Identification of the False Data Injection Cyberattacks on the Internet of Things by using Deep Learning

Henghe Zheng[1], Xiaojing Chen[2*], Xin Liu[3]
Internet Security and Information Management Center, Jining University, Qufu 273155, Shandong, China[1]
Library, Zhejiang Gongshang University, Hangzhou 310018, Zhejiang, China[2]
Information Technology Center, JiNing Medical University, Jining 272067, Shandong, China[3]

***Abstract*—With the expanding utilization of cyber-physical structures and communication networks, cyberattacks have become a serious threat in various networks, including the Internet of Things (IoT) sensors. The state estimation algorithms play an important role in defining the present operational scenario of the IoT sensors. The attack of the false data injection (FDI) is the earnest menace for these estimation strategies (adopted by the operators of the IoT sensor) with the injection of the wicked data into the earned mensuration. The real-time recognition of this group of attacks increases the network resilience while it ensures secure network operation. This paper presents a new method for real-time FDI attack detection that uses a state prediction method basis on deep learning along with a new officiousness identification approach with the use of the matrix of the error covariance. The architecture of the presented method, along with its optimal group of meta-parameters, shows a real-time, scalable, effective state prediction method along with a minimal error border. The earned results display that the proposed method performs better than some recent literature about the prediction of the remaining useful life (RUL) with the use of the C-MAPSS dataset. In the following, two types of attacks of the false data injection are modeled, and then, their effectiveness is evaluated by using the proposed method. The earned results show that the attacks of the FDI, even on the low number of the sensors of the IoT, can severely disrupt the prediction of the RUL in all instances. In addition, our proposed model outperforms the FDI attack in terms of accuracy and flexibility.**

Keywords*—Cyberattacks; false data injection (FDI) attacks; internet of things (IoT); deep learning

I. INTRODUCTION

The current developments and the rapid growth of the Internet of Things sensors have increased the possibility of predictive maintenance. This capability is a method for the prevention of asset damage by the generation of data analysis and the template identification for the prediction of the subjects before which they occur. Using these PdM techniques leads to an $20\% - 25\%$ increment in productivity, a 35%−45% decrease in downtime and the 25%−20% decrease in maintenance cost [1]. Due to this good feature, the equipped PdM solutions with machine learning and IoT sensors are transforming the transportation, oil, gas, aerospace, automotive, national defense and construction industries. For example, recently, the algorithms of deep learning have displayed massive achievement in these applications [2]. However, unfortunately, the sensors of the IoT and the algorithms of deep learning widely are delicate to cyberattacks [3]. This bad feature is a considerable menace to the overall system of the PdM. Due to the provided reportage by Malwarebytes, the cyber menace versus the factories/occupations has enhanced to over 200% in the prior year [4].

In particular, recognizing covert attacks like the false data injection (FDI) attack [5] in the PdM system is quite challenging due to the unique nature of this attack type. The attack of the false data injection (FDI) [5] is in such a way that an attacker secretly compromises the measurements of the sensors of IoT. This is done by the method that the measurements of the manipulated sensor bypass the original detection method of the "defective data" by the sensors. Then they propagate into the output of the sensor. The attack of FDI can be fulfilled by completing the communication network of the sensors, the physical sensors and the processing applications of the data. These types of attacks in the system of PdM may not even display their effect. But, in lieu, the attack propagates aboard the sensor to the machine learning part of the system of PdM. Next, it tricks the system with the prediction of the possession defeat and or the interval of the delayed maintenance. It may evince a considerable cost with the creation of an unplanned defeat and or human life loss on the applications of the safety-critical [6], [7], [8]. In the past, the attacks of the FDI have made the very incidents of the known catastrophic. The most important example is the Northeast blackout in the United States in 2003 and the attack on the Ukrainian power grid. These attacks have influenced more than 230,000 people. They have been without power for multiple hours. A vast investigation has been done about the identification and reduction of the attacks of FDI in the field of cyber-physical systems [9], [10], [11]. The current users of this type of system for aircraft engine maintenance are Honeywell, Rolls-Royce, Pratt & Whitney, US Air Force and General Electronics [6], [12], [13].

The proposed solutions for sensor attack detection, which are provided so far in the field of the system of cyber-physical and IoT, are not enough for the solution of this subject because utmost of the existing method travail from the scalability subjects and the resource overhead when they deployed individually on thousands of the sensors. Many IoT sensors have limited power and limited resources. This paper presents a real-time attendance recognition method for these attacks in earned mensuration by applying the models of deep learning for the precise state prediction along with an impressive abnormal identification approach in the predicted

states with the use of the matrix of the error covariance. When the change rate of the eigenvalues of the error covariance matrix exceeds a predefined threshold, then the network operator indicates the presence of the attack of FDI on a collection of the accessible mensuration. This shows an effective deployment of the scalable 920D. Therefore, our article contributions are as the below:

- By effectively adjusting the presented deep learning-based method parameters, a collection of the indices of the minimum error have been obtained. An encyclopedic compersion between two non-uniform deep learning-based methods and a conventional ML-based method, such as the SVM and an actuarial prediction method, such as the integrated moving average of the autoregressive, is carried out in this work.
- By incorporating the noise into the existing mensuration, the presented deep learning-based method provides flexible action with minimal changes on the indices of the error.
- The presented abnormal recognition scheme shows a robust, real-time and excellent FDI attack recognition approach with the tracking of the change rate of the eigenvalues of the matrix of the error covariance.
- Since our presented method does not require the major modification of the standard BDD, therefore, it represents a cost-impressive method.

The continuation of this paper is as the below: In Section II, the related works is presented. In Section III of the paper, the proposed algorithm details are presented. Then, Section IV presents the earned results from the designed experiments. Eventually, Section V presents the potential conclusions and future perspectives.

