Machine Learning-assisted Energy Management System in an Islanded Microgrid with Resiliency Investigation against Cyber-Physical Attacks

1st Amirhossein Nazeri
International Center for Automotive Research
Clemson University
Greenville, USA
anazeri@g.clemson.edu

2nd Roghieh A. Biroon
International Center for Automotive Research
Clemson University
Greenville, USA
rabdoll@g.clemson.edu

3nd Jan K. Westman
Holcombe Department of Electrical and Computer Engineering
Clemson University
Charleston, USA
jwestma@clemson.edu

4th Pierluigi Pisu
International Center for Automotive Research
Clemson University
Greenville, USA
pisup@clemson.edu

5th Ramtin Hadidi
Holcombe Department of Electrical and Computer Engineering
Clemson University
Charleston, USA
rhadidi@clemson.edu

***Abstract*—This paper presents an integrated energy management system (EMS) for an islanded microgrid, and briefly investigates the system's performance in case of false load injection attack. The proposed energy management system includes a Multi-step Deep LSTM neural network, and a mixed-integer optimization algorithm. The Deep LSTM neural network forecasts the load data, while the optimizer determines the best setpoints for the microgrid's decentralized controllers. The EMS is integrated with an islanded microgrid to evaluate the viability of the proposed system. Finally, the system's performance against cyber-physical attack is taken into the account. It is shown that the attack can significantly affect the microgrid's performance.**

***Index Terms*—Energy management system, Microgrid, LSTM, Machine learning, Cyber-physical attack**

I. Introduction

Electrical load forecasting has been always of great importance for the utilities planning. A successful Energy Management System (EMS) must be able to accurately predict the demand power needed by the users. An accurate load prediction is necessary to hold the equilibrium of energy supply and demand. In the past decades, traditional simple statistical techniques such as the multiplicative autoregressors (ARs) [1], Bayesian estimation model [2], and Kalman filter [3] have been used to forecast the load data. But the problem with these methods is that they are slow and time-consuming. Since they have simple architectures, they are not suitable for the problems with high complexities and big data.

With the invention of classic machine learning and its tremendous application in science and technologies, several machine learning techniques have been introduced to predict the load consumption in power grids. In [4] a support vector regression (SVR) machine, a chaotic sequence, and the evolutionary algorithm are proposed for electric load forecasting. Recently, Deep Neural Network (DNN) has proved to be a good candidate to be replaced by the classical machine learning algorithms. The recent works reveal that DNNs are more powerful than classical machine learning methods for AI applications such as regression and classification. DNN techniques with high computational power can deal with models with very high complexities and massive datasets. Authors in [5] presented a deep regression network to predict solar radiation. The proposed model's performance was better than the classical machine learning methods like Gaussian Process Regression (GPR), and Support Vector Regression (SVR). In [6] a Convolutional Neural Network (CNN) is proposed to forecast load power in a smart grid. The training and test sets are split using K-Means clustering approach. CNN algorithms typically employ fewer unknown parameters than DNNs, so they are faster and less likely to overfit the model. Although DNN and CNN are powerful tools for classification and regression-based applications, they lack efficiency in dealing with time-series data. Because time-series data are strongly dependent on historical data, thus, a suitable machine learning model must memorize the old data and be able to extract the time features of the data to facilitate a better prediction.

A recurrent Neural Network (RNN) retains a memory that keeps informative old data to help predict future data. In [7], the authors introduced an RNN-based model to predict the short-term electricity demand in a city in Indonesia. They showed that the RNN performance was much better than the Vector Autoregressive (VAR) model on the same dataset. That said, RNN suffers from vanishing and exploding gradients, and forgets long-term dependencies. Thus, it is unsuitable for data with long-term dependencies like electrical load data which possess long-term historical and seasonal features. To tackle

this problem, Long Short-Term Memory (LSTM) networks are introduced [8]. LSTM is designed in order to store the most relevant past data and ignore the redundants. LSTM includes three parts, known as gates. The first gate is Forget gate; the second and third are the Input and the Output gates, respectively. The Forget gate is responsible for determining whether the previous timestamp data is essential to keep or must be forgotten. The Input gate tries to learn from the new input data, and the Output gate updates the information and the next timestamp. Authors in [9] presented an LSTM model to forecast the load data for the Energy Management System. However, they failed to provide an in-detail description of the proposed model.

