Sustainable Cities and Society 77 (2022) 103523

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Accuracy improvement of electrical load forecasting against new cyber-attack architectures

Arshia Aflaki [a], Mohsen Gitizadeh [a,*], Burak Kantarci [b]

[a] Department of Electronics and Electrical Engineering, Shiraz University of Technology, Shiraz, Iran
[b] School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa K1N 6N5, ON, Canada

ARTICLE INFO

Keywords:
Cybersecurity
Data integrity attack
Civil attack
Electrical load forecasting
Gaussian process regression

ABSTRACT

The cyber challenges faced by cybercriminals are growing dramatically as the power system strives to become more intelligent and more stable. Load forecasting is a well-known problem in the energy management field, but the state-of-the-art lacks contributions that consider data integrity aspects. Despite the existing effective methods on load forecasting, power system requires robust schemes that are also successful in performing accurate load forecasting under cyber-attacks. A novel cyber-attack named Civil Attack (CA) is employed and faced by the two non-linear regression methods. In recent years, numerous regression techniques such as methods called Multiple Linear Regression (MLR), Artificial Neural Network (ANN), Support Vector Regressor (SVR) and etc., were employed to perform electricity load forecasting under false data injection (FDI) attacks. While all of the techniques listed are inaccurate in zones with high load covariance, mostly industrial zones, we propose two non-linear methods called Gaussian Process Regression (GPR) with optimized kernel functions and Random Forest Regression (RFR) to address the problem, while the data integrity attack is used for comparing our methods with other proposed methods.

1. Introduction

Load forecasting is crucial in the operation of the power grid. While the modern power system is going toward being smarter, numerous challenges remain, and addressing cyber threats is of the highest priority. Forecasting loads for smart grids is a crucial task that facilitates economic dispatch, and optimal power flow for different grid zones, and inaccuracy in the loads may lead to economic loss or even blackouts. Uncertainty in load patterns is a non-negligible phenomenon in forecasting, which is often experienced with unsupervised learning methods as in Charwand, Gitizadeh, Siano, Chicco and Moshavash (2020). Since the load forecasting problem under different cyber-attacks has not adequately been discussed, we employ a well-known database from Global Energy Forecasting Competition (GEFCom) in 2012 (Hong, Pinson & Fan, 2014) [dataset] which contains both electrical loads and zonal temperatures. Along with different load patterns in years, the "outlier detection" problem is studied not only for the electrical networks (Y. Chen et al., 2018) but also in the gas networks (Akouemo & Povinelli, 2016) and communication networks (Branch, Giannella, Szymanski, Wolff & Kargupta, 2013). Cyber-attack defense frameworks are implemented even more in the transmission or distribution network by using the components of the power system which may significantly impact load forecasting (Cui & Wang, 2021). This paper presents a stochastic Gaussian solution to the issue of cyber-attacks in the power industry, which was first proposed by Andrew in Andrew (2004), and a random forest approach (Ho, 1998).

Time series and supervised learning regression methods are two well-known algorithms that are commonly used for forecasting. Machine learning and deep learning methods are widely implemented in the power industry, with numerous applications ranging from detecting illegal consumers (Ghasemi & Gitizadeh, 2018) and energy management programs (Bahrami, Chen & Wong, 2020) to eliminating cyber-sabotages in the transient mode of the power system (Aflaki, Gitizadeh, Razavi-Far, Palade & Ghasemi, 2021). As mentioned, Deep learning techniques are also applicable for detecting the cyber-sabotages, such as False Data Injection (FDI), Denial of Service (DoS) attacks, and Load Altering Attack (LAA) (Al-Abassi, Karimipour, Dehghantanha & Parizi, 2020; C. Chen, Cui, Fang, Ren & Chen, 2020; Fang, Xu, Xu & Zhao, 2019). Regression methods, all of which are subcategories of the machine and deep learning, both linear and non-linear, are also used as approaches to the cyber-attack issue (Y. H. Chen & Chen, 2019), along with forecasting the electricity consumption

* Corresponding author at: Department of Electrical and Electronic Engineering, Shiraz University of Technology, Modares Blvd., Shiraz, Iran.
E-mail addresses: gitizadeh@sutech.ac.ir (M. Gitizadeh), burak.kantarci@uottawa.ca (B. Kantarci).

https://doi.org/10.1016/j.scs.2021.103523
Received 10 June 2021; Received in revised form 25 September 2021; Accepted 27 October 2021
Available online 6 November 2021

of households (Kim, 2020). In the renewable energy portion of the power industry, numerous cases are studied such as energy policies for electric vehicles (Lei & Mohammadi, 2021) and renewable energy forecasting (Nam, Hwangbo & Yoo, 2020). The Civil Attack (CA) is rather a novel topic in the power industry, but in computer science, some cases of cyber-attacks on GPS, which is the fundamental feature of CA, are studied (Zheng & Sun, 2020) and as a real-time situation (BBC News, 2017) investigates an attack on GPS in England. Additionally, a blockchain framework is employed in Ghiasi et al. (2021) as the technology is able to facilitate data security in different sectors of power system and Internet of Things (IOT). In specific, blockchain innovation offers numerous alluring highlights for IoT frameworks, such as decentralization, reliability, trackability, and permanence.

In the case of cyber-attacks on forecasting, Zhang proposes a question in Zhang, Chu, Sankar and Kosut (2018) that investigates the probability of FDI attack on load history used for forecasting algorithms. The basis of data integrity in forecasting is that some of the load history data is going to increase or decrease using malware implemented on the Supervisory Control and Data Acquisition (SCADA) system, which potentially results in economic losses and protracted blackouts. Malwares, such as "Trojans", are able to penetrate to the SCADA servers and access the historical data, in our case, training data, and the hackers are able to perform data integrity attacks on the data by using these malwares. Using linear regression shows great quality and accuracy in eliminating the data integrity attacks. Another option for adversaries attacking Phasor measurement units (PMUs) to inject false data into the database leads to inaccurate power system state estimation (Liu, Ning & Reiter, 2011). Therefore, a robust and accurate load forecasting method being able to predict huge electrical loads under malicious cyber-attacks is required to decrease the cost. In recent years, some linear regression methods were implemented to face the cyber-sabotages in forecasting electricity consumption, such as Multiple Linear Regression (MLR), Artificial Neural Network (ANN), Support Vector Regression (SVR), and fuzzy interaction regression (FIR). Being the first article to discuss the data integrity problem in load predicting (Luo, Hong & Fang, 2018a), writers tried to benchmark the robustness of the mentioned methods. The first related article, however, was that of (Xie & Hong, 2016) in which a probabilistic load forecasting method was first discussed. These methods, however, failed to stay accurate in case of data integrity attacks on historical forecasting data. In Luo, Hong and Fang (2018b), the authors propose three robust regression models for load forecasting, iteratively re-weighted least squares with 'bisquare' weight function (IRLS-bis) and the other one with 'logistic' function (IRLS-log) while the last one is based on $l1$ norm called ($l1$) which shows great accuracy in forecasting while historical loads are under cyber-attacks. All of the seven mentioned methods failed to forecast loads with high covariance in industrial zones leading us to a question: *Is it possible to forecast industrial zones more accurately both in standard operation and under novel cyber-attacks?*