II. Related Works

The available studies on the data injection attacks on smart networks are listed in [27] to [35]. The work in [29] introduces an analysis of the economic effects of data injection on electricity markets in the smart power grid. In this reference, it is assumed that an attacker participates in the virtual transactions of the electricity market with complete information that he has from the network and it designs his attack strategy based on the manipulation of the electricity price in order to maximize the profitability and by observing all the limitations of the attack. In [30], the operation of the data injection attack in the electricity market environment is considered for a connected micro-grid to the power system. This attack can affect the optimal outputs of micro-grid energy management, such as the total cost of production. The research in [31] suggests the monetization of malicious data attack on electric energy production markets and the necessary strategy to maximize the revenue. The study in [32] proposes LR as a type of FDIA that the load distribution attack can affect the operation of the smart grid by attacking the economic load distribution bound by the security constraints (SCED). To solve this problem, [33] has introduced the problem of the distributed resilient economic load distribution under cyber-attacks. With the aim of directly controlling local marginal prices (LMPs) in real time through FDIA, [34], a control theory based on a method is presented to analyze the effect of attack implements pricing stability.

In [35] and [36], a zero-sum game is formulated between an attacker and a defender, in which the attacker changes the estimated throughput of the lines to manipulate the prices. According to this game theory, a two-level optimization problem is formed. In [37] and [38], the economic effect of the structured information attacks as a generalized type of FDIA in electricity markets by using the virtual bidding activities is studied. The structured information of smart grids is used to exploit the system for management. The network is very vital in a safe way, but this information can be manipulated by a cyber-attacker by changing the on/off state of the power switches. In addition to these, recently in [39], an attack strategy has been proposed in which a cyber-attacker can effectively change LMPs by manipulating some vital parameters of the model and achieve the financial gain. Also, an FDIA can be well matched with a coordinated physical attack and actually create a coordinated physical-cyber-attack (CCPA), which has a more destructive effect on the normal operation of the smart network.

In [40], the coordinated attack includes connecting the physical shortening of the transmission lines, after infiltrating the communication network with the cyber protection layers. The research in [41] has designed a CCPA with the aim of maximizing disruption in the day-ahead (DA) and real-time electricity markets. The study in [42], an attack of a CCPA based on AC state estimation proposes to disrupt the operation of the electricity market by manipulating the nodal prices. All the above related studies are based on the hypothesis that the cyber attacker has complete knowledge about the target smart grid information, which includes the network topology, the branch parameters, etc. In fact, in any given smart grid, the network information is vast and highly secure and vital. Moreover, information is dynamic; because the network topology can be reconfigured in both normal and event situations. Therefore, in practice, it is very difficult for a limited attacker to access the complete information of the network. In several recent works based on [33] to [35], this aggressive challenge in FDIA design has been addressed to some extent according to different tools, techniques and requirements.

In study [43], the attacker has formulated a secret profitable attack without prior knowledge of network topology and only through phasor observations by using the linear independent component analysis. In study [44], the attacker designs an online attack strategy against the real-time electricity market based only on real-time information received from measuring devices and without the need for the network topology information. A profitable data injection attack on electricity markets by limited attackers with incomplete network information is studied in [45]. In this reference, the uncertainties associated with random network information, a model and a possible framework for designing an undetectable and profitable attack are presented. One of the problems in this reference is the need for past data to properly

estimate the probability distribution functions of the parameters.

III. Proposed Scheme for the FDI Attack Detection

In this section, the presented method for detecting the attacks of false data injection is detailed. For this purpose, first, a brief explanation of these types of attacks and how the definition of them are provided. In the following, the proposed scheme is expressed.

A. Definition of FDI Attack

At first, it should be stated that the only purpose of the attack of the FDI is the bypassing of the remaining test in the centers of control with the attenuation of the climacteric vulnerabilities of the sensors and RTUs. This progressive cyberattack scheme in various networks (such as the Internet of Things) leads to the change of a group of the state estimations from a group of the obtained mensuration. A vector expansion approach of the indiscoverable covert attack for the nonlinear algorithm of the state prediction is presented, which shows:

$$a_1 = h(\hat{x}_{a_1}) - h(\hat{x}) \quad (1)$$

$$\hat{x}_{a_1} = \hat{x} + c' \quad (2)$$

$$z_{a_1} = z + a_1 \quad (3)$$

where, $a_1 \in R^m$ represents the vector of the injected attack to the obtained collection of the mensuration z for the presentation of a group of the corrupt mensuration $z_{a_1} \in R^m$. Therefore, it creates a set of the false estimation states $\hat{x}_{a_1} \in R^n$. The statistical remaining test, which is performed by the BDD in the above conditions, can be seen as follows:

$$r_{a_1} = ||z_{a_1} - h(\hat{x}_{a_1})||_2 = ||z + a_1 - h(\hat{x}_{a_1}) + h(\hat{x}) - h(\hat{x})||_2 = ||z - h(\hat{x})||_2 = r \quad (4)$$

From the above equations, it can be seen which vector of the extended attack can bypass as successfully the remaining test. Therefore, it leads to climacteric operational scenarios.

The existing operators in the center of the control adopt the algorithms of the state prediction for the definition of the climacteric network actions, such as the load prediction, the load distribution of the economy, and so on [14]. The mensuration in the SCADA is broadcasted via BDDs to meet the integrity and the quality of the mensuration. Then the bad information removes according to the noise in the networks of communication, the meter malfunction, and so on. In most of the unfavorable papers [15], [16], [17], a method of the nonlinear state prediction is presented, that is shown as follows:

$$z = h(x) + e_1 \quad (5)$$

where, z $\in R^m$ represents the available measurements which are obtained from the BDDs. Also, x $\in R^n$ represents the set of operational states while $e_1 \in R^m$ displays the vector of the error for the prediction method. Furthermore, $h()$ represents the nonlinear function that draws a collection of the obtained mensuration by the network operational states. For the estimation of a collection of the operational states with the use of the method of the nonlinear state prediction as displayed in Eq. (5), a flattish start method is adopted, as is displayed in Eq. (6):

$$x[0] = [0\ 0\ ...\ 1\ 1]^T \quad (6)$$

With the use of the flattish start method, an iterative Gauss-Newton approach is performed for the determination of a set of estimated states. In it, the matrix of Jacobian J $\in R^{m\times n}$ is reformulated in each epoch. The exiting BDD in the EMS module on the SCADA performs the remaining test of the actuarial that is shown below:

$$r = ||z - h(\hat{x})||_2 \leq \tau \quad (7)$$

where τ depends on the degrees of freedom $(m - n)$ throughout the specified system, since the obtained mensuration has enough redundancy on them, the mensuration, which shows the remaining higher than τ, successfully scraped as the worst possible information.

