Tabriz Journal of Electrical Engineering (TJEE), vol. 54, no. 3, Autumn 2024 Serial no. 109
DOI: 10.22034/tjee.2023.57914.4685

A Cyber Secured optimal scheduling framework for AC microgrids based on dragonfly optimization and deep learning

Ali Heidary[1], Reza Eslami[2,*]

[1]Electrical Engineering Faculty, Sahand University of Technology, Tabriz, Iran
[2*]Electrical Engineering Faculty, Sahand University of Technology, Tabriz, Iran
eslami@sut.ac.ir
[*]Corresponding author

Received: 20/08/2023, Revised:22/10/2023, Accepted: 27/12/2023.

Abstract
Smart grid is a cyber-physical system, a combination of physical devices and computational processes. Enhancing interaction between the cyber and physical layers is crucial for optimizing system operation, management, and security. Motivated by this, in this paper, a framework for solving the optimal scheduling of an AC-microgrid (ACMG) system, is presented. The optimal scheduling of the system is modelled as an optimization problem. Also, the dragonfly is utilized as a powerful optimization technique to solve the proposed optimization problem. On the other side, considering cyber-attacks as a great threat to the system which can cause disruption and outage in smart grids, a deep-learning-based method, long short-term memory (LSTM), along with the concept of prediction interval is utilized to develop a cyber-attack detection model for false data injection attacks on smart meters. In this structure, the optimization is carried out using dragonfly optimization. Also, the LSTM, which is a subset of recurrent neural networks, is designed. With an accuracy of 97%, this model can ensure the cyber-security of the structure. Furthermore, to demonstrate the excellence of the proposed method, it is compared to an Artificial Neural Network (ANN). As the results show, the deep learning LSTM approach outperforms the ANN method in terms of accuracy and cyber-security. The proposed cyber-attack detection model is first trained using historical data and then is used in real-time conditions. For investigating the effectiveness of the proposed approach, the modified IEEE 33-bus test system is utilized. The results significantly show the effectiveness of the proposed methodologies.

Keywords
Optimal scheduling, False data injection attacks, AC microgrids, Dragonfly optimization technique, Practical swarm optimization.

1. Introduction

By increasing the awareness of the environmental impacts and global energy development, the use of smart grids as a modernized electrical network for optimal operation, low network losses, and improved reliability has become a key action in the power system. These systems contain several microgrid (MG) at the distribution level. MG, Known as a low voltage and self-organized electricity distribution system, includes various dispatchable loads, distributed generation units, and different energy storage and conversion technologies. Although the MG can be beneficial to the power system in many ways (i.e., facilitating the implementation of renewable sources, improving reliability, reducing operation costs, decreasing greenhouse emissions, etc.), they are complicated cyber-physical systems that have various challenges in terms of operation. The physical layer of MG mainly includes legacy devices such as transmission lines, FACT (flexible ac transmission system) devices, protection equipment, etc. The cyber layer includes communication and data aggregation platforms such as smart metering devices, data aggregators, etc. In this regard, it is vital to consider MG as a cyber-physical system and address challenges associated with both layers simultaneously. To this end, in this paper, both the management and cyber security of MG are considered.

Due to the presence of different energy sources with different generation pattern and cost, one of the main challenges associated with such a complicated energy system is the optimal resource management. The optimal resource management scheme must determine how much energy each unit should generate such that the total cost of the system is minimized and all loads are supplied. The first part of this paper is devoted to proposing a robust energy management program for the physical operation of the grid.

Regarding the operation of the physical layer of the MG, a reliable and optimal energy management program is required to ensure the cost-efficient and dependable operation of smart grids under different conditions [1, 2]. Generally, MG can be linked to the power system through a point of common coupling and can exchange power with the utility grid considering the operation cost

of the system and upstream grid power cost. Thus, it is important to consider the effect of dynamic pricing of the energy market in the optimal energy management framework. There are several works of literature addressing the challenges in MG. In the following, some of the most advanced and recent works in this area are presented. In [3] a searching algorithm named the "crow search algorithm" to solve the stochastic energy management problem for hybrid MG has been presented. In [4], the 2m point estimation technique has been considered to create a stochastic framework for MG. The authors in [5] have provided a management strategy for plug-in electric vehicles integrated MG considering energy storage devices, fuel cell units, and renewable energy sources by applying a feeder reconfiguration method. In [6], a stochastic cloud-fog-based optimal scheduling solution for MG has been developed, which the uncertainties associated with renewable sources and load are captured using the fuzzy adaptive leader method. Authors in [7] have proposed an optimal scheduling framework for hybrid AC-DC MG considering cyber-attacks which the teacher learning optimization is used with the aim of operating cost minimization in the system. Also, in [8], a machine learning-based energy management technique has been presented for hybrid MG using whale optimization algorithm. Authors in [9] go into the depth of the components and fundamentals of MG. A stochastic mathematical model of renewable energy sources, as well as operational zones, optimization methodologies, load flow calculation methods, and control strategies, has been provided in this paper. Authors in [10] have offered a stochastic energy policy framework for intelligent vehicles. In the proposed work, several generation units are investigated, and system instabilities are considered using the unscented transform. Although the above works investigate significant topics about the physical layer of MG, the research in this area is limited.

Motivated by recent literature, most research has been focused on the physical characteristics of MG, while cyber security within such networks is frequently overlooked. In the MG, to make bidirectional communication between different parts of the grid possible, the advanced metering infrastructure is provided, which uses communication pathways to make connections. Online monitoring of the MG is the key to the reliable and smart operation of the electricity grid. Considering the point that the cyber layer of the MG is a data-driven system, it is vulnerable to cyber-attacks. In order to achieve secured and reliable operation of the MG, it is essential to use advanced and accurate cyber-attack detection models, which the research in this area there has been limited in the last decades.

