A Robust Support Vector Regression Model for Electric Load Forecasting

Jian Luo

School of Management Science and Engineering, Dongbei University of Finance and Economics, Dalian 116025, China.

Tao Hong

Systems Engineering and Engineering Management Department, University of North Carolina at Charlotte, Charlotte, NC 28223, USA.

Zheming Gao

Graduate Program in Operations Research, North Carolina State University, Raleigh, NC 27695, USA.

Shu-Cherng Fang

Edward P. Fitts Department of Industrial and Systems Engineering, North Carolina State University, Raleigh, NC 27695, USA.

Abstract

Electric load forecasting is one of the key operations in the energy industry. Various forecasting methods and techniques have been employed and tested to support this operation. One growing interest is to develop robust load forecasting in consideration of the cybersecurity with malicious data manipulation. In this paper, we propose a robust support vector regression (SVR) model to forecast the electric demand under data integrity attacks. We first introduce a weight function to calculate the relative importance of each observation in the load history, and then construct a weighted quadratic surface SVR model. Some theoretical properties of the proposed model are derived. Extensive computational experiments are based on the data from Global Energy Forecasting Competition 2012 and ISO New England, which are publicly available. To imitate data integrity attacks, we have deliberately increased or decreased the historical load data following different normal or uniform distributions. Finally, the computational results highlight the superior performance of the proposed robust model over other well-known load forecasting models in the literature, in terms of load forecasting accuracy.

Keywords: forecasting; electric load forecasting; support vector regression; data attacks; weight function.

Email addresses: luojian546@hotmail.com (Jian Luo), hongtao01@gmail.com (Tao Hong), zgao5@ncsu.edu (Zheming Gao), fang@ncsu.edu (Shu-Cherng Fang).

Preprint submitted to *International Journal of Forecasting*

1. Introduction

Load forecasts are constantly applied across all segments of the power industry. The under-forecasts of electric loads may lead to "brownouts" or even "blackouts", while the over-forecasts may lead to the economic losses due to the over-capacity and opportunity costs. Accurate load forecasts are crucial to power systems operations and planning. In recent years, the new technologies of internet, communication networks, and computers have made the operations of power grids much more efficient than before. However, new technologies also bring potential cyberattacks to the power systems. Cybersecurity nowadays presents a serious challenge to the resilience of the power grid (Ericsson, 2010). The cyberattack on Ukraine's power grid (Perez, 2016) is a real-life threat. Data integrity attack is one form of cyberattacks. Hackers can access the supposedly-protected datasets and inject misleading information to the grid measurements in a way that may not be easily detected by the existing operational practice. It is imperative to develop a robust load-forecasting model for the accurate forecast of electric demands under data integrity attacks.

The accurate forecasting of electric loads is essential to the efficient operation of unit commitment, energy transfer scheduling, load-frequency control, and maybe others in the power industry (Hahn et al., 2009). Power companies count on accurate load forecasts to operate in a safe manner, to optimize operational costs, and to improve the reliability of distributional networks (Arora & Taylor, 2018). Moreover, the limited capability of storing electricity implies a volatile price, especially when the interval between the transaction and delivery of electricity shortens (Bessec & Fouquau, 2018). In today's deregulated electric power markets, the accurate load forecasts are also critical to support the electricity transactions and decision making. The accurate load forecasting based on the historical information subject to possible data integrity attacks presents a great challenge to the industry.

In the past decades, a wealthy literature on load forecasting has been developed (Hong & Fan, 2016; Weron, 2006). Most of the published studies focus on developing and implementing various load forecasting models including multiple linear regression (MLR) (Charlton & Singleton, 2014; Hong et al., 2014), artificial neural networks (ANN) (Hippert et al., 2001), support vector regression (SVR) (Chen et al., 2004), and fuzzy interaction regression (FIR) (Hong & Wang, 2014). The two Global Energy Forecasting Competitions, namely, GEFCom2012 and GEFCom2014 (sponsored by IEEE Power and Energy Society and organized by the IEEE Working Group on Energy Forecasting), have also stimulated many novel ideas of hierarchical load forecasting and probabilistic load forecasting (Hong et al., 2016; Hong et al., 2014). In addition, the combinations of stationary wavelet transform forecasts and seasonal exponential smoothing forecasts are applied to electric load forecasting in (Bessec & Fouquau, 2018) and (Rendon-Sanchez & Menezes, 2019), respectively. The temporal hierarchies with autocorrelation are also introduced for hierarchical load forecasting in (Nystrup et al., 2020).

Several winners from the aforementioned competitions conducted the procedures of outlier detection and data cleansing before performing load forecasting (Charlton & Singleton, 2014; Xie & Hong, 2016). Some other papers touched on the anomaly detection with varying degrees of emphasis (Akouemo & Povinelli, 2016; Luo et al., 2018; Yue et al., 2019). While most of the existing studies focused on small-scaled random outliers or anomalies, how data integrity attacks may affect electric load forecasting has not been seriously investigated. As the first of its kind, the

empirical study in (Luo et al., 2018) benchmarked the robustness of four representative load forecasting models (i.e, MLR, ANN, SVR, and FIR). It clearly demonstrated that the forecasting accuracy of each of these four models deteriorates dramatically as the level of malicious data integrity attacks on the historical load data increases. Under data integrity attacks, a large portion of historical load data could be maliciously altered with large magnitudes by hackers, resulting in many observations deviating markedly from the normal levels. Consequently, the anomalies tend to greatly impact the commonly used least square estimators. To alleviate the impacts of anomalies from data attacks, the iteratively re-weighted least squares (IRLS) and L1 regression are introduced in (Luo et al., 2019) to reduce the impacts of large least square residuals. However, these robust regression models in (Luo et al., 2019) are not able to generate accurate forecasts under large-scaled data attacks, especially when the percentage of attacked data becomes greater than 40%.