To answer this question, we should keep in mind that industrial loads data mostly have more noisy patterns than household loads data. Therefore, a probabilistic model with the capability of detecting noises is more suitable for the proposed issue, and a non-linear regression model based on boosted tree regressor is able to diagnose the fluctuation of the electricity load. As proposed in Richardson, Osborne and Howey (2017), Lithium-ion batteries' state of charge is an uncertain issue that depends on many features and even previous data similar to load forecasting, which depends on load history, temperature, etc. and it is tackled by the Gaussian Process Regression (GPR) method. We tried to use GPR in the load forecasting model to decrease the relative errors in special zones, and for data integrity attacks. As it is studied in Khammas (2020), we employed the Random Forest Regression (RFR) to tackle the cyber-attack issue. In addition to (Luo et al., 2018a, 2018b), the novel civil attack is proposed in this article and tackled by two regression models GPR and RFR. It is worth noting that kernel functions are vitally important parts of the GPR, and in this article, we optimized them with aggregated 24hour data from GEFCom 2012. Table 1 presents a comparison of related articles and highlights the contribution of this article.

Table 1
Comparison between different studies.

	Data integrity attack	Civil attack	Machine and Deep learning-based approach
This article	✓	✓	✓
(Luo et al., 2018a)	✓	×	✓
(Luo et al., 2018b)	✓	×	✓

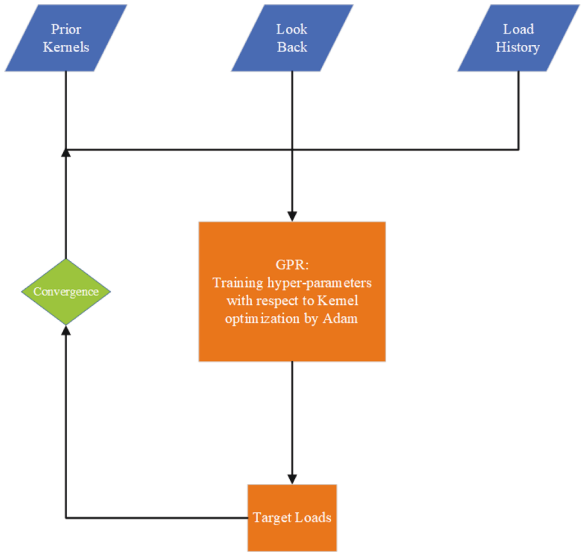

Fig. 1. How GPR works for load forecasting.

The contribution of this article is three-fold: 1) it introduces the forecasting field to an innovative development challenge: forecasting under cyber-attacks. 2) it introduces a novel cyber-attack named Civil Attack, 3) it compares and contrasts the robustness of eight different models under data integrity attack at different levels along with the novel CA in the industrial zones.

The rest of the paper is arranged as follows. In Section 2, we propose a new GPR method for regression with optimized kernels and RFR method, along with a brief explanation of the proposed civil attack. Section 3 will discuss the database and benchmarking of GEFCom 2012 with temperature settings and zonal loads with cyber-attacks settings. The numeric results are presented in Section 4 and discussion, and this paper is concluded in Section 5.

2. Regression and cyber-attack models

This section investigates how the GPR method works and introduces the novel cyber-attack model called civil attack. It is worth noting that we are using temperature as a feature that facilitates GPR to predict the electricity consumption of different zones and make this study more practical. No data preprocessing methods are employed in this article.

2.1. Gaussian process regressor

Gaussian Processes (GP) are supervised learning methods that can be used to solve problems like regression and probabilistic classification (1.7. Gaussian Processes — Scikit-Learn 0.24.1 Documentation, n.d.). While the GPR method employs GP for regression purposes, the mean value can be set whether zero or the mean of a given dataset. As for covariance of the method, numerous kernel functions are available,

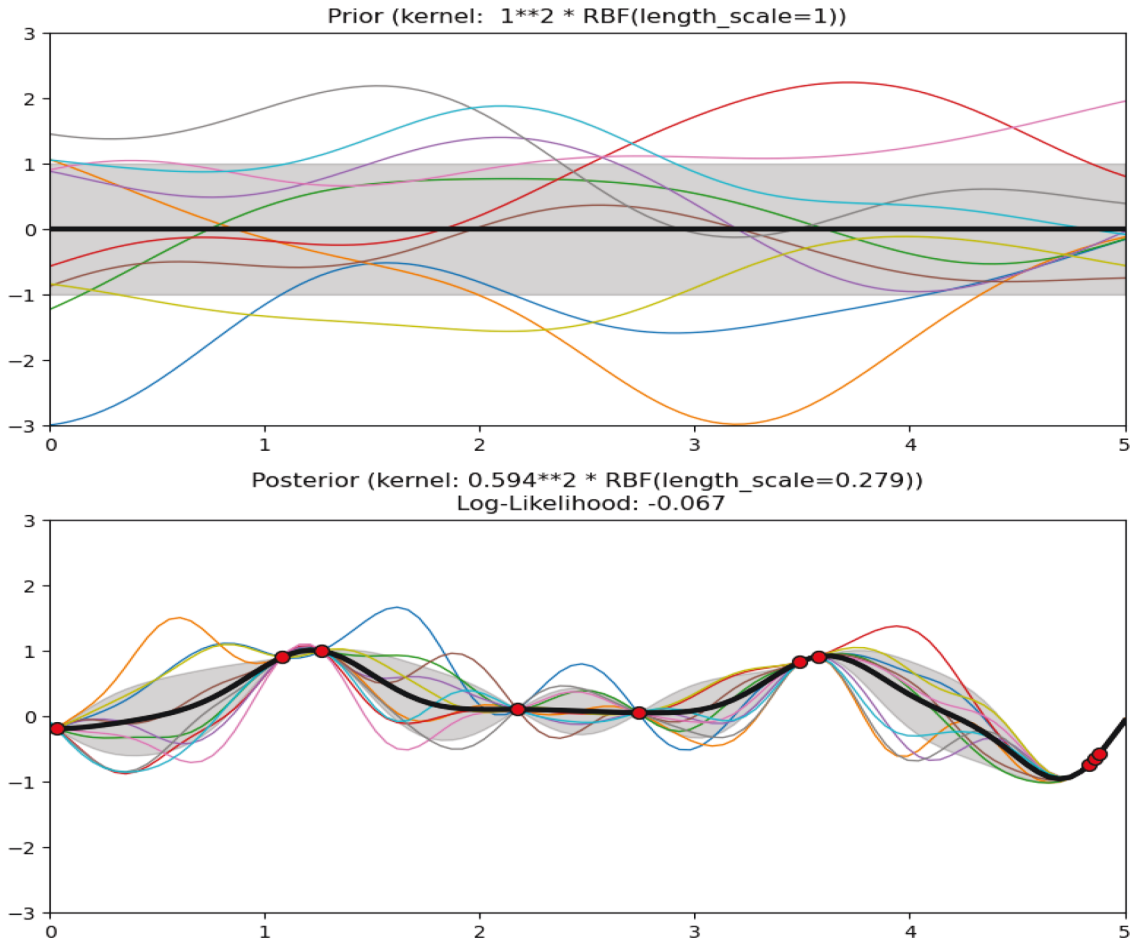

Fig. 2. Prior and posterior resulting of GP with RBF as kernel function, Mean, standard deviation, and 10 samples are shown for both prior and posterior. (1.7. Gaussian Processes — Scikit-Learn 0.24.1 Documentation, n.d.).

ranging from white kernel to a constant. Like other regression methods, GPR accepts an input vector called x and passes a continuous output such as $y = f(x)$. If we assume that samples in our input vector are part of a stochastic process, then $f(x)$ function is able to calculate the output if and only if the x contains some finite numbers.