B. Proposed Scheme

The accurate and impressive performance of the analysis based on the regression has been demonstrated by the methods of deep learning. This data-driven prediction approach has shown the onomastic error in forecasting [18], [19], [20]. The current article considers MAE, MSE and RMSE for the performance parameters that are defined below:

$$\text{RMSE} = \sqrt{\sum_{a''=1}^{b''} \frac{(f''_{a''} - s''_{a''})^2}{b''}} \quad (8)$$

$$\text{MSE} = \sum_{a''=1}^{b''} \frac{(f''_{a''} - s''_{a''})^2}{b''} \quad (9)$$

$$\text{MAE} = \sum_{a''=1}^{b''} \frac{|f''_{a''} - s''_{a''}|}{b''} \quad (10)$$

The estimated operational states with f, is denoted and the actual operational states with s is denoted. The bald number of the instances for the estimation is b''. With the effective optimization of the meta-parameter, the presented neural network by the scenario of the network steady-state effectively can estimate the predicted states by the lowest value for the performance parameters. In the current article, a strong nonlinear structure of the LSTM is proposed.

The LSTM model is a particular architecture from the RNN that helps with the learning of the patterns of the complex temporal, which are provided in the dataset of the training. This particular type of RNN is able to the nature maintaining of the data at a given step of the time. Thus, the LSTM provides the possibility to read, retain, and remove the data from the memory cells by setting three distinct controllable gates, which is named the gate of the forget $g''_1(t)$, the gate of the input $j''_1(t)$ also, the gate of the output $p''_1(t)$. Fig. 1 shows the structure with the single cell for a module of LSTM. Also, the model of the presented LSTM is displayed in Fig. 2.

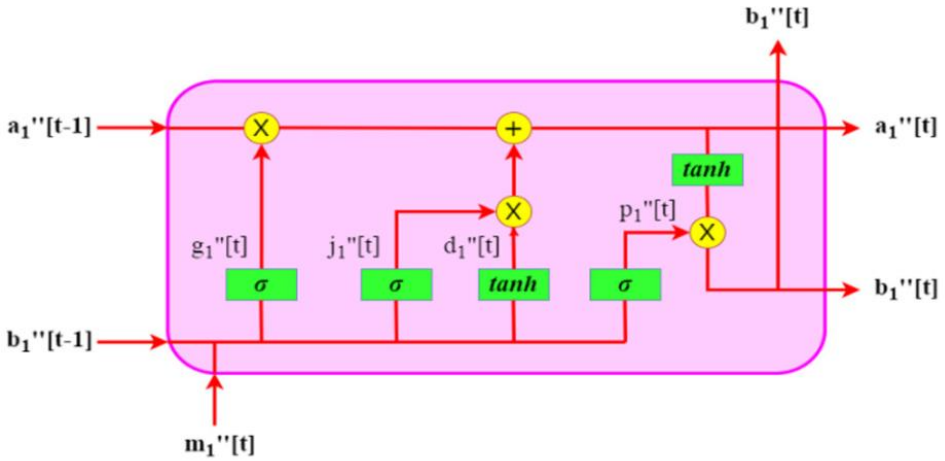

Fig. 1. Single-cell structure from an LSTM cell.

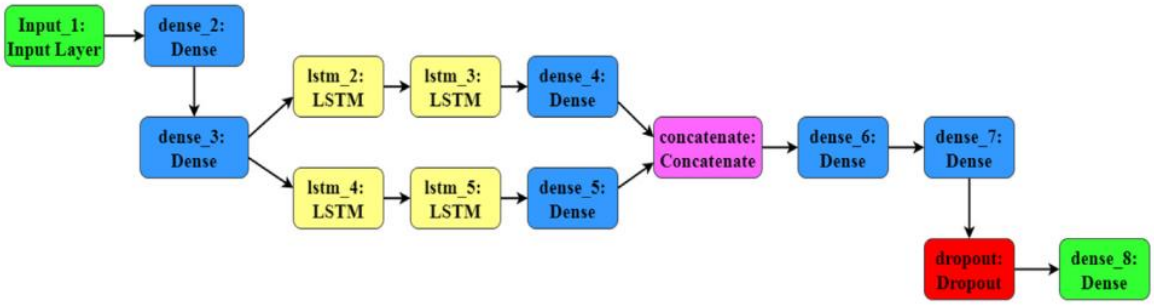

Fig. 2. The proposed LSTM model.

The admission or the rejection of the information in the form of the binary (0 or 1), which is related to the current state of the cells, depends on the gate $g''_1(t)$. The forget gate is defined by Eq. (11). On the modules of LSTM, the activation function of *sigmoid* is used. $j''_1(t)$ represents the gate of the input from the module of LSTM, which is displayed in Eq. (13). For the updation of the state of the current cell, generally, a decision of the binary by means of the gate of the input is taken. For the module of LSTM, the updated cell state is denoted with $a''_1(t)$ also, the novel contributor is $d''_1(t)$. As shown in Eq. (15), the accumulated data is discharged to the next neurons. The weights with $w''_{1(.)}$ is denoted. Also, the outputs are denoted with $b''_1(t)$, the inputs are denoted with $m''_1(t)$ and finally, the biases are denoted with $b''_{1(.)}$. These cases are shown in Eq. (11) to Eq. (16). The concatenation operation is indicated by $[.,.]$.