Several data security efforts in the MG are covered in the subsequent section. A machine learning-based intrusion detection system (IDS) for detecting false data injection attacks on advanced metering infrastructure has been provided in [11]. An overview of several types of smart grid measurement systems has been presented in [12]. The authors in [13] have investigated the effect of data integrity attacks on the steady-state operation of MG and have recommended a novel countermeasure. In [14] concentrates on energy theft cyber-attacks. In the proposed research, transformer sensors have been employed and a detection approach has been proposed to find abnormalities in load consumption behaviour. In [15], the authors have used a deep learning model which uses a combination of an embedding layer, a modified CNN, and an LSTM to identification of the exact location of an exon in a DNA sequence. In another work, a multi-layer perceptron model is proposed and implemented using deep machine learning to distinguish between malicious and normal traffic based on their behavioral patterns [16]. In [17] the authors have focused on false data injection attacks on state vector estimation methods and proposed a deep learning system to detect such assaults. Similarly, in [18], a cyber-attack detection approach based on the support vector machines (SVM) algorithm and wavelet transform to identify and prevent cyber-attacks on the electric car controller area network (CAN) bus has been employed. In [19], a two-level strategy for increasing data transmission security in advanced metering infrastructures has been provided. This approach makes use of a dedicated authentication server to prevent unauthorized nodes from accessing the system. To identify compromised zones in wireless sensor networks, the authors in [20] have proposed a zone-based detection technique based on the sequential probability ratio test. In [21], a hybrid cyber-attack detection model based on unsupervised learning and a neural network for data integrity attacks is proposed.

According to our knowledge, most research has focused on the physical characteristics of MG, while cyber security within such networks is frequently overlooked. Also, recent studies addressed critical MG operating and security issues. By the way, research in this sector, particularly data security, is still in its early stages. To address the data security as well as energy management issue in ACMG, this research proposes a strategy for ACMG's optimal scheduling and a deep learning-based cyber-attack detection model for enhancing data security in the system. This paper tackles the optimal energy management of AC MG considering energy storage devices, renewable energy resources (RERs), energy markets, and dispatchable microturbines. For the optimization method, we utilize dragonfly [22] as our solver to point out the system's functional issues to find the best solution. According to the mentioned information above, this paper's key contributions are presented as follows:

- Considering MG as a cyber physical system and investigating the operation and security of the system simultaneously.
- Proposing a novel optimal scheduling scheme based on a powerful optimization technique called dragonfly algorithm.
- Considering various renewable energy sources and energy storage devices in operation of the ACMGs.

- Taking to account the cyber security of the system and proposing a novel cyber attack detection model using deep learning.

The rest of this paper is categorized as follows: Section 2 includes the MG mathematical model. Section 3 explains the details of the dragonfly optimization model. The details of the proposed deep learning IDS are presented in section 4. Section 5 provides the numerical simulation of employing the proposed approach on the utilized test system. Finally, section 6 concludes the paper.

2. Smart Hybrid AC- Microgrid

ACMG is a cyber-physical system that integrates several technologies, which is depicted schematically in Fig. 1. In the proposed MG, each component in the grid is equipped with corresponding devices which collect and send physical layer data, such as active power, reactive power, and voltage MG central control regular. Each node in the system has a smart metering device that communicates with the MG's central control through channels of communication. The MG central control optimally manages the system depending on the system characteristics and expected values. In the following subsection, the operation of ACMG is modelled as a limited optimization problem, and different constraints are presented.

2.1. Problem Formulation and Constraints

The objective function of the hybrid MG incorporates the entire cost of the system as (1) and (2):

$$\begin{aligned} Min\ \ h(X) = \sum_{t=1}^{N_T}\Big(\sum_{i=1}^{N_g}[u_i^t P_{Gi}^t B_{Gi}^t + S_{Gi}^{on}\max\{0,u_i^t - u_i^{t-1}\}+ \\ +S_{Gi}^{off}\max\{0,u_i^{t-1}-u_i^t\}]+\sum_{j=1}^{N_s}[u_j^t P_{sj}^t B_{sj}^t + S_{sj}^{on}\max\{0,u_j^t-u_j^{t-1}\}+ \\ +S_{sj}^{off}\max\{0,u_j^{t-1}-u_j^t\}]+P_{Grid}^t B_{Grid}^t\Big) \end{aligned} \quad (1)$$

In the above formula, the first term presents the cost of the generation units (generating active power, start up cost, and shutdown cost), the second term is related to energy storage devices, and the last term presents the cost of power exchanged with upstream grid.

Where X represents the control parameters as:

$$\begin{aligned} &X = [P_g, U_g]_{1\times(2\times n\times N_T)}\ ,\ n = N_d + N_s + 1\ ;\ \forall t \in N_T \\ &P_g^t = [P_G^t, P_s^t, P_{Grid}^t]\quad ;\quad P_G^t = [P_{G1}^t, P_{G2}^t, ..., P_{GN_g}^t] \\ &U_g^t = [u_1^t, u_2^t, ..., u_{N_d}^t]\quad ;\quad P_s^t = [P_{s1}^t, P_{s2}^t, ..., P_{sN_s}^t] \\ &P_{Grid}^t = [P_{Grid}^t]\quad ,\quad u_k^t \in \{0,1\} \end{aligned} \quad (2)$$

The above optimization problem is optimized while various practical and technological restrictions are taken into account. (3) and (4) demonstrate the balance of power in the system.

