study of Illinois," IEEE Transactions on Sustainable Energy, vol. 4, issue. 1, pp. 250-261, Jan. 2013.

[4] C. Monteiro, R. Bessa, V. Miranda, A. Botterud, J. Wang, and G. Conzelman, "Wind Power Forecasting," State-of-the-art 2009, ANL/DIS-10-1 Argonne National Laboratory, Nov. 2009.

[5] J. Wang, A. Botterud, R. Bessa, H. Keko, L. Carvalho, D. Issicaba, J. Sumaili, and V. Miranda, " Wind Power Forecasting Uncertaintly and Unit Commitment," Appl. Energy, vol. 88, no. 11, pp. 4014-4023, 2011.

[6] R. Moghaddass and J. Wang, "A Hierarchial Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data," IEEE TRANSACTIONS ON SMART GRID, April 2017.

[7] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in Ami Using Customers' Consumption Patterns," IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216-226, 2016.

[8] C. Cernazanu-Glavan and M. Marcu, "Anomaly Detection Using Power Signature of Consumer Electrical Devices," Advanced in Electrical and Computer Engineering, vol. 15, no. 1, pp. 89-94, 2015.

[9] V. Ford, A. Siraj, and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," In IEEE Symposium on Computional Intelligence Applications in Smart Grid, CIASG, January 2015.

[10] M. Ankerst, M. Breunig, H. Peter Kriegel, and J. Sander, "OPTICS: Ordering Points To Identify the Clustering Structure," In Proceedings of ACM SIGMOD'99, Institude of Cimputer Science, University of Munich, Germany, 1999.

[11] J. Han and M. Kamber, Data Mining: Concepts and Techniques, ELSEVIER Inc, 2nd Edition, 2006.

[12] F. Fathnia, N. Yektay, M.H. Javidi Dasht Bayaz, R. Khalili, "Optimum Design for a Hybrid System with Respect to Cost and Reliability Based on Stochastic Methods," 25th Iranian Coneference on Electrical Engineering (ICEE), 2017.

[13] R. Atia and N. Yamada, "Sizing and Analysis of Renewable Energy and Battery in Residential Microgrid," IEEE Transactions on Smart Grid, vol. 7, issue. 3, pp. 1204-1213. Jan. 2016.

[14] W. Wang and Zh. Lu, "Cyber Security in the Smart Grid: Survey and Challenges," Elesevier, Computer Networks, no. 57, pp. 1344-1371, 2013.

KBEI-2017
DEC. 22, 2017

MINISTRY OF I.C.T
ISLAMIC REPUBLIC OF IRAN

Unified
ACADEMY OF INNOVATION
NEW ZEALAND

IEEE Xplore®
Digital Library

CERTIFICATE OF PRESENTATION

This is to certify that

Farid Fathnia, Fatemeh Daburi Farimani, Froogh Fathnia, Mohammad Hossein Javidi Dasht Bayaz

Has participated in **2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI),** held on Dec. 22, 2017, at Iran University of Science and Technology, Tehran, Iran and Orally Presented the paper entitled:

"The Effect of Cyber Attacks on the Demand Dispatch Application and Identify Them by OPTICS"

Dr. Behrouz Minaei Bidgoli
Scientific Committee Chair

Iran University of Science and Technology

Location:
Iran University of Science and Technology,
Hengam St., Resalat Sq., Tehran, Iran,
Postal Code: 16846-13114
website: www.kbei.ir, Email: info@kbei.ir

ID No: KBEI-0257
Code: HN-02540305