Cyber-attack Detection on Distributed Frequency Control of Islanded MGs Using Machine Learning

Narayan Bhusal, *Student Member, IEEE*, Mukesh Gautam, *Student Member, IEEE*,
and Mohammed Benidris, *Member, IEEE*
Department of Electrical and Biomedical Engineering, University of Nevada, Reno, NV 89557, USA
Emails: bhusalnarayan62@nevada.unr.edu, mukesh.gautam@nevada.unr.edu, and mbenidris@unr.edu

***Abstract*—Several coordinated control strategies along with extensive communication networks have been proposed and employed for proper monitoring and control of increased penetration of distributed generators (DGs) in microgrids (MGs). Because of communication networks, MGs are being exposed to numerous cyber-attacks with possibility of impacting active power sharing. In this context, an attacker can launch individual as well as coordinated data falsification attacks on distributed frequency control systems of MGs. This paper proposes a two-stage machine learning-based approach to detect and locate data falsification attacks on distributed frequency control of islanded MGs. In the first stage (regression), environmental parameters including solar irradiance, ambient temperature, and wind speed are provided to a machine learning regressor to predict active power from DGs. In the second stage (classification), a logistic regression compares the predicted active power of DGs with the measured active power of DGs to detect and locate data attacks in real time. Case studies on a modified version of the IEEE 123-node distribution system show that the proposed work can detect low margin attacks on distributed frequency control schemes with 97% accuracy.**

***Index Terms*—Active power sharing, cyber-attack, machine learning, distributed generator, frequency control, microgrids.**

I. INTRODUCTION

Microgrids (MGs) are small power systems that have the capability to operate in grid connected as well as islanded modes. Different types of distributed generators (DGs) are being integrated into MGs to support their autonomous operation. With the increased grid penetration of DGs, several coordinated control strategies through the deployment of advanced automation and communication networks have been proposed to facilitate reliable active power sharing and efficient frequency control following a disturbance. However, the increased adoption of advanced communication technologies are exposing active power sharing and frequency control of MGs to multiple types of attacks from adversaries.

Frequency control can be divided into primary (local), secondary (power balance redispatch), and territory (economic dispatch) levels. Types of secondary and territory frequency control can be broadly categorized into: (i) centralized control and (ii) distributed control. In the centralized control scheme, a master controller receives information from DGs including available net active and reactive power injections, frequency, and operational cost from the participating DGs, and provides operation decisions to participating DGs. Since this scheme heavily depends on two-way high-bandwidth communication technologies to monitor and control DGs, any failure in communication systems will expose a single point failure and impact the performance of MGs [1]. Distributed control schemes, on the other hand, are equipped with a master controller, which communicates with some of local DGs (referred to as pinned DGs) for flow of information. Pinned DGs communicate with other DGs through sparse communication for active power sharing and frequency control, reactive power sharing and voltage control, and economic operation [2]. Involvement of communication networks and information flow makes MG controllers susceptible to denial of service attacks and false data injection (FDI) attacks [3].

An FDI attack can have several impacts on the operation of MGs. In an FDI attack, adversaries may inject, alter, block, delete, and/or modify data of a single or multiple participating DGs in a coordinated manner by attacking any portion of communication links or DG nodes. Combination of multiple intelligent attacks launched in multiple nodes and communication networks in a sneaking fashion not only deteriorates the power system but also makes them formidable [4]. Impacts of FDI attacks on active power sharing have been studied in [5]–[7]. Although research on cybersecurity of MGs is relatively new field, some insightful studies (including [6], [7]) have been proposed for the detection of cyber-attacks on the distributed frequency control in MGs. However, further research is needed for maturity of attack prevention, detection, and recovery measures of active power sharing and frequency control in MGs. In our previous work [8], we have proposed the coordinated data falsification detection in the DG domain. Work presented in [8] is focused on the manipulation of the DGs for the monetary benefits. The work presented in this paper mainly focuses on the manipulation of DGs and their impact on power sharing regulate system frequency. Although the approaches are similar, however, conceptually these papers are different.