$$P_j^{inj,t} = \sum_{n=1}^{N_b} V_j^t V_n^t Y_{jn}\cos(\theta_{jn} + \delta_j - \delta_n) \quad (3)$$

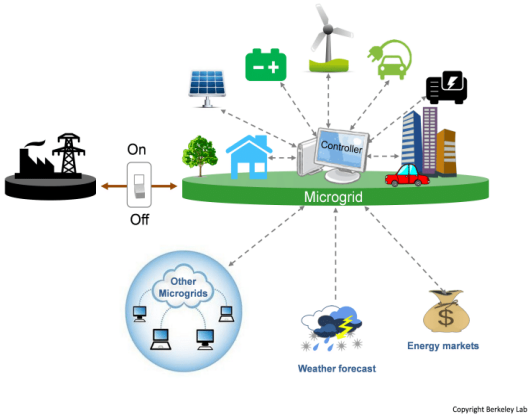

Fig. 1. Schematic illustration of AC MG's physical layer

$$Q_j^{inj,t} = \sum_{n=1}^{N_b} V_j^t V_n^t Y_{jn}\sin(\theta_{jn} + \delta_j - \delta_n) \quad (4)$$

Other limitations are represented as (5):

- Utility grid, batteries, and distributed generation units' capacity is limited by following constraints:

$$\begin{aligned} &P_{Gi,\min}^t \le P_{Gi}^t \le P_{Gi,\max}^t \\ &P_{conv,\min}^t \le P_{conv}^t \le P_{conv,\max}^t \\ &P_{Grid,\min}^t \le P_{Grid}^t \le P_{Grid,\max}^t \\ &P_{sj,\min}^t \le P_{sj}^t \le P_{sj,\max}^t \end{aligned} \quad (5)$$

- Spinning reserve at each hour of the day can be modelled using following formula.

$$\sum_{i=1}^{N_d} u_i^t P_{Gi,\max}^t + P_{Grid,\max}^t \ge \sum_{k=1}^{N_{Load}} P_{Load,k}^t + P_{loss}^t + \mathrm{Re}\,s^t \quad (6)$$

It is worth noting that the network P_{loss} depends on the physical structure of the network and the amount of generated power. Taking into account the loss coefficient 'b', and the optimal power flow, the power losses can be calculated from the following equation:

$$Ploss = \sum_{i=1}^{N}\sum_{j=1}^{N_d} B_{ij} P_i P_j + \sum_{i=1}^{N} B_{io}^t P_i + B_{oo} \quad (7)$$

- The amount of power that each feeder in the system can transfer is limited by a maximum value as below.

$$|P_i^{Line,t}| \le P_{i,\max}^{Line} \quad (8)$$

- The voltage of each bus in the system has a predefined range as presented in the following.

$$V_m^{\min} \le V_m^t \le V_m^{\max} \quad (9)$$

- The output of each generation units at each hour can change only by a limited amount as illustrated in following constraint.

$$| P_{Gi}^{t} - P_{Gi}^{t-1} | \leq UR_i, DR_i \quad (10)$$

3. Dragonfly Optimization Algorithm

In order to solve the operation problem in section II, a powerful optimization technique is required. For this purpose, in this section the dragonfly is proposed. As mentioned previously, the Dragonfly Algorithm mimics the dragonfly's behaviour and relocation tools. This algorithm has several advantages over other proposed Meta heuristic methods. One of the reasons that this algorithm has been able to contribute to different applications is that it is very simple and easy to implement. Furthermore, selecting the predators from the archive, the worst (most populated) hypersphere prevents the artificial dragonflies from searching around non-promising areas. Moreover, having few parameters for tuning is another advantage of this algorithm. Furthermore, the convergence time of the algorithm is reasonable. Over other optimization algorithms, it is firmer and it easily can be merged with other algorithms. Dragonflies fly in tiny groups in search of food in nature, which is known as a chasing instrument. Larger groups of dragonflies fly in the very same direction, causing the population to move in what is known as a movement component cycle. Fig. 2 illustrates the two types of behaviour for chasing and regulating dragonfly-amassing activity when searching.

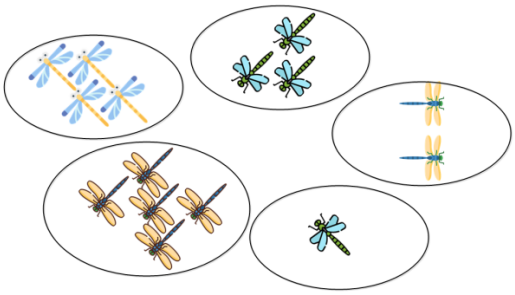

Fig. 2. Chasing and taking care of amassing conduct of dragonflies when searching

The dragonfly amassing habit is described by five administrators:

1. Separation is the element that guarantees that the investigators are kept apart in the location. (11) shows a numerical representation of detachment behaviour.

$$S_i = -\sum_{j=1}^{N} X - X_i \quad (11)$$

2. Synchronization demonstrates how the pace of a certain investigation specialist is synchronized with the speed of other chase operators in the neighbourhood. (12) shows a numerical proof of the arrangement behaviour.

$$A_i = \frac{\sum_{j=1}^{N} V_j}{N} \quad (12)$$

Where V_j is the speed of the j^{th} neighbour.

3. Cohesion indicates how individuals go from their home to the centre of mass. It refers to the population tendency to gravitate toward the nearest point of mass. The eq. (12) presents a numerical example of the behaviour of cohesion.

$$C_i = \frac{\sum_{j=1}^{N} x_j}{N} - X \quad (13)$$

4. Attraction refers to how the food supply attracts those that fly towards it. The numerical demonstration of this behaviour is seen in (14).

$$F_i = F_{loc} - X \quad (14)$$

Where F_{loc} represents the position of the food source.