$$g''_1(t) = sig(w''_{1_{g''_1}}[b''_1(t-1).m''_1(t)] + b''_{1_{g''_1}}) \quad (11)$$

$$a''_1(t) = [g''_1(t) \times a''_1(t-1)] + [j''_1(t) \times d''_1(t)] \quad (12)$$

$$j''_1(t) = sig\left(w''_{1_{j''_1}}[b''_1(t-1).m''_1(t)] + b''_{1_{j''_1}}\right) \quad (13)$$

$$d''_1(t) = \tanh\left(w''_{1_{d''_1}}[b''_1(t-1).m''_1(t)] + b''_{1_{d''_1}}\right) \quad (14)$$

$$p''_1(t) = sig\left(w''_{1_{p''_1}}[b''_1(t-1).m''_1(t)] + b''_{1_{p''_1}}\right) \quad (15)$$

$$b''_1(t) = p''_1(t) \times \tanh(a''_1(t)) \quad (16)$$

Fig. 2 displays which the model of the presented LSTM has $eight$ layers hidden along with one layer of the output and one layer of the input. It can be viewed that in the second layer of the hidden, the model is divided into the layers of the sub-hidden. These layers of the sub-hidden combine the structures of LSTM by the neural networks of the dense for improvement of the efficiency of the state prediction. These models of the nonlinear are found by the layers of the sub-hidden for the representation of a superior approach for the prediction. Finally, all layers of the sub-hidden are compromised in a common layer which is called the layer of the concatenation. Two layers of the dense are placed in place of the layer of the concatenation, and then the layer of the output is placed. The drop-out regularization is effectively adopted for the avoidance of the model over-inflating. The proposed nonlinear method is fed with the activation function of *ReLU* to each layer which is expressed by Eq. (17).

$$y''_{1_{i'_1}} = ReLU(w''_{1_{i'_1}} k'_{1_{i'_1}} + b'''_{1_{i'_1}}) \quad (17)$$

For layer i'_1, the set of predicted features is equal to $y''_{1_{i'_1}}$ and the input features are equal to $k'_{1_{i'_1}}$. Other parameters of a specific layer consist of bias $b'''_{1_{i'_1}}$ and weight $w''_{1_{i'_1}}$. The output of the layer of LSTM from the presented nonlinear method is directly entered into the next layer of the dense that this layer has the activation function of *ReLU*. The layer of the

output of this nonlinear method includes an activation function of *ReLU* according to Eq. (17). The proposed model is trained in 500 iterations and using the optimizer of *Adam*. The initial rate for the learning of the proposed method is equal to 0.001.

By effectively training the model, a superior policy can be demonstrated for the estimation of states by the indices of the minimum error. The scheme of the real-time FDI attack recognition, which is the basis of the matrix of the error covariance, is presented in Fig. 3. The algorithm of the presented anomaly detection performs the vector of the developed error according to the predicted operational states and predicted operational states in the SCADA.

$$e(t) = \hat{x}_{for}(t) - \hat{x}_{test}(t) \tag{18}$$

$\hat{x}_{for}(t) \in R^n$ represents the predicted set from the estimated states, which is obtained by the benchmark of the scalable nonlinear neural network and $\hat{x}_{test}(t) \in R^n$ represents the predicted states of the step of the time t, which are recovered with the use of the algorithm of the state prediction. Also, $e(t) \in R^n$ represents the error vector.

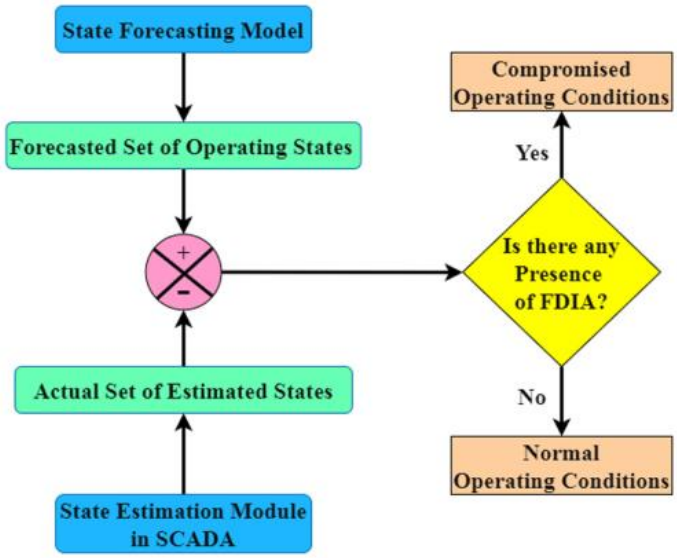

Fig. 3. The proposed method for the detection of the attack of FDI.

The main purpose of the method of anomaly recognition is the identification of the eigenvalues change rate of the matrix of the error covariance, which is displayed as follows:

$$\frac{d\mu}{dt} = x_1^T(t)\frac{dE(t)}{dt}x_1(t) \tag{19}$$

$$\frac{dE}{dt} \approx \frac{E(t)-E(t-\delta t)}{\delta t} \tag{20}$$

$x_1(t) \in R^n$ represents the eigenvector for the matrix of the error covariance $\mathrm{E(t)} \in R^{n\times n}$ which is generated pending the time of the current sampling t. Since $E(t)$ and $E^T(t)$ are the matrices of the symmetric positive definite covariance. Therefore, these matrices have the same eigenvalues and the same eigenvectors. The change rate of the eigenvalues among two intervals of the consecutive time t and $(t-\delta t)$ can be shown by Eq. (19) and Eq. (20), respectively. The proposed detection scheme for the FDI attack that performs the change rate of eigenvalues is described as follows:

$$\varepsilon = \begin{cases} 1 & \frac{d\mu}{dt} > RMSE + \delta_1 \\ 0 & otherwise \end{cases} \tag{21}$$

where ε displays the criterion of the recognition that is adjusted with 1. Thus, if the change rate of eigenvalues in a specific time t exceeds a particular threshold, as is displayed in Eq. (21), it shows the presence of the FDI attack inside the obtained measurements. δ_1 displays a numerical constant with a very small positive value which belongs to the operator knowledge. This parameter inherently is insignificant because the model of the nonlinear state prediction shows better accuracy for prediction.

IV. Evaluation Results of the Proposed Method

In this section, the results of the evaluation of the presented method are examined. First, the used dataset is described. In the following, the results of the proposed deep learning method for the prediction of RUL are evaluated. Then, the continuous and temporary signatures from the FDI attack are provided, and then the attack's impact on the prediction of RUL is stated. The Python programming language has been used for the implementation of these tests. The presented method is implemented on a computer which has a Core (TM) i7 CPU, 3.0 GHz Intel(R) and 8G RAM.