This paper proposes a two-stage machine learning-based approach to detect and locate cyber-attacks in distributed frequency control of MGs. The proposed work can detect coordinated attacks on DG nodes and communication links of distributed control schemes. Since power output of DGs (e.g., PV systems) depends upon environmental parameters such as solar irradiance, ambient temperature, and wind speed, the first stage (regression) utilizes these parameters to predict active power output of DGs. Several algorithms are investigated for regression performance including Multilayer perceptron (MLP), random forest regressor (RFR), convolutional neural

network (CNN), long short-term memory (LSTM) neural network, and CNNLSTM. In the second stage (classification), a logistic regression compares the predicted and measured active power of DGs for online detection of attacks. Case studies on a modified version of the IEEE 123-node distribution system show that the proposed work can detect low margin cyber-attacks on distributed secondary frequency control schemes with 97% accuracy.

The rest of the paper is organized as follows. Section II provides a brief description of distributed frequency control and data attack models. Section III describes the proposed cyber-attack detection mechanism. Section IV verifies the proposed solution. Section V provides concluding remarks.

II. Coordinated Distributed Frequency Control

In this work, inverter-based controllable DGs, specifically PVs and wind turbine generators, are deemed to operate in isolated MGs. DGs are assumed to participate in the secondary frequency control for maintaining the power balance in MGs [9]. This section describes preliminaries of distributed frequency control and cyber-threat models.

A. Preliminaries of Communication Network

Communication networks connecting DGs in a microgrid can be modeled by a digraph. A digraph is generally expressed as $G = \{V, E, A\}$ where $V = \{v_1, v_2, \cdots, v_N\}$ denotes the set of N vertices (nodes); E is set of arcs (edges) $E \subseteq V \times V$; and $A = \{a_{ij}\}_{N\times N}$ denotes adjacency matrix. DGs at N locations represent the vertices and communication links between these DGs represent the arcs in the digraph. Let (v_i, v_j) be an arc from vertex i to j (i.e., vertex j can receive information from vertex i), i.e., $a_{ij} = 1$ if $(v_i, v_j) \in E$; otherwise $a_{ij} = 0$. The in-degree matrix can be expressed as $D = \text{diag}\{d_i\} \in \Re^{N\times N}$ with $d_i = \sum_{j=1}^{N} a_{ij}$. Now, the Laplacian matrix of the digraph can be expressed as $L = D - A$. In case of distributed coordinated control strategy, the master controller (MC) communicates only with pinned (leader) DGs and the pinned DGs are responsible for transmitting information to other DGs using sparse communication [10]. Fig. 1 shows an architecture of a MG and information flow between DGs.

B. Active Power Sharing and Secondary Control

Active power sharing among participating DGs on the primary control is based on their rated capacities of the droop setting, which can be expressed as follows [11].

$$\omega_i = \omega_{ni} - m_i P_i \tag{1}$$

where ω_i denotes frequency of DG i; m_i represents droop coefficient of DG i; ω_{ni} denotes reference set point for DG i; and P_i is active power injection from DG i.

When power imbalances occur in a microgrid because of sudden changes in system operating conditions (e.g., islanding, load changes, generator unit tripping, etc.), microgrids may not be able to compensate frequency deviations using primary frequency control alone. Under such circumstances, the secondary frequency control is required. In this context, communication networks are inevitable to coordinate between participating DGs for secondary frequency control [12].