5. Distraction refers to people's tendency to flee from a foe. The numerical difference between the i^{th} configuration and the opponent, is shown in (14).

$$E_i = E_{loc} + X \quad (15)$$

Where E_{loc} symbolizes the enemy's position.

During the search cycle, the rival with the highest wellness updates the well-being of the food supply and the region. Furthermore, the candidate with the most obvious flaws upgrades the opponent's health and position. The dragonfly method employs the nonexclusive system of the particle swarm optimization approach, which employs two vectors to update a dragonfly's situation: the advancement vector (X), which is identical to the particle swarm optimization (PSO) delivery of effective and the position vector. The progress vector (see (16)) influences dragonfly development.

$$\Delta X_{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + w\Delta X_t \quad (16)$$

where s, a, c, f, and e are loads of the partition S_i, arrangement A_i, attachment C_i, development speed into the food source F_i, and the foe aggravation level E_i of the i^{th} individual separately. In eq. (17) is shown how these boundaries are set adaptively during the progress cycle to ensure a suitable balance of research and exploitation. The latency weight, denoted by W, is derived by (17). More details on these boundary estimates and their influence on dragonfly algorithm behaviour can be seen in [22].

$$W = 0.9 - Iter \times \frac{(0.9 - 0.4)}{(MaxIter)} \quad (17)$$

where pct is calculated as (18).

$$W = \begin{cases} 0.1 - Iter \times \dfrac{(0.2 \times Iter)}{(MaxIter)} & if \quad (2 \times iter) \le \max Iter \\ 0 & o.w \end{cases} \quad (18)$$

Where r is an arbitrary number in the range of [0,1].
The situation of an individual is refreshed based on (19):

$$X_{t+1} = X_t + \Delta X_{t+1} \quad (19)$$

In which t is the present step.
The pseudo-code for the dragonfly method is shown in Algorithm 1. The software starts by creating an arbitrary population and randomly instating it with step vectors. The method iteratively performs the accompanying strides until an end basis is achieved. The primary coefficients (i.e., s, w, a, c, f, and e) are then refreshed by the algorithm. Following that, the administrators: separation (S), alignment (A), cohesiveness (C), food source (F), and enemy (E) are altered.

Algorithm 1. Process of dragonfly optimization algorithm

Initialize $\Delta X_i (i = 1, 2, ..., n)$
while (end condition is not satisfied) do Evaluate each dragonfly
Update (F) and (E)
Update the main coefficients (i.e., s, w, a, c, f, and e)
Calculate S, A, C, F, and E ((10) to (14))
Update step vectors ΔX_{i+1} using (15)
Update X_{t+1} using (18)
Return the best solution

4. The Deep Learning-Based IDS

This section offers an IDS using LSTM to identify false data injection attacks on smart load meters in the MG. The main advantage of the proposed IDS is that unlike most of the FDIA detection method, it doesn't have a fix threshold for detection, meaning that since at each point the model just looks at its *n* previous data points, the threshold by which a decision is made changes accordingly and dynamically. Another advantage is the high accuracy of the model, which is due to great performance of the LSTM is forecasting. Having only two parameters another advantage of the proposed model. The flowchart of the proposed IDS is depicted in Fig. 3.

Since LSTM has a recurrent structure, it is very powerful in modelling and forecasting sequential data (e.g. time series). In this regard this model is used to develop an accurate IDS. The main role of LSTM in the proposed model is to predict the next measurement (which we want to assess whether it's legitimate or not) as accurate as possible. The predicted value is then used to compute the normal forecast error (As shown in Eq. (20)). Afterwards, according to Eq. (21), the NFE is compared with a specific range known as the confidence interval, and a decision is made. In other words, when a new measurement is received in the central control, the normal distribution characteristics (mean and standard deviation) of the NFE of n previously collected data are calculated. Then, the NFE of the received data point is compared with two thresholds and a decision is made as modelled in the following equations.

$$NFE_{l,i} = ((P_{l,m}{}^{i} - P_{l,f}^{i}) / P_{l,f}^{i}) \quad (20)$$

$$Decision: \begin{cases} Attack & o.w \\ No\text{-}attack & m_i^t - g' s_i^t < NEF_{l,i} < m_i^t + g' s_i^t \end{cases} \quad (21)$$

The value of γ represents the breadth of the confidence interval as well as the degree of confidence. In the proposed model, bigger values of γ presents bigger confidence levels. The exact value of γ and n, which are known as the model's hyper-parameters, are determined by system's operators based on their desired degree of confidence.

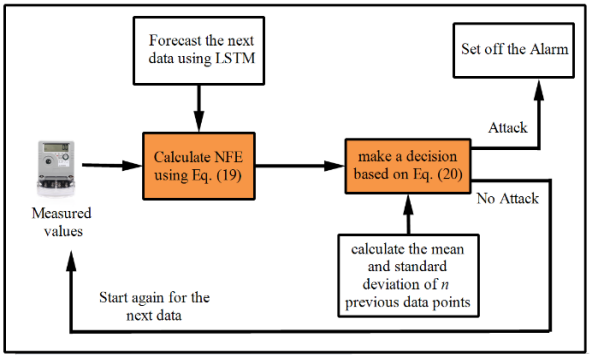

Fig. 3. The flowchart of the proposed IDS

The proposed LSTM that is used for load prediction is thoroughly detailed below.
The normal distribution function and different prediction ranges for different values of γ, is introduced, as well as the larger values of γ result in wider intervals, is depicted in Fig. 4.