Energy Management System (EMS) is an indispensable part of power systems like grids and microgrids. Microgrids' energy management systems (EMS) are responsible for reliable and economic operation through generation scheduling, economic dispatching, and demand side management. In general, energy management systems rely heavily on information and communication technologies (ICTs) in order to implement advanced monitoring and management algorithms. The capability of wireless measurements, online data transmission, and connectivity among units in microgrids enhance the efficiency and controllability of these systems. Therefore, emerging as cyber-physical systems, microgrids with a higher level of connectivity are vulnerable to cyber security threats, such as False Data Injection (FDI), Man in the Middle, and Denial of Service attacks [10], [11]. Cyber-attacks can compromise critical operations of microgrids by exploiting vulnerabilities at the networks, systems, and/or application levels [12]. In the existing literature, the methods to enhance the security of cyber-physical systems can be classified into two categories: (i) model-based detection approaches [13]–[15]; and (ii) data-driven detection methods [16], [17]. Under cyber-attacks, a microgrid network comprises several subnetworks. Therefore, the security assessment and attack detection task becomes very complex and challenging. The proposed approaches for power systems are not always suitable for the security of microgrids and a few numbers of literature particularly focuses on the security of microgrids [18]–[20]. It is more difficult to use the model-based approach for autonomous detection at the unit level in microgrids since, for any unit, a detailed model of the rest of the microgrid is commonly unavailable [21]. However, a unit can learn from observing the available data acquired from accessible units and/or the EMS. This paper addresses the need for microgrid autonomous anomaly detection to enhance their reliability. In this study, we particularly focus on developing and evaluating the theoretical foundation of a real-time cyber-attack impact on microgrid energy management systems while considering potential uncertainties.

II. Load Forecasting using Deep LSTM Neural Network

A. Data Preparation and Preprocessing

The load dataset used for the training is one year of load demand from Jan-1st 2020 to Jan-1st 2021 borrowed from The New York Independent System Operator [22]. The load datapoints are recorded with a time interval of 5 minutes. In the first phase of the data preparation the dataset it cleaned by removing the null values, outliers, duplicated and missing timestamps. Fig. 1 shows the dataset load demand for a year.

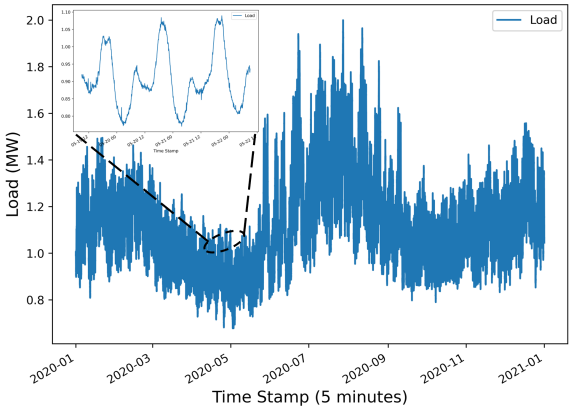


Fig. 1: One-year cleaned load profile

Since the load data is inherently time-dependent, its future value is correlated to the current and past values. Therefore, the time features are extracted and concatenated with the load data as the inputs to the machine learning model. The extracted time features in this study include Minutes, Hours, Daylight, Day-of-Week, and Weekdays. In the next step, a Min-Max scaler function normalizes the inputs in the range [0, 1] so the algorithm will converge faster. Then, keeping the temporal order of timestamps, the dataset is divided into the train, validation, and test sets. Firstly, the dataset is split into train-validation and test sets by 99/1 ratio. Then the train-validation set is split into train and validation subsets by ratio of 80/20.