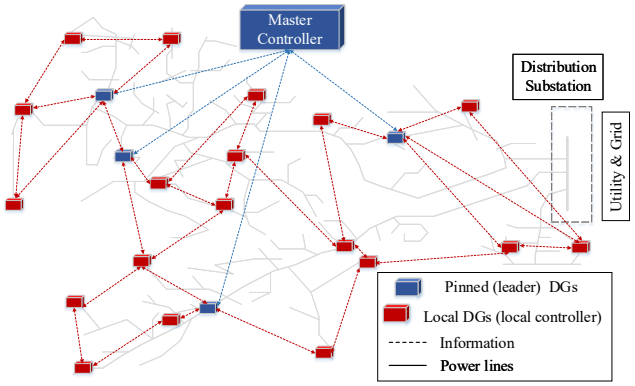

Fig. 1. Communication network for distributed control systems in MGs, where the master controller can exchange information only with pinned DGs. Each DGs has local control scheme and can communicate with neighboring DGs.

The operational objectives of the secondary frequency control in MGs are: (a) no frequency deviation between DGs during synchronized conditions (i.e., $\omega_1 = \omega_2 = \cdots = \omega_N = \omega^*$) and (b) proportional active power sharing among all DGs (i.e., $m_1 P_1 = m_2 P_2 = \cdots = m_N P_N$). Therefore, the objective of the secondary control system is to select ω_{ni} to synchronize the following frequency control input, u_i^{ω}, and active power sharing control input, u_i^{δ}, to zero.

$$u_i^{\omega} = \sum_{j=1}^{N} a_{ij} (\omega_j - \omega_i) - g_i (\omega - \omega^*) \tag{2}$$

$$u_i^{\delta} = \sum_{j=1}^{N} a_{ij} (m_j P_j - m_i P_i) - g_i (m_i P_i - m_i P_i^*) \tag{3}$$

where $g_i = 1$ if DG i is pinned, otherwise $g_i = 0$; and P_i^* and ω^* are optimal active power and frequency set points respectively.

C. Potential Cyber-threat Model

As described in section II-B, the secondary frequency control in an isolated MG is performed through the communication between the participating DGs and their neighbors. In this process, frequency and active power sharing information of participating DGs are shared through sparse communication networks to compute the set point for each DG. Because of the reliance of secondary frequency control systems on communication networks, it can be susceptible to cyber-attacks. A malicious input signal injected by an attacker can alter the frequency set point infringing the optimal operating points of participating DGs.

Cyber attacks can lead to violations of the active power limits of DGs, which can further lead to system wide instability. Adversaries can attack communication links between DGs, local DGs (local controllers), and the master controller [6]. The proposed work mainly concerns with detection of

data falsification attacks on control inputs, u_i^{δ}, of the sparse communication links and local controllers. The study on attack detection on frequency control input, u_i^{ω}, and sophisticated attack on master controller is left as future work.

When one or more communication links are attacked and false data are injected, active power sharing control input u_i^{δ} can be modified as follows.

$$\begin{aligned} u_i^{\delta} = & \sum_{j \in V_c a} a_{ij} \left(m_j (P_j + \Delta P_j) - m_i P_i \right) \\ & + \sum_{k \in V - V_c a} a_{ik} \left(m_k P_k - m_i P_i \right) - g_i \left(m_i P_i - m_i P_i^* \right) \end{aligned} \tag{4}$$

where V_{ca} denotes a set of DGs whose active power sharing information is received from compromised communication links and ΔP_j is the active power bias inserted by an adversary on the active power injection of DG j through the compromised communication links. In (4), the first term represents active power sharing information received from DGs that are connected to compromised communication links, and the second term represents the active power sharing information received from DGs that are connected to uncompromised communication links.

Similarly, when one or more local controllers of DGs are attacked, the active power sharing control input, u_i^{δ}, can be modified as follows.