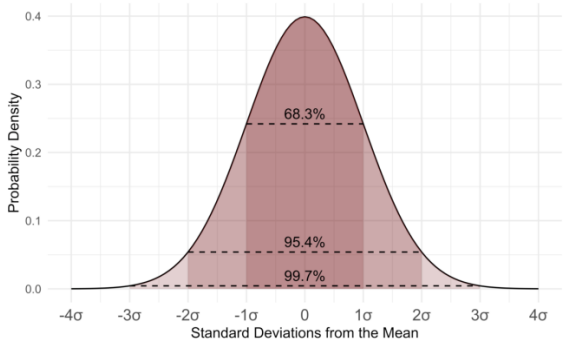

Fig. 4. Schematic illustration of Gaussian probability function with different confidence levels

4.1. The Long Short-term Memory

Generally, the long short-term memory (LSTM) is given as a solution to the gradients disappearing problem in classic recurrent neural networks [23]. The LSTM uses the memory cell and three cell gateways to record and store information. The input and forget gates describe which information will be added to / deleted from the cell state. In addition, the output gate determines which fraction of the current block must be utilized in the output. Fig. 5 depicts the construction of the LSTM cell. It should be noted that the LSTM network is trained using the backpropagation method [24]. The LSTM transition equations are presented in (22):

$$h_t = H(W_{x,h}x_t + W_{h,h}h_{t-1} + b_h) \quad (22)$$

$$y_t = W_{h,y}h_t + b_y \quad (23)$$

The function H is implemented as follows:

$$i_t = \partial(W_{i,x}x_t + W_{i,h}h_{t-1} + b_i) \quad (24)$$

$$f_t = \partial(W_{f,x}x_t + W_{f,h}h_{t-1} + b_f) \quad (25)$$

$$\bar{c}_t = \tanh(W_{\bar{c},x}x_t + W_{\bar{c},x}h_{t-1} + b_{\bar{c}}) \quad (26)$$

$$o_t = \partial(W_{o,x}x_t + W_{o,h}h_{t-1} + b_o) \quad (27)$$

$$C_t = f_t \cdot c_{t-1} + i_t \cdot \bar{c}_t \quad (28)$$

$$h_t = o_t \cdot \tanh(c_t) \quad (29)$$

5. Numerical Simulation Results

In previous sections, the details and mathematical model of the proposed cyber-physical framework for secured optimal scheduling of ACMG was presented. To examine the effectiveness and evaluate the accuracy of the proposed methodology, this section is devoted to the simulation of the proposed methodologies. This section consists of two subsections. In the first subsection, the performance of the optimal scheduling framework for the physical layer is examined and in the second subsection, the proposed false data injection attack detection method is evaluated. The entire simulations are performed on a personal laptop with an Intel Core-i7 CPU and 8 gigabytes of ram.

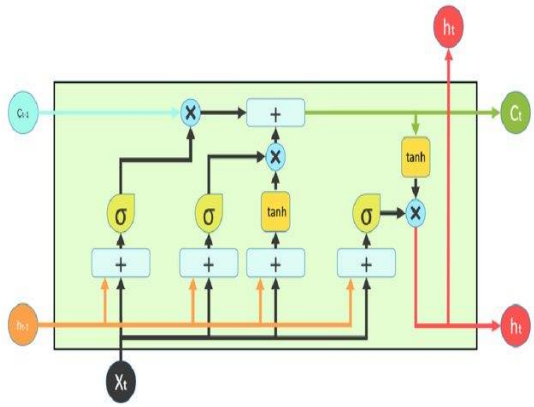

Fig. 5. Structure of LSTM cell

5.1. Optimal Scheduling Framework for Physical Layer

In order to model a practical grid, the IEEE 33-bus test system is used as a test case. For more realistic results, several components including two wind turbines, one photovoltaic (PV) unit, three micro turbines, and one energy storage unit are added to the test system. The specifications and characteristics of the system are presented in Table I.

Table I. Characteristics and specifications of the components of the grid

Type	Min output (kW)	Max output (kW)	Bid ($/kWh)	Start-up/Shutdown Cost ($)	Ramp rate	Location (Bus number)
Micro turbine 2	100	1300	0.675	70	220	12
Micro turbine 3	90	1100	0.675	75	180	25
Wind turbine1	0	550	1.073	0	-	30
Wind turbine2	0	450	1.073	0	-	21
Photovoltaic1	0	400	2.584	0	-	16
Energy storage	-350	350	0.318	0	0	18
Micro turbine1	35	300	0.475	70	110	15

Also, a graphical presentation of the test system is depicted in Fig. 6. In order to respect the concept of renewable energy grids, the renewable sources (i.e., wind turbines and photovoltaic) are considered non-dispatchable units, meaning that their entire generation is consumed without considering the cost and benefits. The level of voltage in the entire system is 12.7 kV and also, in this section, the system is scheduled for 24 hours considering one-hour time intervals. Additionally, to consider the effect of the dynamic energy market on the performance of the model, it is assumed that the MG are able to purchase/sell energy from the upstream grid based on non-fixed prices which are presented in Fig. 7 [25].