A. Used Dataset

For the performance evaluation of the presented method, the dataset of the NASA C-MAPSS turbofan engine destruction simulation is used. The used dataset consists of 21 data of the sensor by the number of the conditions of the operational and the conditions of the different error. On the used dataset, four subsets (FD001-04) are defined. Each subset includes the data from the training and the data from the test. The data of the test is reached to the data of the defeat from the multiple engines with the same group. In the data of the test, each row is a cycle of time that is defined as one hour of working. A cycle of time has 26 columns which column 1

displays the ID of the engine and column 2 displays the number of cycles of the current operation. Columns 3 to column 5 display the three settings of the operational and also, the columns 6 to column 26 display the 21 values of the sensor. The data of the time series is only terminated when it encounters an error. The data of the test consist of only the information for some cycles of the time because our purpose is the estimation of the cycles of the time of the remaining operational before the occurrence of a defect.

B. Results of the Proposed Method of RUL Prediction

For the confirmation of the proper efficiency of the presented algorithm, which is the basis of the LSTM, this method has been evaluated on the dataset of C-MAPSS. For the performance evaluation of predictors, RMSE, MSE and MAE are used. These metrics are widely used as the criteria of evaluation in the studies of the evaluation of the model. The results are related to the network, which this network has 100 nodes in the layers hidden from the first layer. In addition, it has 100 nodes in the layers hidden from the second layer and 100 nodes in the layers hidden from the third layer.

Furthermore, the length of its sequence is equal to 80. Table I shows the meta-parameters of the proposed LSTM model (inspired by [21]). Fig. 4 shows the performance results of the presented method. Also, Table II shows the results of the error evaluation for the presented method and the similar presented methods in [22], [23] and [24].

TABLE I. THE HYPER-PARAMETERS SETTINGS OF THE PRESENTED LSTM MODEL

Model	Hidden Neuron	Dro-pout	Batch Size	Epochs	Activation Function
LSTM	100	0.2	200	100	ReLU

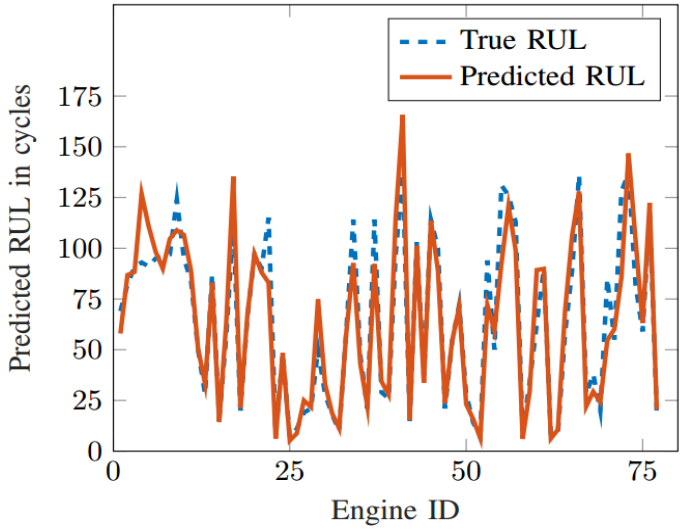

Fig. 4. The comparison results of the prediction of RUL by the proposed scheme and the actual RUL value.

TABLE II. THE COMPARISON RESULTS BETWEEN THE PRESENTED METHOD AND THE SIMILAR METHODS

Model	RMSE	MSE	MAE
Proposed LSTM	6.948	3.241	132.894
Proposed in [22]	7.422	5.022	145.488
Proposed in [23]	9.711	8.925	150.961
Proposed in [24]	13.324	10.052	166.922

It is evident from Fig. 4 and Table II that the proposed algorithm with a sequence length equal to 80 has the lowest amount of error. This means that the presented method is very precise about the prediction of RUL on the used dataset. It should be noted that the displayed results in Table II state that the prediction method basis on LSTM does much better than the presented works on [22], [23] and [24]. In the next stage, the attack of FDI in the proposed LSTM-based method is modeled for the evaluation of their resilience against the attack of FDI.

C. Modeling Two FDI Attack Scenarios and the Impact Examination of these Attacks in RUL Prediction

The average engine degradation point N_{avg}^{d}, for the FD001 dataset, is taken to be 130 [25]. It is assumed that the system of the monitoring dispatches 20 cycles of the time (N_b) from the data to the side of the ground. The dataset of the training and the dataset of the test have 21 data of the sensor. The attack of FDI is performed in 21 sensors. However, for the creation of the realistic attack, the FDI attack only in *three* sensors ($T24$, $P30$ and $T50$) is performed. The details of 21 sensors are provided in [26]. On the first FDI attack scenario,

i.e. the scenario of the continuous, the attacker has begun the attacks since N_{avg}^{d} (that is equal to 130-time cycles) and the duration of the attacks is up to the engine life's end. In the second scenario of an FDI attack, i.e. scenario temporary, the attacker has begun the attacks since N_{avg}^{d} (that is equal to 130 cycles of time). The duration of these attacks is 20 hours. With respect to the attack begins, since 130 cycles of the time, only the engines with data greater than 130 cycles are considered. In the FD001 dataset, the number of these engines is equal to 37. The resulting dataset is re-appraised with the use of the proposed LSTM-based model. The obtained values for RMSE, MSE and MAE are respectively equal to 20.651, 10.236 and 159.415.

To model the FDI attack on the sensors, a null vector is added to the main vector that changes the output of the sensor with a so little border equal to 0.01% to 0.05% for a random FDI attack and equal to 0.02% for a biased FDI attack. Here, the random FDI attack means that the added noise to the output of the sensor has a span equal to 0.01% to 0.05%. At the same time, the biased FDI attack adds a fixed noise value to the output of the sensor. Fig. 5 displays a collation of the signal of the output of the main FDI attack and the signal of the output of the biased FDI attack from the second sensor for the engine with an ID equal to 3. On the continuous attack of FDI, the output of the sensor from 130 cycles of time up to the engine life end is attacked. In the case of a biased attack of FDI for a period of the temporary, similar to Fig. 6, the duration of the attack only is 20 cycles of the time (130 cycles of the time to 150 cycles of the time). Be careful; on the limited attack, the attacker has restricted accessibility to the sensors. Similar to Fig. 5 and Fig. 6, the attack signature is very analogous to the main signal. Its detection makes it hard even with the common defense mechanisms.