$$\begin{aligned} u_i^{\delta} = & \sum_{j \in V - V_{da}} a_{ij} \left(m_j P_j - m_i (P_i + \Delta P_i) \right) \\ & + \sum_{k \in V_{da}} a_{ik} (m_k (P_k + \Delta P_k) - m_i (P_i + \Delta P_i)) \\ & - g_i \left(m_i (P_i + \Delta P_i) - m_i P_i^* \right) \end{aligned} \tag{5}$$

$$\begin{aligned} u_j^{\delta} = & \sum_{s \in V - V_{da} - v_i} a_{js} \left(m_s P_s - m_j P_j \right) + \\ & \sum_{r \in V_{da} + v_i} a_{jr} \left(m_r (P_r + \Delta P_r) \right. \quad \left. - m_j P_j \right) \\ & - g_j \left(m_j P_j - m_j P_j^* \right) \end{aligned} \tag{6}$$

where $V_{da} + v_i$ is a set of compromised DGs. Equation (5) denotes the active power sharing control input of an attacked DG, where the first term represents active power sharing information received from unattacked DGs and the second term represents the active power sharing information received from attacked DGs. Equation (6) denotes active power sharing control input of an unattacked DG in which the first term represents active power sharing information received from unattacked DGs and the second term represents the active power sharing information received from attacked DGs.

It can be seen from (4), (5), and (6) that an attacker can manipulate power injection, $P + \Delta P$, in a single or multiple vertices (DGs) to alter the active power sharing control input. Therefore, this paper proposes a machine learning-based method to detect and locate attacks on active power injections of DGs. In this paper, we have assumed that an attacker inserts additive injection bias (i.e., $\Delta P > 0$). Note that the proposed approach can also be applied to detect a deductive injection bias (i.e., $\Delta P < 0$).

III. The Proposed Attack Detection Model

This section describes the proposed attack detection mechanism including attributes, two-stage regression and classification models, training attributes, and evaluation metrics.

Note that the data processing, feature engineering, hyperparameter tuning, etc., are the important strategies that are integral parts of machine learning-based approaches in the real applications and numerous works have been dedicated to it. However, details on optimal parameter tuning, feature engineering, data cleaning, etc., are out of scope of this paper.

A. Attributes of the Proposed Attack Detection Mechanism

Most of existing machine learning-based attack detection approaches are based on binary classification problems that detect whether there is an attack or not (1 or 0). In this paper, instead of using a label for the entire system, we label each DG by '1' or '0' (i.e., attacked or not, respectively) to appropriately locate cyber-attacks. Therefore, the proposed approach is an N-label-based multi-label classification. From the perspective of machine learning-based methods, classifying an attack on a system to success or failure is a single-label classification problem whereas classifying more than one DG at the same time with multiple labels is a multi-label classification problem. Although machine learning techniques have achieved significant progress in the single-label classification problem, they are still facing several challenges in solving multi-label classification problems. Therefore, deliberate attention is needed to design multi-label classification problems.

Fig. 2 shows the block diagram of the proposed approach. In the proposed work, we use a two-stage approach consisting of regression and classification stages to detect data falsification attacks on active power sharing in MGs. The attack can also be detected directly only with multi-label classification. However, the proposed two-stage approach has the following advantages over existing approaches: (a) since the regression stage predicts the power output of each DG, predictions can be used to set active power sharing information if the attack flag is 'on' at any instance; (b) after obtaining predicted values from the regression model, the task of the classification problem is to compare predicted values with measured quantities by developing a threshold to detect attacks; therefore, a complicated multi-label classification problem turns into a simple comparison problem.

This paper mainly deals with data falsification attacks on active power injections of inverter-based DGs including PVs and wind turbines. As power outputs produced by DGs depend upon environmental parameters, the proposed model takes current weather data including solar irradiance, ambient temperature, and wind speed as input in the regression stage (brief description of regression model is provided in III-B) and predicts outputs of DGs as shown in Fig. 2. The output

from the regressor model and the current active power measurements are provided as input to the classification model to decide whether DGs are attacked or not.