B. Deep LSTM Machine Learning Model

In this section a deep LSTM model is proposed to predict electric load demand that is formulated as a multivariate multi-step time-series forecasting problem. The proposed deep LSTM model forecasts one hour (12 data points) in the future by looking at one day in the past (288 data points). The extracted time features in the section II-A are normalized and concatenated with the normalized load data and set as input to LSTM model. The model architecture consists of input layer, two hidden LSTM layers along with two Dropout layers at the end of each LSTM layer. Finally, a fully connected feed-forward dense layer is placed at the end of the second hidden layer. Validation loss is selected as the metric to evaluate the performance of the trained LSTM model. python 3.9.12 and TensorFlow 2.9.0 are utilized to implement the deep LSTM model. The model's hyperparameters are optimized through the Random Search technique using the Keras-tuner from Keras module. The hyperparameters after optimization are as below: two hidden layers of LSTM with 128 neurons each, a fully connected feed-forward dense layer with 12 neurons, two dropout regularization layers after each hidden

layer with value of 0.2 each, and LeakyReLU with alpha = 0.5 is considered as activation function for LSTM hidden layer. Adam optimization algorithm with learning rate of 0.0003 is selected for the stochastic gradient descent for model training. Fig. 2 demonstrates the architecture of the proposed deep LSTM model.

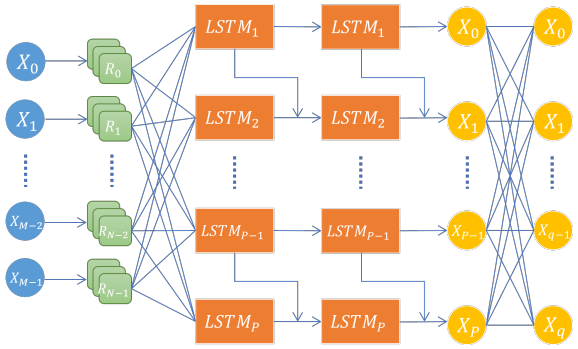


Fig. 2: The architecture of the proposed deep LSTM model

C. Load Forecasting Results

The dataset is split into three subsets, training, testing and validation sets. The date starting 1-Jan-2020 to 5-Oct-2020 (80000 datapoints) is assigned as training set. 6-Oct-2020 to 14-Dec-2020 (20000 datapoints), and 15-Dec-2020 to 26-Dec-2020 (1500 datapoints) are set as validation and test subsets, respectively. The model is trained by the computational help of an NVIDIA GPU GeForce RTX(TM) 3070 8GB GDDR6. The batch size and number of training epochs are 256 and 50 after fine tuning, respectively. The Mean Squared Error (MSE) for the forecasted data on the training set is 4e-4 while it is 1.5e-4 on the validation set. Fig. 3 shows the evaluation of the trained deep LSTM model on the test set compared to the actual data. The time interval between two records is 5 minutes.

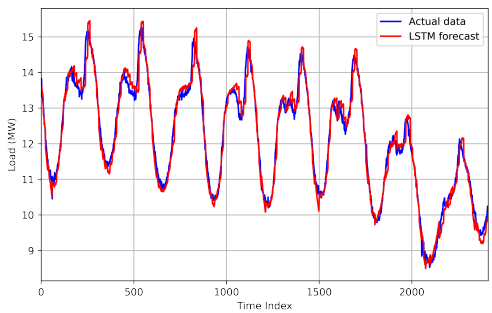


Fig. 3: The forecasted load of the trained deep LSTM model on the test set

III. Microgrid Power Management

The goal of this section is to minimize the exploitation of the battery in the microgrid system and to find the appropriate BESS point and Genset for the battery's invertor and generator controllers. To achieve this goal, a mixed-integer linear optimization algorithm with nonlinear constraints is formulated and solved by Gurobi Software optimization module in Python. The proposed optimizer hourly determines the power profiles of battery and generator for the span of one hour in the future. The data of one hour includes 12 observations, considering the time intervals of 5 minutes between successive observations. The battery optimization problem is formulated as below:
Objective function:

$$minimize \sum_{t=1}^{t=N=12} P_b^t \tag{1}$$

Constraints:

$$P_{Gen}^t - P_{L_{forecast}}^t + P_b^t * (2*U-1) = 0; 1 < t < N = 12 \tag{2}$$

$$soc^t = soc^{t-1} + \frac{\eta_b * P_b^{t-1} * (1-U) * \Delta t}{B} - \frac{P_b^{t-1} * (U) * \Delta t}{\eta_b * B} \tag{3}$$

$$\begin{gathered} 0.45 < soc^1 < 0.55 \\ 0.45 < soc^N < 0.55 \\ 0.1 < soc^t < 0.9; 2 < t < N-1 \\ 0.5MW < P_{Gen}^t < 1.2MW \\ -0.3MW < P_b^t < 0.3MW \end{gathered} \tag{4}$$