Let assume that we possess a training data set called D of n observations $D = \{(x_i, y_i) \mid i = 1, 2, \ldots, n\}$, for further explanation see (Seeger, 2004), while in this article, the input vector is the hourly load of GEFCom 2012 with an eleven days lookback and keep it in mind that another feature which can be used is the zonal temperature. Fig. 1 illustrates a typical GPR algorithm used for load forecasting. GPR is a supervised learning method that requires optimizing two hyper-parameters: the variance (σ) and the step length (l). In each iteration, this task will be carried out by prioritizing, choosing optimal kernels, and refining hyper-parameters based on the training set (Seeger, 2004). As mentioned, optimized kernel functions are vital for minimizing the prediction error. In this article, optimizing the kernel functions is conducted by Tensorflow Adam kernel optimizer (Tf.Keras. Optimizers.Optimizer | TensorFlow Core v2.4.1, n.d.), which is able to adjust kernels in such a way that the method can use multiple starting points in kernel functions which will affect the hyper-parameters (Z. Chen & Wang, 2018).

It is worth noting that three well-known kernel functions are implemented as the initial kernels in our models, 'Dot-product'; 'Radial-basis function' and 'Matern', all of which are formulated as below (1.7. Gaussian Processes — Scikit-Learn 0.24.1 Documentation, n.d.).

- Dot-product: a non-stationary function with prior of $N(0, \sigma^2)$.

$$k(x_i, x_j) = \sigma_0^2 + x_i . x_j \tag{1}$$

As electricity load models fluctuate highly over time, the Dot-product function can easily fit the predicted data with peaks.

- Radial-basis function (RBF): a stationary function parameterized by a length-scaled parameter called l.

$$k(x_i, x_j) = \exp\left(\frac{-d(x_i, x_j)^2}{2l^2}\right) \tag{2}$$

Where d is the Euclidian distance. The prior and posterior of a GPR with different kernels are shown in Fig. 2. For both the prior and posterior, mean, standard deviation, and ten samples are illustrated, explaining why this function is selected as the initial kernel function.

- Matern: stationary function

$$k(x_i, x_j) = \frac{1}{\Gamma(v)2^{v-1}}\left(\frac{\sqrt{2v}}{l} d(x_i, x_j)\right)^v K_v\left(\frac{\sqrt{2v}}{l} d(x_i, x_j)\right) \tag{3}$$

Selected as one of the optimized kernel functions, Matern is a generalized form of RBF in which K_v is a modified Bessel function, Γ is the gamma function, and v is the parameter that controls the smoothness.

From Fig. 2, it is clear that the RBF kernel was not properly fitted to the actual data, black line, before optimization, but after optimization, the length and Log-Likelihood were set in such a way that the RBF would

fit with noisier data plotted in the mentioned figure. Hence, RBF is employed as one of the initial kernels to improve the GPR prediction accuracy for our electricity load data. It is worth noting that the hyperparameters optimization is conducted by the Tensorflow optimization tool (Tf.Keras.Optimizers.Optimizer | TensorFlow Core v2.4.1, n. d.).

2.2. Random forest regressor

In this section, we present a well-known non-linear regression technique called random forest. The random forest and random tree regressor's fundamental random subspace method were first proposed in Ho, (1998). Also called feature bagging, the assembly learning method tries to reduce the difference between the estimated values in an ensemble by choosing random features for training instead of all of them. The random forest method was first analyzed by Breiman (Breiman, 2001). Assume a training data set $X = x_1, x_2, \ldots, x_n$ with the responses $Y = y_1, y_2, \ldots, y_n$ in which n is the number of samples, bagging will create a random sample with replacement to boost the accuracy in B repeat. Therefore, a sample of training data X_b, Y_b, $b = 1, 2, \ldots, B$, is created, and the RFR can be fitted by using them, and after that, other non-tested samples x' will be fitted. A massive advantage of RFR is that in the scale of the whole forest, the variance will be decreased without increasing the bias, meaning that the model is not sensitive to noise. The training process of non-tested data is as follows by assuming f as forest regressor.

$$f = \frac{1}{B}\sum_{b=1}^{B} f_b(x') \tag{4}$$

And the standard deviation can be formulated as below:

$$\sigma = \sqrt{\frac{\sum_{b=1}^{B}(f_b(x') - f)^2}{B-1}} \tag{5}$$

2.3. Civil-Attack model on load forecasting

In 2017, hackers penetrated the GPSs of electric vehicles in London and changed the receiver IP of several cars so that the navigation signals led different cars in the direction asked by another car. In the power system, it is also possible to change the IP address of measurement units, zone stations, PV solar farms, and the list can be continued. Assume that adversaries are able to penetrate the database of load forecasting and we are forecasting hourly loads concerning the last 24-hours, so we have input data such as $X_i = \{x_i^1, x_i^2, \ldots, x_i^{24}\}$ and i is the number of the respective zones while x_i^{new} is the output of our forecasting program. What Civil-Attack does is that it changes the past 24 h values of two or several different zones as it is formulated below:

$$X_{i,attacked} = \left\{x_j^1, x_j^2, \ldots, x_j^{24}\right\} = X_j \; while \; i \neq j \tag{6}$$

The load forecasting program misuses the inputs of zone j instead of i for forecasting the next hour total electricity consumption of zone i. by using (6) it is clear that

$$f_i\left(X_{i,\ attacked}\right) = x_{i,attacked}^{new} = f_i\left(X_j\right) \tag{7}$$

In which f_i is linear or non-linear (depends on load forecasting program) equations that use past 24 h to predict the next hour load. Since the forecasted load is clearly based on inaccurate historical data, our prediction is incorrect.