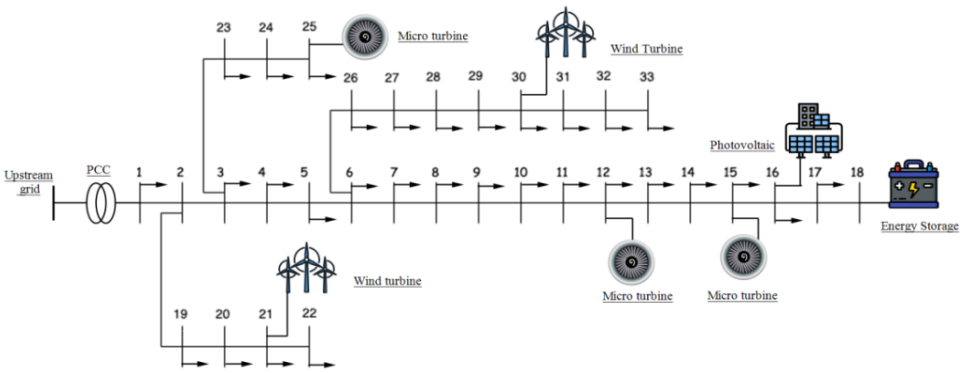

Fig. 6. Graphical visualization of the test system

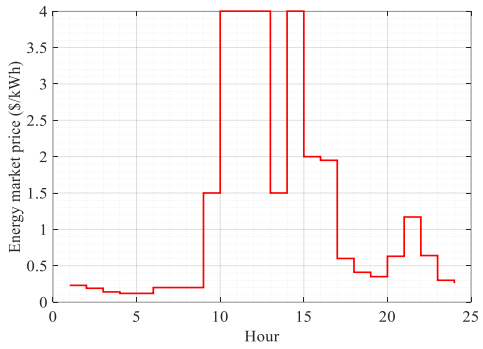

Fig. 7. Hourly energy market prices

Regarding the system's loads, a 24-hour load factor is considered where the load of every bus in the system is computed by multiplying these factors by the maximum load of every bus in the day. The 24-hour load factor values are given by [24]. Also, the normalized output of renewable sources is presented in Fig. 8 and Fig. 9, respectively. It is worth noting that all renewable sources follow this pattern.

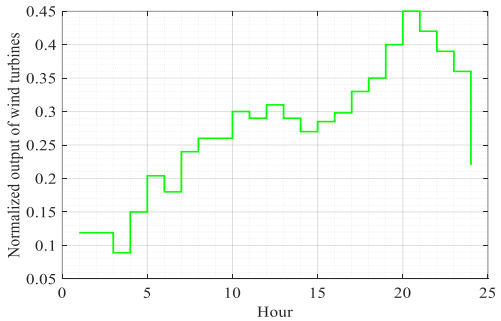

Fig. 8. Hourly normalized output of wind turbines

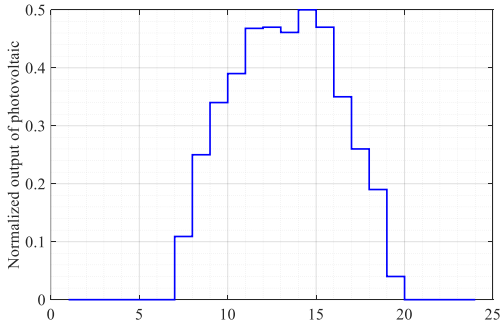

Fig. 9. Hourly normalized output of photovoltaics

In order to show the great performance of the dragonfly in minimizing the cost objective function of the system in the operation day, the results of the dragonfly in compared with two other well-known methods called teacher learning based optimization (TLBO) and PSO. The total cost of the system, total power loss of the system, and maximum voltage deviation of the system, considering different optimization techniques, are presented in Table II. It is worth noting that the results in Table II are the average results obtained from running the program 10 times considering 200 iterations. As can be seen from table II, the dragonfly optimization has had a better performance compared to other methods. The operation costs of the system considering dragonfly method, are equal to 1497$ and 2552$ lower than TLBO and PSO, respectively. This shows the great performance and robustness of the optimization technique in minimizing the operation cost of the system.

Table III shows the results of the optimal scheduling of the network and output power of generation units and batteries at different hours of the day. Note that the output of renewable sources is not optimally set and is based on nature.

According to Fig. 7 and Table III, in the early hours of the day when the energy market price is lower than the generation cost of units, priority is given to the upstream grid to minimize the operation cost. In this regard, all dispatchable units are turned off and according to Fig. 10, the amount of power purchased from the upstream grid is at the highest level.

Table II. Comparing the results of the optimal scheduling for different optimization methods

Method	Total cost ($)	Power loss (kW)	Maximum voltage deviation (p.u.)
Dragonfly	48768	2385	0.08
PSO	51320	2652	0.07
TLBO	50265	2973	0.05

On the other hand, as can be seen from Table III and Fig. 10, in the middle of the day, when the energy price is high, all generation units are operating near their maximum capacity. This is a beneficial policy to avoid purchasing expansive power from the upstream grid. Additionally, it can be seen that due to the ramp rate limitation, the output power of generation units has increased gradually. This behaviour models the practical

assumption that micro turbines can only increase their generation smoothly and cannot reach to the maximum capacity suddenly.

Table III. Optimal output power of generation units

Hour	Micro Turbine 1	Battery	Micro Turbine 2	Micro turbine 3	Wind turbine 1	Wind turbine 2	PV
1	0	-350	0	0	65.45	53.55	0
2	0	-350	0	0	65.45	53.55	0
3	0	-350	0	0	48.95	40.05	0
4	35	-350	0	180	82.5	67.5	0
5	0	-350	0	100.0164374	112.2	91.8	0
6	35	-350	204.0178975	280.0164374	99	81	0
7	70.4290712	-335.071	424.0178975	460.0164374	132	108	43.6
8	150.4290712	-342.293	644.0178975	640.0164374	143	117	100
9	230.3014818	350	864.0178975	820.0164374	143	117	136
10	300	350	1084.017897	1000.016437	165	135	156
11	300	350	1299.743419	1100	159.5	130.5	187.2
12	300	350	1300	1100	170.5	139.5	188
13	300	350	1300	1100	159.5	130.5	184.4
14	300	350	1300	1100	148.5	121.5	200
15	300	350	1300	1100	156.75	128.25	188
16	300	327.323	1300	1100	163.9	134.1	140
17	231.6735533	-331.859	1300	1031.396778	181.5	148.5	104
18	181.0388398	-340.601	1300	862.4305479	192.5	157.5	76
19	220.7533328	-345.353	1300	742.1776719	220	180	16
20	255.6281862	350	1080	562.1776719	247.5	202.5	0
21	277.6603903	350	1300	538.1986504	231	189	0
22	197.6603903	311.5846	1300	358.1986504	214.5	175.5	0
23	117.6603903	-350	1300	178.1986504	198	162	0
24	78.55115728	-349.213	1300	0	121	99	0