The proposed objective function minimizes the battery's usage in the microgrid system. The $P_Gen, P_{L_{forecasted}}, P_{pv}$, and P_b are the power of generator, load, solar, and battery, respectively. soc is the state of charge of battery. η_b and B are the efficiency of the charging/discharging and total capacity of the battery, respectively. U is a binary parameter representing the operational state of the battery. Battery is discharging if $U = 1$, while it is charging if $U = 0$. Superscripted t denotes the time t while the time interval between two successive records is 5 minutes, such that, $t - 1$ is 5 minutes prior to the time t. The power of the generator is bounded between 0.5 MW and 1.2 MW, and the charging-discharging power of the battery is bounded between -0.3 MW to 0.3 MW based on its operating mode (charging-discharging). The state of the charge of the battery can vary from 10% to 90%. The optimizer predicts the power profile of the battery and the generator at time t based on the forecasted load demand and the solar power at time t. An ideal solar power is considered in this paper, so that, we assume the similar yearly solar power is generated every year. Thus, there is no need for the solar power prediction providing that the solar data of a single year exists. The solar resource data is obtained from NREL database [23]. Fig. 4 demonstrates the optimized input and output powers in the Microgrid for a time span of 150 hours (1800 datapoints). Each datapoints is equivalent to 5 minutes in time. The optimization is carried out every 5 hours, with overall number of 16 optimization. After each optimization, the forecasted load data is replaced by the real data for the next optimization.

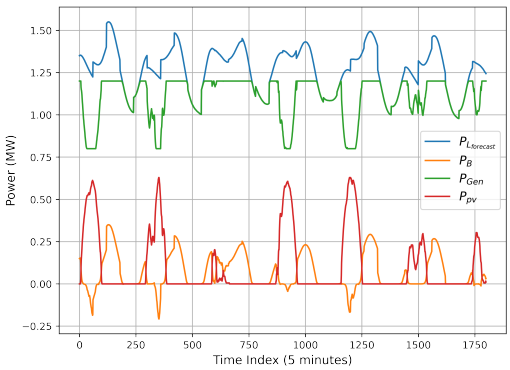


Fig. 4: Optimization results of the P_B and the P_{Gen} with respect to the forecasted demand load $P_{L_{forecasted}}$ and solar power P_{pv}

IV. Islanded Microgrid Structure

In this paper an islanded microgrid is designed to undergo a cyber-physical security resiliency test. An islanded Microgrid is disconnected from the utility grid and it can integrate various sources of the power generation to feed the local loads [24]. The grid power outage does not affect the islanded microgrid and it is more resilient against security breaches than a grid-connected microgrid. The proposed microgrid include a storage battery unit, PV system, back-up generator, and local load that are attached to a common AC Bus. The Simulink model of the microgrid is shown in Fig. 5. The historical PV data are used in this project. The PV system is adjusted to produce up to 600kW. The output of the solar panel is controlled by an MPPT unit to operate at the desired voltage and achieve the maximum available power. The battery plays an essential role to achieve a satisfactory stability and reliability in the Microgrid. By charging and discharging, battery keeps the power balance between the generation and demand. A Lithium-ion (Li-Ion) battery with 8 MWh capacity is employed. A bi-directional D2D converter is linked to the BESS to control the charging/discharging states of the battery. A decentralized controller is embedded in the inverter block of the battery to sustain the frequency within the appropriate range. The controller is obtained from [25], [26]. The controller presented in [25] is a combination of the droop control and virtual inertia. The controller aims to minimize the steady state error. The virtual inertia comes handy in case of sudden changes in voltage or frequency.