2.4. Data integrity attack model on load forecasting

As one of the most common cyber-attacks, data integrity attacks are able to inject false data to a dataset. In the power system, data banks are not immune from hackers who are able to access the servers making them able to change the historical data used for load forecasting. Similar to the previous subsection, assume that we have input data such as $X_i = \{x_i^1, x_i^2, \ldots, x_i^{24}\}$, while i is the number of the respective zones in our dataset, and x_i^{new} is the forecasted value. Data integrity attack changes the values of X_i. Assume the attack vector of data integrity attack as $A = \{a^1, a^2, a^3, \ldots, a^k\}$, in which k is the probability of attack which is between 1 and 24 meaning that the attack vector can influence the input data ranging from only one of them to all of the inputs as formulated below.

$$X_{i,\ attacked} = X_i + A = \begin{cases} \{x_i^j + a^m\} \; for \; j = m \\ \{x_i^j\} \; for \; j \neq m \end{cases} \tag{8}$$

in which j ranges from 1 to 24, and m ranges from 1 to k. The difference between civil-attack and data integrity attack is as follows: in a civil-attack, attackers are able to simply use the existing data in the servers and just swap them with each other. On the other hand, in a data integrity attack, attackers inject false data to the datasets which requires more time and effort.

3. Benchmarking and cyber-attacks settings

This section introduces the benchmarking framework and cyber-attack settings.

3.1. Benchmarking framework

The GEFCom 2012 dataset has 21 zones. The first 20 zones are all from USA stations, and the last zone is the sum of the other twenty zones. For temperature, we used the method proposed by Hong, Wang and White, (2015). The database contains electricity load and small-scaled data for 4.5 years in the USA from 2004 to 2008. Along with electricity consumption, temperature for each zone are used as features for the proposed load forecasting algorithms to draw a fair comparison between our methods and those of (Luo et al., 2018a, 2018b). We used the first three years as training data while 2007 marked as test data. In most load forecasting programs, Mean Absolute Percentage Error (MAPE) and Root Mean Squared Error (RMSE) are the evaluation metrics for forecasting accuracy.

$$MAPE\% = \frac{100}{n}\sum_{t=1}^{n}\left|\frac{y_{test,t} - y_{predict,t}}{y_{test,t}}\right| \tag{9}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{t=1}^{n}\left|y_{test,t} - y_{predict,t}\right|^2} \tag{10}$$

In which n is the number of predicted samples, y_{test} is the actual load, and $y_{predict}$ is the predicted load forecasted by the given method. It is worth noting that smaller MAPE and RMSE means more accuracy of the forecasting method. In comparing tables, the lowest MAPE in each scenario or zone is bolded, and those MAPEs that are more than 10, which means not too accurate in case of predicting, are shaded in gray. The GPR and RFR methods are simulated using Python 3.8 and scikit-learn library (Pedregosa et al., 2011). The other six methods data are derived from Luo et al., (2018a), 2018b. Here, the NN method setting is illustrated as follows. It is worth mentioning that the Sklearn preprocessing method called StandardScaler (Pedregosa et al., 2011) is used to scale the load and temperature data before entering the proposed models.

The ANN model consists of a three-layer feedforward back-propagation neural network with 45 input neurons (Hour, Month, Weekday, Temperature, and Trend) and one output neuron (namely Load). The number of neurons in the hidden layer is set to 22 in the numerical experiments in the mentioned paper, and the transfer functions for the hidden and output layers are set to 'logsig' and 'purelin,'

Table 2
Modules used in the implementation.

Model	Module
IRLS_bis	robustfit with defaulted "wfun" input (MATLAB)
IRLS_log	robustfit with "wfun" input "logistic" (MATLAB)
l_1	linprog (MATLAB)
MLR	robustfit with "wfun" input "ols" (MATLAB)
ANN	Neural Network Toolbox (MATLAB)
SVR	quadprog (MATLAB)
RFR	SKlearn random forest with "n_estimators = 200″ and "min_samples_split = 2″ (PYTHON)
GPR	SKlearn Gaussian Process with mentioned initial kernel functions and "alpha = 0.1″ (PYTHON)

respectively. The ANN model's training and learning functions (for measuring weights) are set to 'trainlm' and 'learngdm,' respectively. The ANN model's stopping criterion is either 1000 maximum epochs or the MATLAB module 'newff's default stopping criterion. Table 2 shows the modules that were used to implement the models.

Table 3 compares different methods used in the two mentioned articles with our proposed methods. From Table 3, it is clear that in GPR is the most accurate method in the aggregate zone. What is unique about the mentioned method is that in special zones, which are zones with high electricity load covariance, GPR managed to lower the MAPE% significantly due to the non-linear and noise-fitting behavior. In the case of RFR, most predictions are accurate, and MAPE is within an acceptable range and, similar to GPR, it performs greatly in special zones, in which all of the other methods from the other articles failed to forecast accurately.v It is worth noting that zones 4 and 9 are industrial zones and load data in these zones have higher covariance than residential zones. l_1, MLR, and GPR were the leading methods in case of accuracy, and the proposed method ranked first in the accuracy of most zones. As it is observable, non-special zones MAPEs are not far apart in different methods. This low difference is mainly due to the small-scaled data and loads covariance, which set a limit for prediction accuracy. However, in the industrial zines, the proposed methods boosted the accuracy of load forecasting significantly fulfilling the main goal of the article. Fig. 3 shows the daily predicted load and expected load in 2007.

3.2. Data integrity attack and civil attack settings

For data integrity attacks, we propose two types of attacks, one of which is targeting system blackouts, while the other is targeting economic loss. It is worth noting that both of the cyber-attacks target historical (training) data; hence test data are not attacked / compromised.

By randomly selecting some historical data and decreasing them, the load forecasting program miss predicts the, as an example, 24 h load lower than the actual one, and by allocating the wrong amount of production to different power utilities, there will be a significant chance of blackout. Let assume that the hacker is able to randomly attack k% of data ranging from 10 to 40 and decreasing them by p% varying from 10 to 90, we have 36 scenarios for the first type of data integrity attacks. It is worth noting that k is the scattering index and p is the severity of attack and scatter attacks with high severity increase the MAPE and RMSE significantly.

It is worth noting that as the speed of MATLAB modules are different from Python ones, we only calculated the speed of our proposed methods. While some random data increase, the predicted load is going to be more than expected, so more production will be planned, which will lead the system to economic loss. Another different scenario can be described for this type of data integrity attack, and while k is set to be 30%, p% is going to increase from 1/32 to 8 percent by doubling it. It is worth noting that the aggregate zone of the year 2007 is employed as test data set, and all seven methods are examined under various scenarios.

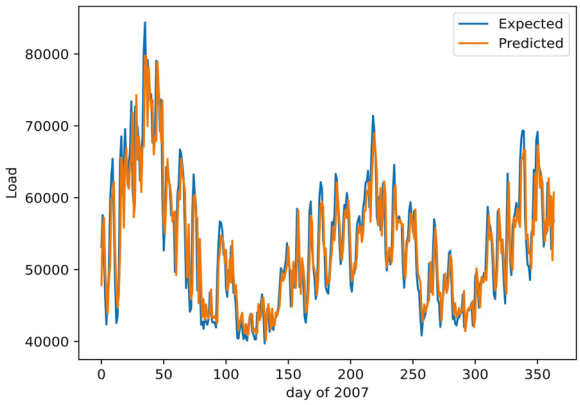

Fig. 3. Daily load curve of 2007 using GPR method with 5.21 percent of MAPE.

Table 3
Hourly load benchmarking of GEFCom 2012, MAPE% in the year 2007.