During the training phase of the classifier, a combination of current active power measurements and the predicted active power vector, ($z_t = z_t^1, z_t^2, ..., z_t^{2N}$), is provided as input and class labels, y_t, are provided as output. The training output class labels are determined as follows.

$$y_t^i = \begin{cases} 1, & \text{if DG } i \text{ is attacked at instance } t \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

B. Regression Stage: Active Power Prediction

Power generated by PV systems depends upon solar irradiance and ambient temperature whereas that of a wind turbine depends upon wind speed. Therefore, during training, weather data are used as input to the regression and active power produced by DGs are used as output. During online operation, the trained regressor model takes weather data as input to predict the active power. Then, the predicted power is compared with measured active power to detect the presence of attacks. Machine learning models including random forest, MLP, CNN, LSTM, and CNN-LSTM are investigated to test their performance for active power prediction of DGs in MGs. These models are chosen because of their capability to map the highly nonlinear relationships between weather parameters and active power of DGs. Specifications of the models used in the proposed work is provided in section IV. Since machine learning models can accurately predict the power, attacks smaller than the forecast error are insignificant. Therefore, these can be used as a basis to classify cyber-attacks on real measurements.

C. Classification Stage: Logistic Regression

The task of the logistic regression in the proposed work is to compare predictions obtained from a regressor with actual measurements to produce class labels. As the inbuilt logistic regression classifier in scikit-learn library of Python is a binary classifier $(0/1)$, the multi-output classification support of the scikit-learn library is used for the multi-label classification of the proposed work. The main concept of this setting is to use one classifier per target, which allows multi-label classification with a binary classifier. Detailed description of logistic regression is not included for bravity; interested reader can refer to [13], [14].

D. Evaluation Metrics

Mean absolute error (MAE) and root mean square error (RMSE) are used to evaluate the performance of the regressor. MAE and RMSE can be expressed as follows.

$$\text{MAE} = \frac{1}{T}\sum_{t=1}^{T}|x^t - \hat{x}^t| \tag{8}$$

$$\text{RMSE} = \sqrt{\frac{1}{T}\sum_{t=1}^{T}(x_i^t - \hat{x}_i^t)^2} \tag{9}$$

where T is total number of test samples; and x^t and $\hat{x}^t$ represent actual and predicted active power of DGs, respectively.

The performance of the classification model for the proposed work is evaluated using the following standard evaluation metrics.

$$\text{Accuracy: A} = (Tp + Tn)/(Tp + Tn + Fp + Fn) \tag{10}$$

$$\text{Precision: P} = T_p/(T_p + F_p) \tag{11}$$

$$\text{Recall: R} = T_p/(T_p + F_n) \tag{12}$$

$$\text{F1-Score} = 2 \times (P \times R)/(P + R) \tag{13}$$

$$\text{False Alarm: FA} = F_p/(F_p + T_n) \tag{14}$$

In these metrics, T_p is the number of compromised DGs labeled as compromised; T_n is the number of uncompromised DGs labeled as uncompromised; F_p is the number of uncompromised DGs labeled as compromised; and F_n is the number of compromised DGs labeled as uncompromised.

IV. Simulation and Verification

Simulations and verification are carried out on the modified IEEE 123-node test feeder. The following DGs are added to the system: total of 5 PV systems and 5 wind turbine generators each of size 120 kVA are added at nodes $1, 18, 40, 47, 49, 55, 60, 66, 76, 99$ respectively as shown in Fig. 3. Network data of the IEEE 123-node test feeder are given in [15].

As it is described in section II, an attacker can alter one or multiple DGs. In this process, we assume that out of the total 10 DGs, 6 DGs are compromised. Since an intelligent attacker can change power injection biases, from time to time, the proposed model is trained and tested on a data-set with time-varying injection biases. At each time sequence, a random number between 5 and 20 is generated and that percentage of actual injection is used as a power injection bias of the instant. Power injection biases are limited within 5% to 20% (i.e., $\Delta P_t = 0.05 * P_{DG,t}$(act) to $0.2 * P_{DG,t}$ (act)) because generation biases higher than 20% can be easily detected and generation biases lower than 5% may not be of interest for attackers. Algorithm 1 provides the procedure of attack function and class label generation.