V. Machine Learning-assisted Energy Management

A. Architecture & Description

In this section all components are connected together to make a smart microgrid work properly. The operation of the proposed smart microgrid is discussed in this section. The first element is the Deep LSTM load forecasting block which is

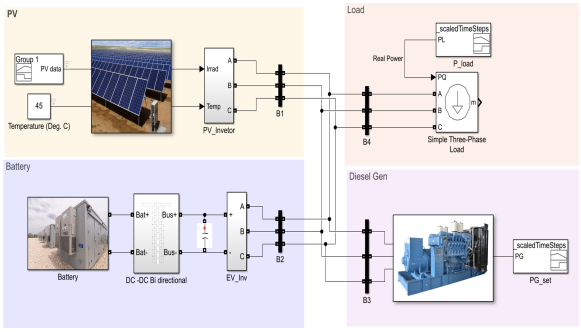


Fig. 5: The microgrid model in Simulink

responsible for forecasting the load profile of the next one hour in the future named $P_{L_f}^{t_{i+1}}$. The time t_i refers to the current one-hour time span while t_{i+1} represents the next hour in the future. subscripts f and M refer to forecasted and measured data, respectively. In the beginning, the historical load data of the last two days enter the deep LSTM block as initial load values, and the deep LSTM block forecasts the load profile for one hour in the future based on the historical data. A mixed-integer linear optimizer with nonlinear constraints is embedded in the Energy management block. The Energy management block determines the corresponding battery and generation amounts ($P_{B_f}^{t_{i+1}}$ and $P_{Gen}^{t_{i+1}}$) based on the forecasted load data and ideal solar data, $P_{L_f}^{t_{i+1}}$ and $P_{pv}^{t_{i+1}}$. Then $P_{B_f}^{t_{i+1}}$ and $P_{Gen_f}^{t_{i+1}}$ are fed into the Microgrid network as BESS and Genset points. This loop will be executed every one hour. Fig. 6 demonstrates the schematic of the proposed smart grid.

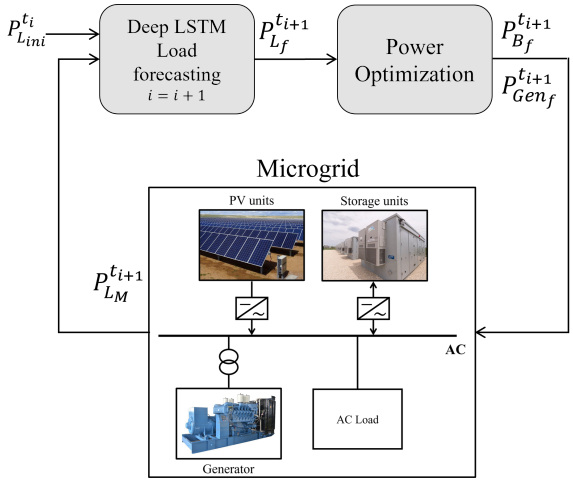


Fig. 6: The schematic of the proposed energy management system

B. Simulation Results

The Microgrid is implemented in Simulink Matlab while the Deep LSTM machine learning and the power optimization blocks are coded in Python. The Microgrid model reads the input control parameters every hour and send back the processed results to the Deep LSTM unit in each cycle. The

system in 6 is executed for one hour and power generation results are depicted in Fig. 7. Fig. 8 demonstrates the load frequency response. The frequency is flat and maintained very well within the standard frequency limit close to 60 GHz that shows the stability and the reliability of the proposed energy management system.