	Zone	IRLS_bis	IRLS_log	l_1	MLR	ANN	SVR	GPR	RFR
Aggregated zone	21	5.30	5.27	5.33	5.22	5.69	5.23	**5.21**	5.70
Regular zone	1	7.08	7.03	7.08	**7.01**	8.88	7.02	7.55	8.38
	2	5.56	5.56	**5.52**	5.62	5.99	5.61	6.02	6.54
	3	5.56	5.56	**5.52**	5.62	6.19	5.61	6.02	6.57
	5	9.69	9.67	9.64	9.88	10.80	9.93	**8.45**	9.04
	6	5.56	5.54	**5.53**	5.55	6.34	5.55	6.05	6.58
	7	5.56	5.56	**5.52**	5.62	6.15	5.61	6.02	6.57
	8	7.59	7.56	7.59	7.50	8.57	7.47	**6.28**	7.01
	10	**6.70**	6.73	6.79	**6.70**	7.39	6.75	8.28	8.31
	11	7.97	7.94	8.20	**7.70**	9.46	7.75	**7.70**	8.46
	12	6.95	6.91	6.99	**6.78**	8.45	6.88	8.32	8.46
	13	7.48	7.46	7.44	7.39	9.46	7.40	**5.94**	6.38
	14	9.41	9.39	9.40	9.38	11.08	9.48	**9.33**	10.94
	15	7.38	7.39	7.40	7.44	9.36	7.47	**6.87**	7.53
	16	8.13	**8.11**	**8.11**	8.12	9.74	8.24	9.75	10.27
	17	5.31	5.29	5.30	**5.26**	6.41	5.27	7.18	7.65
	18	6.77	6.74	6.73	**6.72**	7.79	6.77	7.97	8.62
	19	7.88	7.88	**7.87**	7.90	10.28	7.96	8.12	9.00
	20	5.73	5.71	5.68	5.74	6.67	5.75	**5.38**	5.88
	Avg	7.017	7.002	7.017	6.996	8.278	7.029	7.290	7.944
Special Zone	4	15.83	15.90	15.89	16.08	17.72	16.06	**5.26**	5.56
	9	164.05	152.10	153.48	139.16	128.2	140.04	27.97	**26.18**
Speed (*sec*)	×	×	×	×	×	×	×	0.725	**0.041**

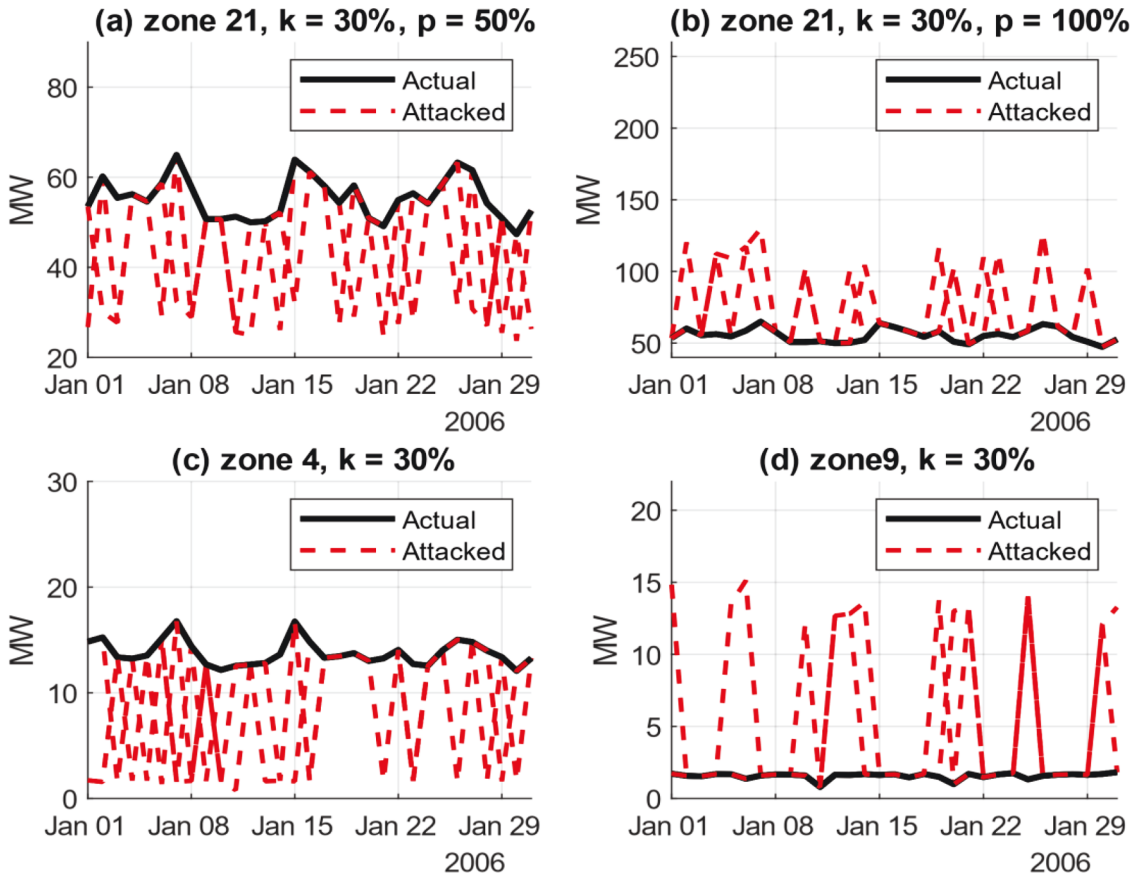

Fig. 4. The daily load pattern of zones 4, 9, and 21 under different cyber-attacks.

Table 4
MAPE (%) / RMSE (10^5) of load forecasting under data integrity attack targeting blackouts with $k = 10\%$.

	pk	10	20	30	40	50	60	70	80	90
IRLS_bis		5.50/1.26	**5.39/1.23**	**5.30/1.21**	**5.29/1.21**	**5.29/1.21**	**5.29/1.21**	**5.29/1.21**	**5.29/1.21**	**5.29/1.21**
IRLS_log		5.48/1.26	5.54/1.27	5.55/1.27	5.55/1.27	5.55/1.27	5.55/1.27	5.55/1.27	5.55/1.27	5.55/1.27
l_1		5.46/1.26	5.47/1.26	5.47/1.26	5.47/1.26	5.47/1.26	5.48/1.26	5.48/1.26	5.48/1.26	5.48/1.26
MLR	10	5.50/1.26	5.90/1.35	6.42/1.46	7.05/1.59	7.74/1.72	8.51/1.87	9.32/2.02	10.16/2.17	11.03/2.33
ANN		5.88/1.34	6.34/1.44	6.89/1.56	7.63/1.71	8.52/1.90	9.25/2.06	10.14/2.25	11.04/2.44	12.24/2.70
SVR		5.51/1.26	5.92/1.36	6.42/1.46	7.04/1.59	7.73/1.72	8.49/1.86	9.29/2.00	10.12/2.16	10.99/2.31
RFR		5.98/1.38	5.99/1.38	5.76/1.34	5.82/1.33	5.83/1.33	5.87/1.34	5.67/1.31	5.87/1.44	5.84/1.43
GPR		**5.43/1.26**	5.95/1.37	6.59/1.51	7.28/1.68	8.25/1.80	8.69/1.88	9.37/2.00	9.67/2.04	9.91/2.10

In the case of Civil Attack, we chose two special zones, 4 and 9, as the test zones with daily load forecasting and lookback of 11 days. The historical data that are the inputs of the load forecasting program is from the year 2004 are switched for the two mentioned years with respect to k, which is the percentage of data that will be switched. The *k* ranges from 10 to 40 percent, and the year 2007 is our test data, and both GPR and RFR methods are examined in these scenarios.