Since the tested system is unbalanced and power flow calculations need to be performed for several scenarios, an integrated OpenDSS and MATLAB environment is used to calculate the power flow in generating a dataset for the proposed method. The unbalanced power flow is solved for 8760 snapshots and active power measurement data of each DG participating in the frequency control are recorded. All aforementioned machine learning models are developed in Python using the scikit-learn and TensorFlow backend keras library. Out of total 8760 hourly data instances, 34% of the data are used for training the regressor model and 66% of the data are used for testing. For classification, 70% of test data of regressor (i.e., $0.7 \times 66 = 46.2\%$ of total data) are used for training and 30% of test data are used for testing the logistic regression (i.e., $0.3 \times 66 = 19.8\%$ of total data).

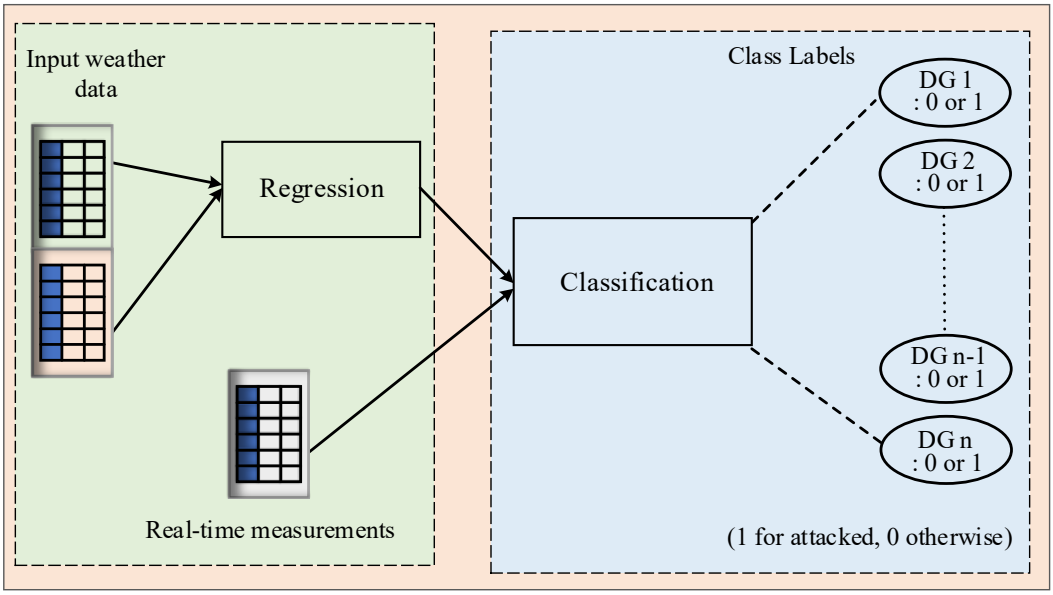

Fig. 2. General block diagram of the proposed attack detection model. Solar irradiance, ambient temperature, and wind speed are provided as input to the regression model which predicts the power output of each of the DGs. The predicted active power is compared with the measured active power to classify the presence of the data attack. The output is the status of DGs, 0 for normal and 1 for the attacked.

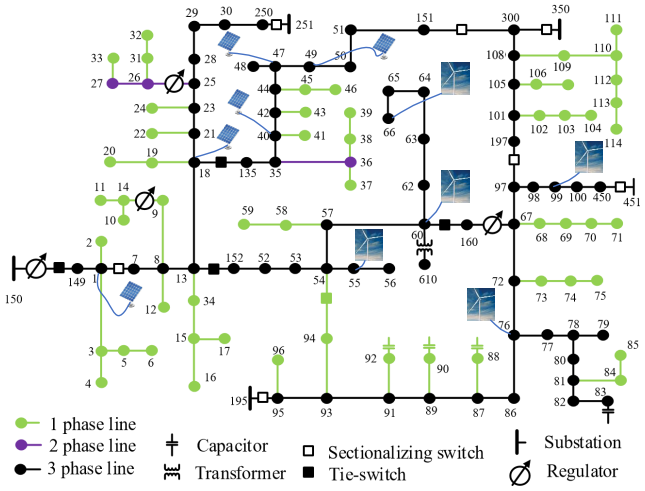

Fig. 3. Modified IEEE 123 node system with PVs and wind turbines.