In terms of battery in the system, according to Table III, it can be seen that in the early hours of the day when the energy is relatively cheap, the battery gets charged at its maximum charging rate. Subsequently, it discharges at peak hours to avoid purchasing power from the upstream grid. This is an extremely beneficial behaviour to the grid from the cost point of view. In general, the presence of energy storage units in the grid can help minimize the operation cost significantly.

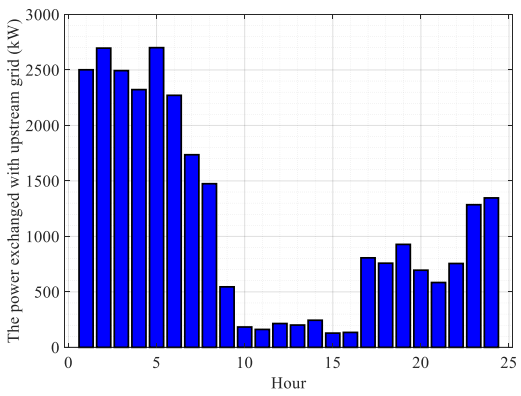

Fig. 10. The power exchanged with the upstream grid during the day

5.2. IDS performance evaluation

In this subsection, we evaluate the performance of the proposed deep learning-based IDS using a real-world data set. In this regard, in the first step, the open access dataset of the hourly load consumption of Johor city in Malaysia is utilized for training the LSTM model. The dataset contains 2 years of data related to a distribution bus [26]. In order to train the LSTM model, we used 18 months of data for training and the remaining 6 months for testing. The LSTM model consists of the 4 LSTM layers and each layer has 100 LSTM cells. The LSTM layers are followed by a dropout layer with a 30% rate to prevent overfitting. The output of the model is a fully connected layer to map information to a single output unit. The activation function for the last layer is linear and the loss function is cross-entropy. For optimization, the ADAM optimizer is used and the size of the sliding lag window is 18. In order to have a better examination, the results of the LSTM are compared with a fully connected artificial neural network (ANN). The evaluation metrics for the trained model, which are mean absolute percentage error (MAPE), mean absolute error (MAE), and root means square error (RMSE), are presented in Table IV. As can be seen from Table IV, the LSTM model outperforms the ANN model in all metrics. This shows the great ability of the deep

structure of LSTM in capturing the long-term pattern of the data.

Table IV. Evaluation metrics of the trained model

model	MAPE%	MAE	RMSE
LSTM	2.108	891.5	1285.2
ANN	4.23	1523	2057.2

Also, the regression diagram for trained models is presented in Fig. 11. The great accuracy and good performance of the LSTM model can be seen at sharp edges.

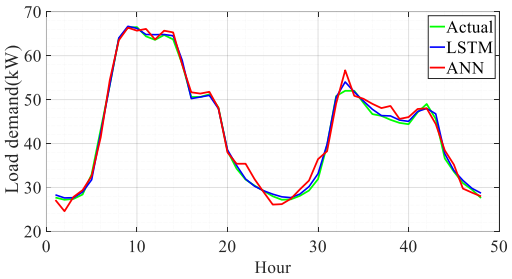

Fig. 11. Regression diagram for 2 randomly chosen days

Now that the model is trained, it's time to test the cyber-attack detection model. For this purpose, we consider 5 different scenarios. In each scenario, 100 different fake measurements with a random amount of deviation from real values are generated. The mean value of the normal distribution in each scenario is the real measured value of the metering device and the standard deviation for each scenario is based on Table V.

Table V. Scenarios of testing the proposed IDS

Scenario	standard deviation
scenario 1	0.03*RM
scenario 2	0.1*RM
scenario 3	0.2*RM

In the above scenarios, $n = 60$. Meaning that for each test point, the two last months of the data are utilized to make a decision based on (19) and (20). The results of the detection for the test scenarios are presented in Table VI. In Table VI, the value of accuracy, Specificity, and F1-score are presented, which are the three most well-known metrics for classification tasks. The results in Table VI show that by increasing attack intensity, the detection accuracy of the model increases drastically, such that in scenario 3 which has the highest attack intensity, the accuracy of the model is near 100 %. This shows the great performance of the model in detecting cyber-attacks.