Fig. 4 illustrates data of the first month of 2006 under data integrity attacks targeting blackouts and economic loss and mentioned data under civil attack for both mentioned zones.

Fig. 4(a) plots the daily load pattern of the first month of 2006 training data under data integrity attack targeting blackouts, while Fig. 4(b) shows the mentioned data under data integrity attack targeting economic loss. The other two subplots illustrate the two industrial zones

Table 5
MAPE (%) and RMSE (10^5) of load forecasting under data integrity attack targeting blackouts with $k = 20\%$.

	pk	10	20	30	40	50	60	70	80	90
IRLS_bis		5.84/1.34	6.03/1.35	**5.42/1.23**	**5.28/1.21**	**5.27/1.21**	**5.27/1.21**	**5.27/1.21**	**5.27/1.21**	**5.27/1.21**
IRLS_log		5.81/1.33	6.22/1.41	6.32/1.43	6.35/1.44	6.35/1.44	6.35/1.44	6.35/1.44	6.35/1.44	6.35/1.44
l_1		**5.66/1.31**	**5.71/1.33**	5.71/1.33	5.72/1.33	5.72/1.33	5.72/1.33	5.72/1.33	5.72/1.33	5.72/1.33
MLR	20	5.88/1.35	6.96/1.58	8.38/1.83	10.05/2.13	11.80/2.44	13.63/2.75	15.39/3.06	17.27/3.39	19.17/3.72
ANN		6.17/1.41	7.34/1.65	8.83/1.95	10.37/2.24	12.28/2.64	14.10/2.99	15.99/3.34	18.01/3.78	19.73/4.10
SVR		5.89/1.35	7.01/1.58	8.38/1.83	10.00/2.12	11.73/2.42	13.52/2.73	15.38/3.05	17.26/3.37	19.16/3.70
RFR		6.21/1.42	6.35/1.44	5.84/1.35	5.63/1.29	5.71/1.30	5.73/1.30	5.78/1.31	5.81/1.33	5.89/1.35
GPR		**5.66/1.31**	6.53/1.50	7.59/1.71	8.48/1.85	9.28/2.00	9.82/2.06	10.20/2.16	10.57/2.19	10.84/2.26

Table 6
MAPE (%) and RMSE (10^5) of load forecasting under data integrity attack targeting blackouts with $k = 30\%$.

	pk	10	20	30	40	50	60	70	80	90
IRLS_bis		6.32/1.45	7.91/1.74	9.84/2.07	11.81/2.39	13.79/2.71	15.67/3.02	17.15/3.25	18.20/3.39	18.68/2.10
IRLS_log		6.28/1.44	7.67/1.69	9.21/1.96	10.69/2.20	12.16/2.44	13.55/2.67	14.67/2.86	15.87/3.05	17.03/3.25
l_1		5.98/1.38	**6.14/1.43**	6.14/1.43	6.15/1.43	6.16/1.43	6.16/1.43	6.16/1.43	6.16/1.43	6.16/1.43
MLR	30	6.35/1.45	8.35/1.83	10.71/2.24	13.35/2.70	16.08/3.18	19.04/3.68	21.70/4.14	24.53/4.63	27.37/5.13
ANN		6.60/1.51	8.69/1.91	11.30/2.54	13.69/2.87	16.36/3.36	19.34/3.93	22.11/4.43	24.85/5.02	28.38/5.67
SVR		6.43/1.36	8.29/1.82	10.70/2.24	13.33/2.70	16.08/3.16	19.04/3.67	21.70/4.14	24.54/4.62	27.38/5.12
RFR		6.36/1.45	6.97/1.57	**5.96/1.37**	**5.75/1.32**	**5.80/1.33**	**5.69/1.31**	**5.79/1.33**	**5.93/1.36**	**5.68/1.31**
GPR		**5.87/1.35**	7.11/1.60	8.22/1.79	9.14/1.98	9.85/2.07	10.05/2.16	10.75/2.24	10.80/2.36	11.06/2.45

Table 7
MAPE (%) and RMSE (10^5) of load forecasting under data integrity attack targeting blackouts with $k = 40\%$.

	pk	10	20	30	40	50	60	70	80	90
IRLS_bis		6.97/1.57	9.77/2.07	13.08/2.64	16.62/3.24	20.37/3.87	23.88/4.48	27.53/5.11	31.18/5.75	34.83/6.38
IRLS_log		6.94/1.57	9.63/2.05	12.77/2.58	16.13/3.15	19.71/3.76	23.02/4.33	26.49/4.93	29.97/5.53	33.44/6.14
l_1		6.64/1.52	7.40/1.69	7.63/1.76	7.82/1.83	8.05/1.94	8.152/0.01	8.30/2.11	8.45/2.28	8.59/2.36
MLR	40	6.97/1.57	9.90/2.10	13.36/2.69	17.04/3.32	20.93/3.98	24.59/4.61	28.38/5.27	32.17/5.93	35.97/6.59
ANN		7.17/1.62	10.07/2.17	13.55/2.81	17.07/3.47	20.87/4.18	24.78/4.91	28.31/5.65	32.47/6.38	36.77/7.12
SVR		6.95/1.57	9.89/2.10	13.35/2.69	17.03/3.31	20.92/3.97	24.59/4.61	28.39/5.26	31.60/5.81	34.54/6.33
RFR		6.59/1.51	**7.15/1.62**	**6.07/1.40**	**5.82/1.33**	**5.69/1.31**	**5.76/1.32**	**5.89/1.34**	**5.58/1.27**	**5.70/1.32**
GPR		**6.25/1.43**	7.47/1.71	8.61/1.88	9.43/2.10	10.10/2.12	10.58/2.18	10.83/2.25	11.10/2.45	10.99/2.43

Table 8
MAPE% of forecasting under data integrity attack targeting economic loss.

P%	IRLS_bis	IRLS_log	l_1	MLR	ANN	SVR	RFR	GPR
1/32	5.13	5.11	5.14	**5.08**	5.57	5.09	5.73	5.28
1/16	5.07	5.05	5.09	**5.04**	5.62	**5.04**	6.00	5.46
1/8	5.22	5.20	**5.12**	5.28	5.88	5.29	6.34	6.04
1/4	6.36	6.15	**5.17**	6.90	7.82	6.91	7.21	7.70
1/2	10.24	9.17	**5.17**	12.72	13.56	12.86	7.57	9.89
1	5.25	14.71	**5.17**	26.63	27.00	26.71	6.21	11.24
2	5.25	23.34	**5.17**	55.46	56.15	55.58	5.87	12.14
4	5.26	31.41	**5.18**	112.50	111.61	112.76	6.02	12.58
8	5.26	34.61	**5.18**	226.33	229.39	226.44	5.99	12.83

under the introduced CA.