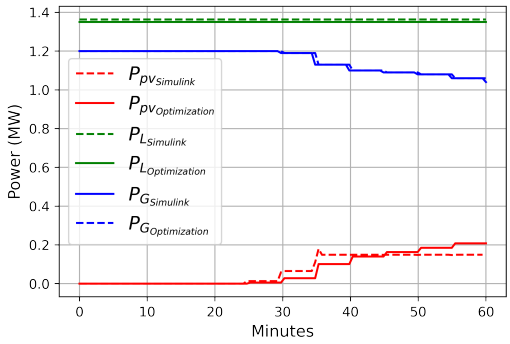


Fig. 7: The power generation and load response in the microgrid

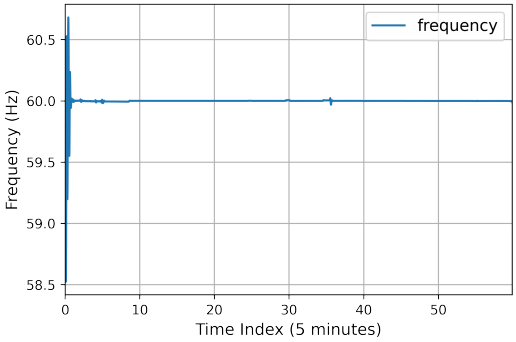


Fig. 8: frequency

C. The System Under Cyber-physical Attack

Decentralized control systems offer, in many cases, better robustness and stability than centralized controls, especially in large-scale systems. Nevertheless, they are more vulnerable to malicious attacks and faults, because each control unit has just access to its local data and looses the overall look to the total system. Microgrids with decentralized control units are susceptible to cyber-attacks because the subsystems have to communicate with each other. Inverters are one of the most critical components in the microgrid systems. Attackers can destabilize the whole system by distorting the local controller of the inverters [27]. This study considers the case that attackers manipulate the output of the deep LSTM neural network and input false BESS points to the inverter of the battery. Fig. 9 shows the cyber-attack insertion to the system. The attacked load profile and the frequency response of the system to that are shown in Fig. 10a and 10b, respectively.

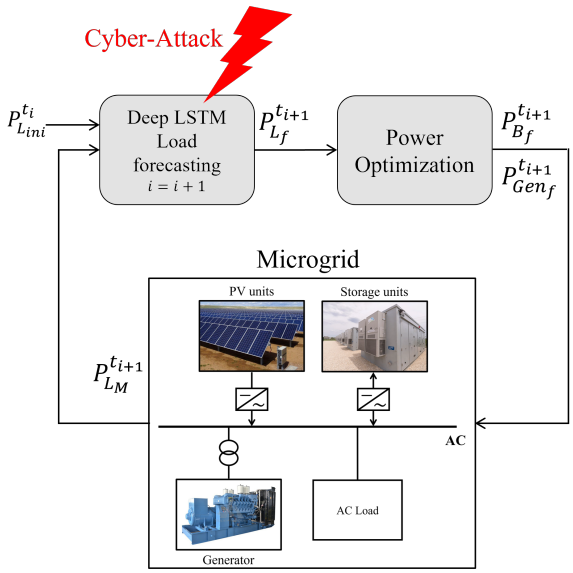
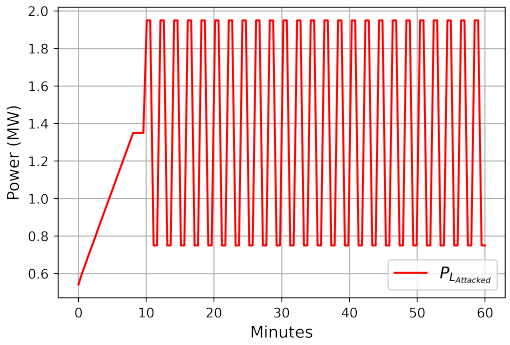
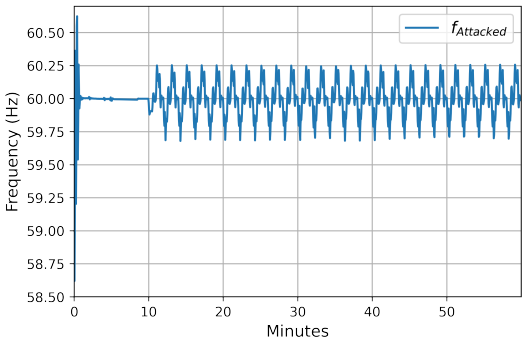


Fig. 9: The integrated EMS under attack injection



(a) The manipulated load



(b) The system frequency under attack

VI. Conclusion

An integrated energy management system is proposed in this paper. The system consists of a Deep LSTM neural network that forecasts the incoming load profile every one hour, and a mixed-integer optimization algorithm that sets the equilibrium between demand and supply in an islanded microgrid. The EMS is connected to an islanded microgrid in Simulink to evaluate its viability for the real power network applications. Finally, a cyber-physical attack is added to the system, from the load side, to investigate the resiliency of the microgrids. The results reveal that the cyber-physical attack has a significant impact on the microgrids' performance. In the future work, authors aim to come up with novel robust machine learning techniques to isolate and remove the incoming cyber-physical attacks to the system.