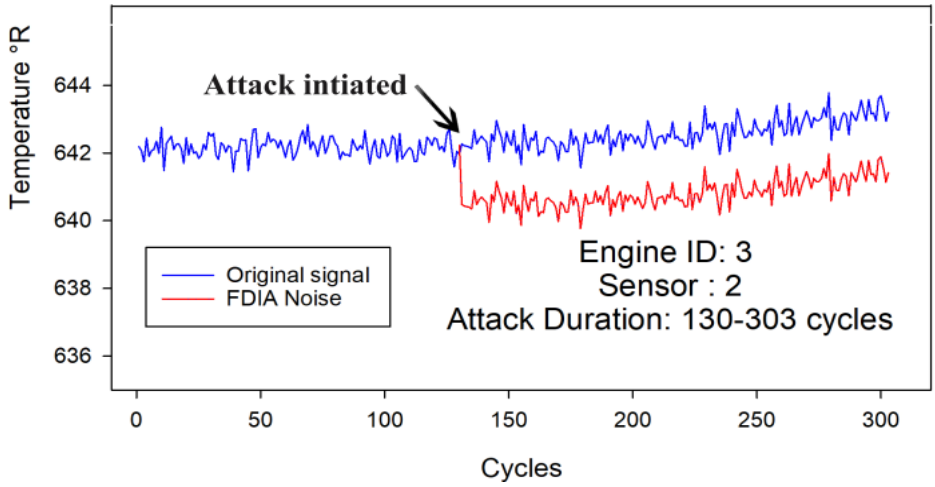

Fig. 5. The continuous FDI attack signature.

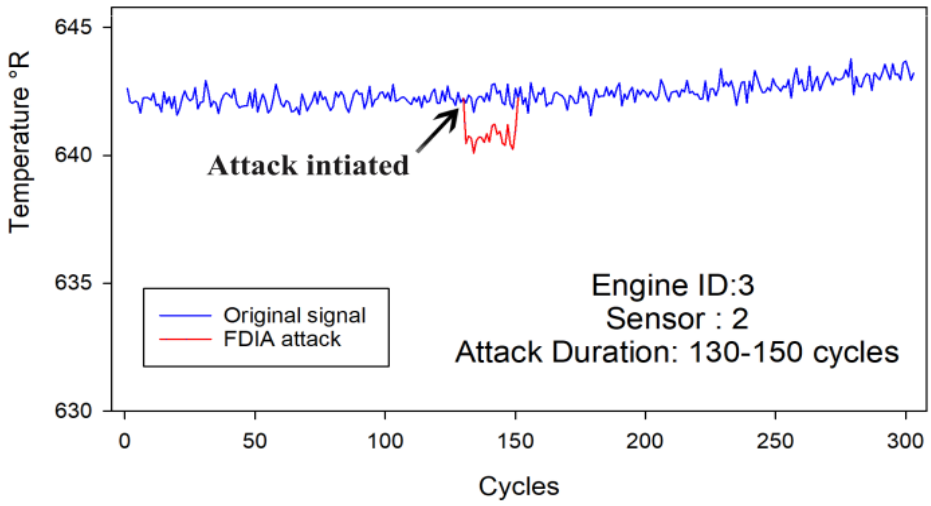

Fig. 6. The temporary FDI attack signature.

Now, the effect of the scenarios of the attack of FDI on the proposed LSTM-based method is investigated. To demonstrate the effect of attack of the attack of FDI on the system of monitoring, an attack by the mentioned scenario is ran. The FDI attack in three sensors ($T24$, $P30$ and $T50$) is performed instead of the attack in all 21 sensors of the dataset. In the scenario of the continuous FDI attack, the attacker makes the attacks from 130 cycles of time until the end of the engine life. It is clear from Fig. 7 that the proposed LSTM-based method is greatly affected by the continuous attack of

FDI. About the fortuitous FDI attack and the biased FDI attack, the random FDI attack has shown a significant impact on the proposed LSTM-based model. Table III shows the relevant results.

In the scenario of the temporary FDI attack, the attacker makes the attacks between 130 cycles of time and 150 cycles of time. It is clear from Fig. 8 that the proposed LSTM-based method is greatly affected by the temporary attack of FDI. Table IV shows the relevant results. With the comparison between the continuous FDI attack and the temporary FDI attack, it can be seen that the error of a continuous attack of FDI is almost twice the error of a temporary attack of FDI. Hence, continuous FDI attacks are stronger than temporary FDI attacks.

D. Discussion

In this work, the proposed method is evaluated on the dataset of C-MAPSS, and the obtained results show the great prospects for deep learning in PdM. It is also observed that sequence length and network architecture are very important in accurately predicting RUL. The proposed work shows that the proposed method is several times better than recent works that use deep learning on the dataset of C-MAPSS. The analysis of the impact of an FDI attack on aircraft sensors in the dataset of CMAPSS provides interesting insights. It is observed that the CNN-based model is strongly affected by random and biased FDI. In the case of temporary FDI, the random and biased RMSE of CNN is several times higher than the true RMSE, and in the case of continuous, the random and biased RMSE is several times higher than the true RMSE. Also, it is observed that the CNN-based model is more flexible in both random and biased cases in compared to other models. In the case of temporary attack, the random and biased RMSE is several times higher than the true RMSE, which makes it disastrous for the PdM system. This may lead to delays in timely maintenance of the aircraft engine and ultimately lead to engine failure in some cases.

Note, the FDI attack signature is very close to the original sensor output, which makes it more difficult to detect by common defense mechanisms in the engine health monitoring system. A piecewise prediction approach is used in visualizing the impact of attacks on sensors, which clearly shows that the PdM system is susceptible to sensor attacks. The CNN-based prediction results show that special measures should be taken when designing and by using PdM systems because they are very sensitive to FDI. Such an analysis can serve as empirical guidance for the development of subsequent data-driven PdM systems. All these obtained results show that DL-based PdM systems have good prospects for aircraft maintenance; however, they are highly susceptible to sensor attacks. Hence, it is necessary to explore suitable detection techniques to identify such stealth attacks and special care should be taken when building IoT sensors for DL/AI applications. For this reason, when designing a PdM system, the designer should also consider the flexibility of the DL algorithm instead of emphasizing the accuracy of the algorithm.