4. Numerical results and discussion

This section contains the simulation results under mentioned cyber-attacks, which will be discussed comprehensively. All of the simulations are carried out using MATLAB 2020a and Python 3.8 with the processor Intel(R) Core(TM) i7–10750H CPU @ 2.60 GHz 2.59 GHz and 16GB of RAM.

Tables 4, 5, 6 and 7 show the simulation results of GEFCom 2012 dataset under data integrity attack targeting blackouts with eight different methods, six of which are derived from Luo et al., (2018a), 2018b. It is worth noting that for MAPE% in forecasting, the rule of thumb that is lower than 10 means the method is appropriate for electrical load forecasting. If not, the model is not accurate enough. The aggregate zone of 2007s data is chosen as test data, and data from 2004 to 2006 are selected as training data.

Table 9
MAPE% of forecasting under civil attack.

k%		RFR	GPR	MLR	SVR	l_1
10	Zone 4	**5.51**	11.88	18.29	24.15	16.02
	Zone 9	**25.88**	32.20	205.69	145.08	155.05
20	Zone 4	**5.55**	12.99	20.07	24.33	16.05
	Zone 9	**26.44**	32.81	296.85	146.51	155.20
30	Zone 4	**5.61**	13.67	25.68	25.16	16.05
	Zone 9	**25.12**	32.74	339.81	147.87	157.33
40	Zone 4	**5.74**	13.86	33.29	26.38	16.06
	Zone 9	**28.84**	32.85	390.19	149.02	157.33

From Tables 4 to 7, it is clear that although GPR method simply outperformed MLR, SVR, and ANN, in cases that lesser historical data are under attack, IRLS_bis, IRLS_log, and l_1 are more accurate methods. Similar to GPR, RFR is not as accurate as of the three mentioned methods in lower *k*%, even though RFRs MAPE% never reached 10 in this simulation, and its numbers were near the accurate methods.

In *k*% more than 20, RFR was predominantly the best method. Some exceptions in $p\% = 10$ and 20 occurred in which GPR and l_1 were leading, mostly due to the overfitting prevention methods used in RFR and the non-linear procedure of this method. GPR, on the other hand, was not the leading method, although GPR outperformed IRLS methods. In colossal data integrity attacks targeting blackouts, RFR leads by a significant difference, making it the most suitable method, while in more humble attacks, it's MAPE% never reached 7 percent, which means that the method is accurate enough. Some fluctuation in errors of different *p* % in RFR is observable, which is basically because of random training data selection of this method that tries to choose the best training dataset.

Table 8 illustrates MAPE% of mentioned methods in load forecasting under data integrity attack targeting economic loss.

It is observable that l_1 is the leading method in most scenarios while GPR, compared to MLR, SVR, ANN, and IRLS_log, managed to limit its error between an acceptable range. In the case of RFR, its error never reached 8 percent, which shows an incredible accuracy of this model under economic loss attack, while l_1 is still the best method in these types of cyber-attacks. IRLS_bis is one of the leading methods, except $p = 0.5$ when the MAPE error passes 10.

RFR is still a reliable method in case of data integrity attack as the MAPE% never reached 8 in all the proposed scenarios, and in most scenarios, the RFR was the leading method in case of accuracy. GPR performed inaccurate in some attack cases with high severity. Both of the proposed methods outperformed other methods in case of load forecasting in special zones making RFR the best method in case of forecasting under cyber-attacks and for special zones.

In Table 9, forecasting errors under civil attack are illustrated. It is worth mentioning that the 2007 daily data of two special zones, 4 and 9, are predicted, while some of their historical data are swapped with each other, which is the basis of civil-attack. Both of the proposed methods are employed in 4 scenarios. It is worth noting that the best forecasting method under cyber-attacks, l_1, along with MLR and SVR, both of which scored the best MAPE in aggregated zones, are the other methods derived from Luo et al., (2018a), 2018b for comparison in the CA scenarios. The numbers may vary as we simulated the mentioned methods in Python and not in MATLAB.

It is clear that RFR predominantly exceeded GPR, l_1, MLR, and SVR in each scenario and zone. As we mentioned in Table 1, forecasting errors of zones 9 and 4 are significantly high by every mentioned method, while RFR and GPR managed to lower the MAPE% of special zones under CA. The RFR method limited the error of each attacking scenario in zone 4 to under six percent, which is a considerable breakthrough, while numbers in GPR are not promising at all. It is clear that the other three methods are not suitable at all for forecasting the electricity consumption of industrial zones under CA. All of the five mentioned methods failed to predict loads in zone 9 accurately. Both zones 9 and 4 are industrial loads in two different areas, and the electricity consumption of the mentioned zones fluctuated significantly over training years. Hence, the MAPE of forecasted loads in the special zones under civil attack is relatively higher than the other zones. We utilized the special zones for this attack due to their vast load difference, as is illustrated in Fig. 4, in order to change the magnitude of training data remarkably to test the robustness and accuracy of our proposed methods under civil attacks with higher intensity.

5. Conclusion

Load forecasting brings new challenges to cybersecurity. We consider two types of data integrity attack along with a novel cyber-attack named Civil Attack, and two non-linear regression methods are proposed. The data integrity attacks inject inaccurate data to the historical loads used for predicting hourly load, and civil attack swaps historical loads of different zones. Overall, for forecasting under the normal situation, GPR ranked first in accuracy and registered the lowest MAPE% in the aggregated zone with only 5.21 percent error. Two special zones, in which previous methods from other articles failed to predict accurately, forecasted quite accurately by proposed methods. Zone 4 is forecasted by GPR with only 5.26 percent of MAPE, while the RFR model predicted the loads with 5.56 percent error. In zone 9, GPR and RFR managed to forecast the loads with 27.97 and 26.18 percent MAPE error, respectively. RFR method surpassed other methods in vast and complicated cyber-attacks. Our methods, in some scenarios, failed to predict correctly under the novel civil attack, which was mainly due to hard to predict nature of the two mentioned zones. As these two zones are industrial zones, the historical loads in these special zones fluctuated significantly over time, making their loads hard to forecast accurately. Cyber-attacks utilized in this paper target historical loads from databases and change them by increasing, decreasing and swapping them with other zonal loads.

As the first of its kind in the power industry, the civil attack is able to target load history. Using deep learning methods for forecasting, such as Long Short-Term Memory, may facilitate hourly load prediction under different cyber-sabotages CA included. It is worth noting that the electricity market depends heavily on the forecasted loads, so the influence of these cyber-attacks on the electricity market can be named one of the future agendas of this article and its effect on energy management programs. Using blockchain-based methods for data security, along with detecting cyber-attacks in online streaming energy data are the future contributions to this literature.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

1.7. Gaussian Processes — Scikit-learn 0.24.1 documentation. (n.d.). Retrieved April 7, 2021, from https://scikit-learn.org/stable/modules/gaussian_process.html.