References

[1] G. Mbamalu and M. El-Hawary, "Load forecasting via suboptimal seasonal autoregressive models and iteratively reweighted least squares estimation," *IEEE Transactions on Power Systems*, vol. 8, no. 1, pp. 343–348, 1993.

[2] A. P. Douglas, A. M. Breipohl, F. N. Lee, and R. Adapa, "The impacts of temperature forecast uncertainty on bayesian load forecasting," *IEEE Transactions on Power Systems*, vol. 13, no. 4, pp. 1507–1513, 1998.

[3] D. J. Trudnowski, W. L. McReynolds, and J. M. Johnson, "Real-time very short-term load prediction for power-system automatic generation control," *IEEE Transactions on Control Systems Technology*, vol. 9, no. 2, pp. 254–260, 2001.

[4] W.-C. Hong, Y. Dong, W. Y. Zhang, L.-Y. Chen, and B. Panigrahi, "Cyclic electric load forecasting by seasonal svr with chaotic genetic algorithm," *International Journal of Electrical Power & Energy Systems*, vol. 44, no. 1, pp. 604–614, 2013.

[5] S. Dey, S. Pratiher, S. Banerjee, and C. K. Mukherjee, "Solarisnet: A deep regression network for solar radiation prediction," *arXiv preprint arXiv:1711.08413*, 2017.

[6] X. Dong, L. Qian, and L. Huang, "Short-term load forecasting in smart grid: A combined cnn and k-means clustering approach," in *2017 IEEE international conference on big data and smart computing (BigComp)*. IEEE, 2017, pp. 119–125.

[7] R. N. Hasanah, R. R. OMP, and H. Suyono, "Comparison analysis of electricity load demand prediction using recurrent neural network (rnn) and vector autoregressive model (var)," in *2020 12th International Conference on Electrical Engineering (ICEENG)*. IEEE, 2020, pp. 23–29.

[8] G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5929–5955, 2020.

[9] T. Panapongpakorn and D. Banjerdpongchai, "Short-term load forecast for energy management systems using time series analysis and neural network method with average true range," in *2019 First International Symposium on Instrumentation, Control, Artificial Intelligence, and Robotics (ICA-SYMP)*, 2019, pp. 86–89.

[10] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2013.

[11] G. Deconinck, T. Rigole, H. Beitollahi, R. Duan, B. Nauwelaers, E. Van Lil, J. Driesen, R. Belmans, and G. Dondossola, "Robust overlay networks for microgrid control systems," in *Proc. Workshop on Architecting Dependable Systems (WADS 2007), co-located with 37th Ann. IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN 2007), Edinburgh, Scotland (UK)*, 2007, pp. 148–153.

[12] A. Mohan, G. Brainard, H. Khurana, and S. Fischer, "A cyber security architecture for microgrid deployments," in *International Conference on Critical Infrastructure Protection*. Springer, 2015, pp. 245–259.

[13] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[14] ——, "Resilient control strategy under denial of service in connected vehicles," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 4971–4976.

[15] P. Pisu, J. Martin, and Z. A. Biron, "A control oriented perspective for security in connected and automated vehicles," *Mechanical Engineering*, vol. 139, no. 12, pp. S17–S20, 2017.

[16] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[17] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765–2777, 2019.

[18] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[19] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[20] K. R. J. Ranjith, D. Kundur, and B. Sikdar, "Transient model-based detection scheme for false data injection attacks in microgrids," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–6.

[21] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[22] in *The New York Independent System Operator—NYISO*.

[23] in *National Renewable Energy Laboratory*.

[24] J. Hu and A. Lanzon, "Distributed finite-time consensus control for heterogeneous battery energy storage systems in droop-controlled microgrids," *IEEE Transactions on Smart Grid*, vol. 10, pp. 4751–476, 2019.

[25] S. Dinkhah, J. S. Cuellar, and M. Khanbaghi, "Optimal power and frequency control of microgrid cluster with mixed loads," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 143–150, 2022.

[26] S. Dinkhah, C. A. Negri, M. He, and S. B. Bayne, "V2g for reliable microgrid operations: Voltage/frequency regulation with virtual inertia emulation," in *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, 2019, pp. 1–6.

[27] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.