Table VI. Results of testing the proposed IDS

	Accuracy	Specify	F1 score
scenario 1	82%	85%	78%
scenario 2	90%	92%	88.40%
scenario 3	97%	97%	91%

6. Conclusion

This paper proposed a cyber-physical framework for optimal operation of ACMG considering false data injection attacks. In this work, the optimal scheduling of ACMG was formulated as a single optimization technique and the dragonfly optimization was utilized to solve the proposed optimization. The performance of the optimal scheduling framework was examined using IEEE 33-bus test system. The results showed the great performance of the proposed methodology in minimizing the operation cost in 24 hours. Also, the results of the dragonfly were compared with two other well-known optimization methods that showed the great performance of the proposed optimization technique. The second part of the paper was focused on the cyber security of electric grids. In order to enhance cyber security in such systems, a novel method based on LSTM was proposed which is the base focus of this problem-solving approach, as a subset of recurrent neural networks (RNNs). This meticulously crafted model exhibits an impressive accuracy rate of 97%, effectively safeguarding the cyber-security of the system under consideration. The result of comparison between the proposed LSTM with a fully connected artificial neural network (ANN) was presented in table IV. Also, in Fig. 11, the accuracy of LSTM was compared with ANN, indicating that the LSTM identifies real data with significantly lower error, underscoring its superior performance.The performance of the proposed cyber-attack detection method was evaluated by a real-world dataset. The results of this part showed the great performance of the proposed IDS in detecting cyber-attacks.

7. References

[1] A. Kavousi-Fard, M. Mohammadi, and A. Al-Sumaiti, "Effective Strategies of Flexibility in Modern Distribution Systems: Reconfiguration, Renewable Sources and Plug-in Electric Vehicles, in Flexibility in Electric Power Distribution Networks", CRC Press. p. 95-119, 2021.

[2] M. Mobtahej, et al., "Effective demand response and GANs for optimal constraint unit commitment in solar‐tidal based microgrids", *IET Renewable Power Generation*, 2021.

[3] B. Papari, et al., "Effective energy management of hybrid AC–DC microgrids with storage devices", *IEEE transactions on smart grid*, 10(1), pp. 193-203, 2017.

[4] A. Baziar, and A. Kavousi-Fard, "Considering uncertainty in the optimal energy management of renewable micro-grids including storage devices", *Renewable Energy*, 59, pp. 158-166, 2013.

[5] X. Gong, et al., "A secured energy management architecture for smart hybrid microgrids considering PEM-fuel cell and electric vehicles", *IEEE Access*, 8, pp. 47807-47823, 2020.

[6] S. Z. Tajalli, et al., "DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid", *IEEE Transactions on Industry Applications*, 56(3), pp. 2968-2977, 2020.

[7] M. Mohammadi, et al., "Effective management of energy internet in renewable hybrid microgrids: A secured data driven resilient architecture", *IEEE Transactions on Industrial Informatics*, 18(3), pp. 1896-1904, 2021.

[8] M. Lei, and M. Mohammadi, "Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand", *International Journal of Electrical Power & Energy Systems*, 128, p. 106702, 2021.
[9] M. Pourbehzadi, et al., "Optimal operation of hybrid AC/DC microgrids under uncertainty of renewable energy resources: A comprehensive review", *International journal of electrical power & energy systems*, 109, pp. 139-159, 2019.
[10] M. Pourbehzadi, et al. "Stochastic energy management in renewable-based microgrids under correlated environment", IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2020, IEEE.
[11] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids", *IEEE Transactions on Industrial Informatics*, 17(1), pp. 650-658, 2020.
[12] N. T. Mbungu, et al., "Overview of the optimal smart energy coordination for microgrid applications", *IEEE Access*, 7, pp. 163063-163084, 2019.
[13] M. Mohammadi, et al., "Reinforcing Data Integrity in Renewable Hybrid AC-DC Microgrids from Social-Economic Perspectives", *ACM Transactions on Sensor Networks*, 2022.
[14] S. Hussain, et al., "Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel‐Tree boosting classifier−A novel sequentially executed supervised machine learning approach", *IET Generation, Transmission & Distribution*, 16(6), pp. 1257-1275, 2022.
[15] A. Darvish, S. Shamekhi, "A hybrid multi-scale CNN-LSTM deep learning model for the identification of protein-coding regions in DNA", *Tabriz Journal of Electrical Engineering*, vol. 52, no. 2, pp. 137-146, 2022.
[16] M. Vasou Jouybari, E. Ataie, M. Bastam, "An MLP-based Deep Learning Approach for Detecting DDoS Attacks", *Tabriz Journal of Electrical Engineering*, vol. 52, no. 3, pp. 195-204, 2022.
[17] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism", *IEEE Transactions on Smart Grid*, 8(5), pp. 2505-2516, 2017.
[18] A. Kavousi-Fard, et al., "An effective anomaly detection model for securing communications in electric vehicles", *IEEE Transactions on Industry Applications*, 2020.
[19] T. Mehra, V. Dehalwar, and M. Kolhe, "Data communication security of advanced metering infrastructure in smart grid", 5th International Conference and Computational Intelligence and Communication Networks, 2013, IEEE.
[20] J. W. Ho, , M. Wright, and S. K. Das, "ZoneTrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing", *IEEE Transactions on Dependable and Secure Computing*, 9(4), pp. 494-511, 2011.
[21] A. Aflaki, et al., "A hybrid framework for detecting and eliminating cyber-attacks in power grids", *Energies*, 14(18), p. 5823, 2021.
[22] S. Mirjalili, "Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems", *Neural computing and applications*, 27(4), pp. 1053-1073, 2016.
[23] S. Hochreiter, and J. Schmidhuber, "Long short-term memory", *Neural computation*, 9(8), pp. 1735-1780, 1997.
[24] P. J. Werbos, "Backpropagation through time: what it does and how to do it", *Proceedings of the IEEE*, 78(10), pp. 1550-1560, 1990.
[25] T. Cheng, et al., "Stochastic energy management and scheduling of microgrids in correlated environment: A deep learning-oriented approach", *Sustainable Cities and Society*, 69, p. 102856, 2021.
[26] H. J. Sadaei, et al., "Short-term load forecasting by using a combined method of convolutional neural networks and fuzzy time series", *Energy*, 175, pp. 365-377, 2019.