Aflaki, A., Gitizadeh, M., Razavi-Far, R., Palade, V., & Ghasemi, A. A. (2021). A Hybrid Framework for Detecting and Eliminating Cyber-Attacks in Power Grids. *Energies, 14* (18), 5823. https://doi.org/10.3390/en14185823

Akouemo, H. N., & Povinelli, R. J. (2016). Probabilistic anomaly detection in natural gas time series data. *International Journal of Forecasting, 32*(3). https://doi.org/10.1016/j.ijforecast.2015.06.001

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). *An ensemble deep learning-based cyber-attack detection in industrial control system* (p. 8). IEEE Access. https://doi.org/10.1109/ACCESS.2020.2992249

Andrew, A. M. (2004). Information Theory, Inference, and Learning Algorithms. *Kybernetes, 33*(7). https://doi.org/10.1108/03684920410534506

Bahrami, S., Chen, Y. C., & Wong, V. W. S. (2020). Deep reinforcement learning for direct load control in distribution networks. *IEEE Power and Energy Society General Meeting*. https://doi.org/10.1109/PESGM41954.2020.9281703, 2020-August.

BBC News. (2017). NHS cyber-attack: GPs and hospitals hit by ransomware. *Bbc*. May 2017.

Branch, J. W., Giannella, C., Szymanski, B., Wolff, R., & Kargupta, H. (2013). In-network outlier detection in wireless sensor networks. *Knowledge and Information Systems, 34* (1). https://doi.org/10.1007/s10115-011-0474-5

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1). https://doi.org/10.1023/A:1010933404324

Charwand, M., Gitizadeh, M., Siano, P., Chicco, G., & Moshavash, Z. (2020). Clustering of electrical load patterns and time periods using uncertainty-based multi-level amplitude thresholding. *International Journal of Electrical Power and Energy Systems, 117*. https://doi.org/10.1016/j.ijepes.2019.105624

Chen, C., Cui, M., Fang, X., Ren, B., & Chen, Y. (2020). Load altering attack-tolerant defense strategy for load frequency control system. *Applied Energy*, 280. https://doi.org/10.1016/j.apenergy.2020.116015

Chen, Y. H., & Chen, J. L. (2019). AI@NTIPHISH — MAcHINE LEARNING MECHANISMS for CYBER-PHISHING ATTACK. *IEICE Transactions on Information and Systems, E102D*(5). https://doi.org/10.1587/transinf.2018NTI0001

Chen, Y., Patel, V. M., Phillips, P. J., Chellappa, R., Poon, T. W. K., Friesen, M. R., et al. (2018). *An optimizing and differentially private clustering algorithm for mixed data in SDN-Based smart grid* (p. 6). IEEE Access.

Chen, Z., & Wang, B. (2018). How priors of initial hyperparameters affect Gaussian process regression models. *Neurocomputing, 275*. https://doi.org/10.1016/j.neucom.2017.10.028

Cui, M., & Wang, J. (2021). Deeply Hidden Moving-Target-Defense for Cybersecure Unbalanced Distribution Systems Considering Voltage Stability. *IEEE Transactions on Power Systems, 36*(3). https://doi.org/10.1109/TPWRS.2020.3031256

Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *Eurasip Journal on Information Security, 2019*(1). https://doi.org/10.1186/s13635-019-0090-6

Ghasemi, A. A., & Gitizadeh, M. (2018). Detection of illegal consumers using pattern classification approach combined with Levenberg-Marquardt method in smart grid. *International Journal of Electrical Power and Energy Systems, 99*. https://doi.org/10.1016/j.ijepes.2018.01.036

Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access: Practical Innovations, Open Solutions, 9*. https://doi.org/10.1109/ACCESS.2021.3059042

Ho, T. K. (1998). The random subspace method for constructing decision forests. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 20*(8). https://doi.org/10.1109/34.709601

Hong, T., Pinson, P., & Fan, S. (2014). Global energy forecasting competition 2012. *International Journal of Forecasting, 30*(2). https://doi.org/10.1016/j.ijforecast.2013.07.001

Hong, T., Wang, P., & White, L. (2015). Weather station selection for electric load forecasting. *International Journal of Forecasting, 31*(2). https://doi.org/10.1016/j.ijforecast.2014.07.001

Khammas, B. M. (2020). Ransomware Detection using Random Forest Technique. *ICT Express, 6*(4). https://doi.org/10.1016/j.icte.2020.11.001

Kim, M. J. (2020). Understanding the determinants on household electricity consumption in Korea: OLS regression and quantile regression. *Electricity Journal, 33*(7). https://doi.org/10.1016/j.tej.2020.106802

Lei, M., & Mohammadi, M. (2021). Hybrid machine learning based energy policy and management in the renewable-based microgrids considering hybrid electric vehicle charging demand. *International Journal of Electrical Power and Energy Systems*, 128. https://doi.org/10.1016/j.ijepes.2020.106702

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security, 14*(1). https://doi.org/10.1145/1952982.1952995

Luo, J., Hong, T., & Fang, S. C. (2018a). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting, 34*(1). https://doi.org/10.1016/j.ijforecast.2017.08.004

Luo, J., Hong, T., & Fang, S. C. (2018b). Robust Regression Models for Load Forecasting. *IEEE Transactions on Smart Grid*. https://doi.org/10.1109/TSG.2018.2881562

Nam, K. J., Hwangbo, S., & Yoo, C. K. (2020). A deep learning-based forecasting model for renewable energy scenarios to guide sustainable energy policy: a case study of Korea. *Renewable and Sustainable Energy Reviews, 122*. https://doi.org/10.1016/j.rser.2020.109725

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., et al. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12.

Richardson, R. R., Osborne, M. A., & Howey, D. A. (2017). Gaussian process regression for forecasting battery state of health. *Journal of Power Sources, 357*. https://doi.org/10.1016/j.jpowsour.2017.05.004

Seeger, M. (2004). Gaussian processes for machine learning. *International journal of neural systems, 14*(2). https://doi.org/10.1142/S0129065704001899

tf.keras.optimizers.Optimizer | TensorFlow Core v2.4.1. (n.d.). Retrieved April 8, 2021, from https://www.tensorflow.org/api_docs/python/tf/keras/optimizers/Optimizer.

Xie, J., & Hong, T. (2016). GEFCom2014 probabilistic electric load forecasting: An integrated solution with forecast combination and residual simulation. *International Journal of Forecasting, 32*(3). https://doi.org/10.1016/j.ijforecast.2015.11.005

Zhang, J., Chu, Z., Sankar, L., & Kosut, O. (2018). Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Transactions on Power Systems, 33*(5). https://doi.org/10.1109/TPWRS.2018.2818746

Zheng, X. C., & Sun, H. M. (2020). Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defined radio. *Sensors and Materials, 32*(8 p2). https://doi.org/10.18494/SAM.2020.2783