TABLE III. THE RELEVANT RESULTS TO THE SCENARIO OF THE CONTINUOUS ATTACK OF FDI

Model	RMSE	MSE	MAE
Model Under Random FDI Attack	50.325	25.614	1036.234
Model Under Biased FDI Attack	37.512	19.512	797.328

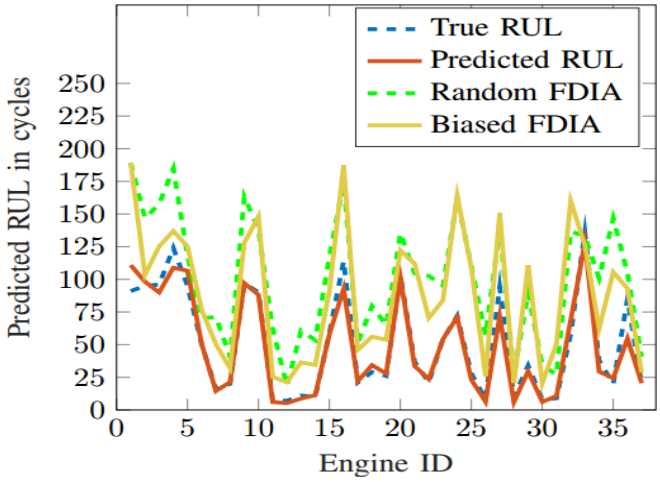

Fig. 7. The relevant results to the RUL prediction in the scenario of the continuous attack of FDI.

TABLE IV. THE RELEVANT RESULTS TO THE TEMPORARY FDI ATTACK SCENARIO

Model	**RMSE**	**MSE**	**MAE**
Model Under Random FDI Attack	27.651	14.351	548.678
Model Under Biased FDI Attack	19.547	10.985	410.365

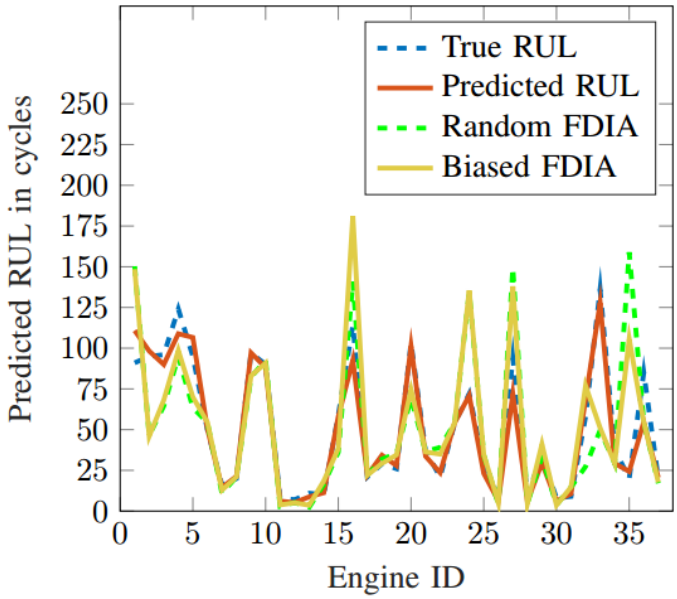

Fig. 8. The relevant results to the RUL prediction in the temporary FDI attack scenario.

V. Conclusions and Suggestions

With the expansion of the use of cyber-physical structures and communication networks, cyberattacks have become a serious threat in various networks, including the sensors of the Internet of Things. These attacks create the so assailable conditions. Therefore, the main consideration of this current paper is the detection in real-time of the done FDI attack on the Internet of Things, which is related to the estimated RUL prediction. The robust and nonlinear structure of the LSTM shows a better view of the RUL prediction compared to similar methods. The method of the presented nonlinear LSTM is successfully implemented in real-time because the efficiency of its computational (the time of the test and the time of the training) is on the scope of the microseconds. In the future, the method of the presented detection can be performed by the scenarios of the contingency of the smart networks and by a more intransigent constraint on the criterion of detection, which ultimately results in a stronger feasibility of the FDI attack detection. Also, an end-to-end method can be developed for the recognition and reduction of attacks on the sensor in a system of network health monitoring.

References

[1] K. Alnowibet, A. Annuk, U. Dampage, and M. A. Mohamed, "Effective energy management via false data detection scheme for the interconnected smart energy hub–microgrid system under stochastic framework," Sustainability, vol. 13, no. 21, p. 11836, 2021.

[2] M. A. der Mauer, T. Behrens, M. Derakhshanmanesh, C. Hansen, and S. Muderack, "Applying sound-based analysis at porsche production: Towards predictive maintenance of production machines using deep learning and internet-of-things technology," Digitalization cases: How organizations rethink their business for the digital age, pp. 79–97, 2019.

[3] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," arXiv preprint arXiv:1802.02041, 2018.

[4] D. An, Q. Yang, W. Liu, and Y. Zhang, "Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach," IEEE Access, vol. 7, pp. 110835–110845, 2019.

[5] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," IEEE Trans Control Netw Syst, vol. 1, no. 4, pp. 370–379, 2014.

[6] D. An, F. Zhang, Q. Yang, and C. Zhang, "Data integrity attack in dynamic state estimation of smart grid: Attack model and countermeasures," IEEE Transactions on Automation Science and Engineering, vol. 19, no. 3, pp. 1631–1644, 2022.

[7] Y. An and D. Liu, "Multivariate Gaussian-based false data detection against cyber-attacks," IEEE Access, vol. 7, pp. 119804–119812, 2019.

[8] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "A brief survey of deep reinforcement learning," arXiv preprint arXiv:1708.05866, 2017.

[9] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Trans Smart Grid, vol. 8, no. 4, pp. 1630–1638, 2016.

[10] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," J Parallel Distrib Comput, vol. 103, pp. 32–41, 2017.

[11] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," IEEE Trans Signal Inf Process Netw, vol. 4, no. 1, pp. 48–59, 2017.

[12] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," IEEE Trans Smart Grid, vol. 9, no. 3, pp. 1636–1646, 2016.