Algorithm 1: Attack function and class labels generation for the proposed work.

Input : Input uncompromised readings $P_{DG}(act)$
Initialize $P_{DG} = P_{DG}(act)$
Randomly generate n_a attack instants from the total classification time sequence data (T_s)
for $k \leftarrow 1$ **to** n_a **do**
  randomly choose N_c (out of total N DGs) DGs that are attacked
  randomly generate the size of percentage generation bias lying between 5% and 20%
  obtain the generation bias for all the attacked DGs
  apply the additive attacks in respective DGs
  obtain the generation values after the attacks
  update P_{DG} including the attacks
Output1: Generation with attack function, P_{DG}
Determine the additive classes
Initialize additive class $P_{\text{class, add}} = \text{zeros}(T_s, N)$
for $i \leftarrow 1$ **to** T_s **do**
  for $j \leftarrow 1$ **to** N **do**
    if $P_{DG}(i,j) > P_{DG}(act)$ **then**
      $P_{\text{class, add}}(i,j) = 1$
Output : P_{DG}, $P_{\text{class, add}}$

To test the regression performance, RFR, MLP, CNN, LSTM, CNN-LSTM are used. For each model (except RFR), ReLU is used as an activation function in input and hidden layers and a linear activation function is used in the final layer. Adaptive moment estimation is used as optimization function and mean square error is used as a loss function. Further specifications of these models are provided as follows.

- Random Forest Regressor (RFR): RFR is an ensemble learning technique that aggregates results from multiple decision trees (classification and regression trees (CART) [16]). For the proposed work, the default model setting provided in scikit-learn library is used.
- Multilayer Perceptron (MLP): In this work, MLP consisting of one input and 5 hidden layers with 30 neurons in each layer; and a final dense layer with 10 neurons is used.

- CNN: The CNN used for the proposed work consists sequentially of: one 1-D convolution layer with kernel size of 3 and 64 filters; one 1-D convolution layer with 64 filters and kernel size of 1; two dense layers with 30 neurons; and a final dense layer with 10 neurons.
- LSTM: LSTM architecture used for the proposed work consists sequentially of: five layers of LSTM each with 30 units; one dense layer with 30 neurons; and final dense layer with 10 neurons.
- CNN-LSTM: The hybrid of CNN and LSTM consists of CNN networks followed by LSTM networks. CNN-LSTM used for the proposed work consists of one 1-D convolution layer with 64 filters and kernel size of 3; three LSTM layers with 30 units; two dense layers with 30 neurons; and final dense layer with 10 neurons.

The performance of RFR, MLP, CNN, LSTM, and CNN-LSTM in terms of RMSE and MAE is shown in Table I. The results show that all the tested models have the capability to capture the complex pattern within the input weather parameters and the output active power of DGs. However, RFR is least sensitive to the parameter variation and the results obtained using RFR are more consistent compared to other tested models.

TABLE I
RMSE AND MAE METRICS FOR THE TESTED MODELS

Metrics	RFR	MLP	CNN	LSTM	CNN-LSTM
RMSE	2.04	2.58	2.70	2.76	2.40
MAE	0.57	0.69	0.58	0.73	0.38

The predicted values obtained from each of the models in the regression stage are compared with real-time measurements obtained from each DG using logistic regression. In this work, the default setting provided in scikit-learn library is used for the logistic regression. Table II shows the performance result, where subscripts with linear regression denote aforementioned regression models and A, P, R, F1-S, and FA denote accuracy, precision, recall, F1-Score, and false alarm, respectively. It can be seen that the logistic regression can detect attacks with all of investigated regression models with high accuracy (above 96%).