[13] N. I. Haque et al., "A survey of machine learning-based cyber-physical attack generation, detection, and mitigation in smart-grid," in 2020 52nd North American Power Symposium (NAPS), IEEE, 2021, pp. 1–6.

[14] A. Abur and A. G. Exposito, Power system state estimation: theory and implementation. CRC press, 2004.

[15] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 1, pp. 1–33, 2011.

[16] F. Wen and W. Liu, "An efficient data-driven false data injection attack in smart grids," in 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), IEEE, 2018, pp. 1–5.

[17] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," IEEE Transactions on Signal Processing, vol. 63, no. 5, pp. 1102–1114, 2014.

[18] D. Mukherjee, S. Chakraborty, P. K. Guchhait, and J. Bhunia, “Machine learning based solar power generation forecasting with and without MPPT controller,” in 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE), IEEE, 2020, pp. 44–48.

[19] D. Mukherjee, S. Chakraborty, P. K. Guchhait, and J. Bhunia, “Application of machine learning for speed and torque prediction of pms motor in electric vehicles,” in 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE), IEEE, 2020, pp. 129–133.

[20] D. Mukherjee and S. Chakraborty, “A deep learning approach for an effective speed and torque forecasting policy of PMS motors in electric vehicles,” in 2022 second international conference on power, control and computing technologies (ICPC2T), IEEE, 2022, pp. 1–6.

[21] A. L. Ellefsen, E. Bjørlykhaug, V. Æsøy, S. Ushakov, and H. Zhang, “Remaining useful life predictions for turbofan engine degradation using semi-supervised deep architecture,” Reliab Eng Syst Saf, vol. 183, pp. 240–251, 2019.

[22] D. Mukherjee, S. Chakraborty, R. Banerjee, and J. Bhunia, “A novel real-time false data detection strategy for smart grid,” in 2021 IEEE 9th Region 10 Humanitarian Technology Conference (R10-HTC), IEEE, 2021, pp. 1–6.

[23] D. Mukherjee, S. Chakraborty, R. Banerjee, J. Bhunia, and P. K. Guchhait, “A novel deep learning framework to identify false data injection attack in power sector,” in TENCON 2021-2021 IEEE Region 10 Conference (TENCON), IEEE, 2021, pp. 278–283.

[24] D. Mukherjee and S. Chakraborty, “Real-time identification of false data injection attack in smart grid,” in 2021 IEEE Region 10 Symposium (TENSYMP), IEEE, 2021, pp. 1–6.

[25] F. O. Heimes, “Recurrent neural networks for remaining useful life estimation,” in 2008 international conference on prognostics and health management, IEEE, 2008, pp. 1–6.

[26] D. K. Frederick, J. A. DeCastro, and J. S. Litt, “User’s guide for the commercial modular aero-propulsion system simulation (C-MAPSS),” 2007.

[27] A. Xu, et al., "Research on false data injection attack in smart grid," in IOP Conf. Series: Earth and Environmental Science, Proc. 8th Annual Int. Conf. on Geo-Spatial Knowledge and Intelligence, vol. 693, Article ID: 012010, Xi'an, Shaanxi, China, 18-19 Dec. 2020.

[28] Q. Zhang et al., "Profit-oriented false data injection on energy market: reviews, analyses and insights," IEEE Trans. on Industrial Informatics, vol. 17, no. 9, pp. 5876-5886, Sept. 2020.

[29] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," IEEE Trans. on Smart Grid, vol. 2, no. 4, pp. 659-666, Dec. 2011.

[30] B. Jin, C. Dou, and D. Wu, "False data injection attacks and detection on electricity markets with partial information in a micro - grid - based smart grid system," International Trans. on Electrical Energy Systems, vol. 30, no. 12, Article ID: e12661, Dec. 2020.

[31] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on realtime electricity market," in Proc. IEEE In. Conf. on Acoustics, Speech and Signal Processing, ICASSP'11, pp. 5952-5955, Prague, Czech Republic, 22-27 May 2011.

[32] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," IEEE Trans. on Smart Grid, vol. 2, no. 2, pp. 382- 390, Jun. 2011.

[33] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," IEEE Trans. on Industrial Informatics, vol. 18, no. 2, pp. 880-890, Feb. 2021.

[34] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in Proc. of the ACM SIGSAC Conf. on Computer & Communications Security, pp. 439-450, Berlin, Germany, 4-8 Nov. 2013.

[35] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: a dynamic Bayesian game-theoretic approach," ISA Trans., vol. 115, pp. 108-123, Sept. 2021.

[36] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," IEEE Trans. on Smart Grid, vol. 4, no. 1, pp. 160-169, Mar. 2013.

[37] C. Jin, Z. Bao, M. Yu, J. Zheng, and C. Sha, "Optimization of joint cyber topology attack and FDIA in electricity market considering uncertainties," in Proc. IEEE Power & Energy Society General Meeting, PESGM'21, 5 pp., Washington, DC, USA, 26-29 Jul. 2021.

[38] D. H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," IEEE Trans. on Smart Grid, vol. 9, no. 2, pp. 512-520, Mar. 2018.

[39] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," IEEE Trans. on Smart Grid, vol. 11, no. 4, pp. 3438-3446, Jul. 2020.

[40] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," Applied Energy, vol. 235, pp. 204-218, Feb. 2019.

[41] P. K. Jena, S. Ghosh, and E. Koley, "A binary-optimization-based coordinated cyber-physical attack for disrupting electricity market operation," IEEE Systems J., vol. 15, no. 2, pp. 2619-2629, Jun. 2020.

[42] P. K. Jena, S. Ghosh, E. Koley, D. K. Mohanta, and I. Kamwa, "Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information," Electric Power Systems Research, vol. 205, Article ID: 107732, Apr. 2022.

[43] M. Esmalifalak, et al., "A stealthy attack against electricity market using independent component analysis," IEEE Systems J., vol. 12, no. 1, pp. 297-307, Mar. 2018.

[44] S. Tan, W. Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," IEEE Trans. on Smart Grid, vol. 9, no. 1, pp. 313-322, Jan. 2018.

[45] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: stochastic robustness," IEEE Trans. on Smart Grid, vol. 10, no. 1, pp. 128-138, Jan. 2019.