TABLE II
ATTACK DETECTION PERFORMANCE OF LOGISTIC REGRESSION

Models	A (%)	P (%)	R (%)	F_1-S (%)	FA (%)
LR_{RFR}	97.29	99.79	84.24	91.36	0.035
LR_{MLP}	96.69	92.86	86.03	89.78	1.153
LR_{CNN}	96.60	95.56	83.90	89.35	0.799
LR_{LSTM}	96.78	91.73	89.12	90.40	1.646
$LR_{CNN-LSTM}$	96.70	94.00	86.10	89.88	1.125

V. CONCLUSION

This paper has proposed a machine learning-based two-stage approach to detect cyber attacks on distributed frequency control strategies. Different machine learning algorithms were used in the first stage (regression) to test their ability to predict the output power of DGs using prominent environmental parameters as input. The predicted values were compared with real-time active power measurements using logistic regression to detect attacks on distributed frequency control. Case studies on IEEE 123-node distribution system showed that the proposed work can detect low margin cyber-attacks on distributed frequency control schemes with as high as 97% accuracy.

ACKNOWLEDGEMENT

This work was supported by the U.S. National Science Foundation (NSF) under Grant NSF 1847578.

REFERENCES

[1] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Unification scheme for managing master controller failures in networked microgrids," *IEEE Transactions on Power Systems*, vol. 35, no. 4, pp. 3004–3014, 2020.

[2] Q. Zhou, M. Shahidehpour, M. Yan, X. Wu, A. Alabdulwahab, and A. Abusorrah, "Distributed secondary control for islanded microgrids with mobile emergency resources," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1389–1399, 2020.

[3] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," in *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, ser. RSES '16. Association for Computing Machinery, 2016.

[4] M. H. Ranjbar, M. Kheradmandi, and A. Pirayesh, "Assigning operating reserves in power systems under imminent intelligent attack threat," *IEEE Trans. on Power Syst.*, vol. 34, no. 4, pp. 2768–2777, 2019.

[5] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Trans. on Indust. Elect.*, vol. 66, no. 2, pp. 1543–1551, 2019.

[6] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[7] L. Lu, H. J. Liu, H. Zhu, and C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.

[8] N. Bhusal, M. Gautam, R. M. Shukla, M. Benidris, and S. Sengupta, "Coordinated data falsification attack detection in the domain of distributed generation using deep learning," *International Journal of Electrical Power Energy Systems*, vol. 134, p. 107345, 2022.

[9] Q. Zhou, Z. Tian, M. Shahidehpour, X. Liu, A. Alabdulwahab, and A. Abusorrah, "Optimal consensus-based distributed control strategy for coordinated operation of networked microgrids," *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 2452–2462, 2020.

[10] S. Manaffam, M. K. Talebi, A. K. Jain, and A. Behal, "Synchronization in networks of identical systems via pinning: Application to distributed secondary control of microgrids," *IEEE Trans. on Control Systems Technology*, vol. 25, no. 6, pp. 2227–2234, 2017.

[11] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded ac microgrids," *IEEE Trans. on Indust. Infor.*, vol. 10, no. 3, pp. 1785–1798, 2014.

[12] Q. Zhou, Z. Li, Q. Wu, and M. Shahidehpour, "Two-stage load shedding for secondary control in hierarchical operation of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3103–3111, 2019.

[13] G. James, D. Witten, T. Hastie, and R. Tibshirani, *An Introduction to Statistical Learning: With Applications in R*. Springer, Dec 2014.

[14] N. Bhusal, M. Gautam, and M. Benidris, "Detection of cyber attacks on voltage regulation in distribution systems using machine learning," *IEEE Access*, vol. 9, 2021.

[15] Distribution System Analysis Subcommittee, "1992 test feeder cases," IEEE, PES, Tech. Rep., 1992. [Online]. Available: http://sites.ieee.org/pestestfeeders/resources/

[16] L. Breiman, "Random forests," *Machine Learning*, vol. 45, pp. 5–32, 2001.