In (Luo et al., 2018), the SVR model was shown to be more robust than the models of MLR, ANN and FIR. A possible reason is that the regression curve obtained by SVR is determined mainly by the underlying support vectors and thus less affected by the outliers and noise. Notice that, to capture the nonlinear relationship between the load and explanatory variables, nonlinear kernel functions are often adopted in SVR models for electric load forecasting (Ceperic et al., 2013; Hahn et al., 2009). A kernel function maps all data points from the original space to a higher dimensional feature space, and then one hyperplane is generated in this feature space to fit the mapped points. However, there lacks a universal rule to automatically choose a proper kernel function for a given dataset. Moreover, for electric load forecasting, the performance of SVR models heavily depends on the parameters selected in the kernel function. It may take a significant amount of computational time and effort to select a proper kernel function and its parameters. More seriously, the singular kernel matrices in some cases can heavily influence the forecasting accuracy and computational efforts of SVR-based load forecasting. Hence, the employment of kernel function greatly limits the efficiency and accuracy of the SVR model for electric load forecasting.

In the field of support vector machine (SVM), to overcome the drawbacks induced by employing kernels, a kernel-free quadratic surface SVM (QSSVM) model was proposed to directly utilize one quadratic surface for nonlinear classification in (Luo et al., 2016). The experimental results indicated the superior performance of the kernel-free QSSVM model over other SVM model with Gaussian or quadratic kernel in terms of classification accuracy. Based on the QSSVM model, a semi-supervised QSSVM model with fuzzy set (Tian et al., 2017) and an unsupervised QSSVM model (Luo et al., 2020) have been developed for mislabeled classification and unsupervised classification, respectively. Notice that, in theory, any twice continuously differentiable nonlinear function has a Taylor approximation in quadratic form. Therefore, we intend to propose a kernel-free quadratic surface SVR (QSSVR) for effective and efficient load forecasting in this paper.

The key contribution of this paper is to propose a robust kernel-free nonlinear SVR model for load forecasting under data integrity attacks. The kernel-free QSSVR model directly utilizes one quadratic surface to fit the data points for load forecasting under data attacks. We develop a weight function to evaluate the relative importance of each data point in the load history to reduce the contributions of attacked points to the regressor. a kernel-free weighted QSSVR (WQSSVR) model is finally proposed for load forecasting under data integrity attacks by

incorporating the weights of points into the QSSVR model. Some theoretical properties of the proposed WQSSVR model are studied. To imitate the data integrity attacks targeting economic losses or system blackouts of modern power grids, we conduct computational experiments in which the majority part of historical load data is deliberately decreased or increased following different normal or uniform distributions. Finally, the proposed WQSSVR model exhibits superior accuracy in forecasting comparing with state-of-the-art robust regression models (IRLS and L1 regression) and other well-known models (MLR and SVR with Gaussian kernel) for electric load forecasting.

The rest of the paper is arranged as follows. Section 2 briefly reviews some commonly-used SVR models for electric load forecasting. Then a robust kernel-free WQSSVR model is proposed for load forecasting in Section 3. Section 4 studies theoretical properties of the proposed model. Computational experiments on electric load forecasting under various types of data attacks are conducted in Section 5 to compare the accuracy of the proposed model with other well-known load forecasting methods. Section 6 particularly shows the numerical tests of the proposed model on a total of 30 datasets in different zones for the discussion of robustness. Section 7 concludes this paper.

2. Review of Related Support Vector Regressions

In this section, we briefly review the classical and frequently used SVR models for electric load forecasting.

As a nonlinear generalization of the generalized portrait algorithm, the support vector (SV) algorithm is first developed in Russia in the sixties (Vapnik & Lerner, 1963). In its current form, the support vector machine (SVM) was largely developed and extensively applied at AT&T Bell Laboratories by Vapnik and co-workers (Cortes & Vapnik, 1995; Vapnik, 1995). As the generalization of SVM, the SVR was developed and attained the excellent performance in many real-world forecasting problems such as predicting the loss given defaults (Yao et al., 2015), corporate bond recovery rate (Nazemi et al., 2018) and so forth. Electric load forecasting is particularly important in the utility industry. The first notable development of SVR model for electric load forecasting was performed by Chen et al. at the EUNITE competition 2001 (Chen et al., 2004).

In (Chen et al., 2004), for the given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$, where the input vector $x^i = (x_1^i, x_2^i, \cdots, x_m^i) \in R^m$ denotes the calendar attributes (including dates and holidays) and temperature attribute, and an $y^i \in R$ (i.e., the related output of x^i) denotes the load value of the *i*th day, the following classical SVR model is introduced to find the parameters $w \in R^m$ and $b \in R$ of a fitting hyperplane $y = w^T x + b$ of this training data set:

$$\begin{aligned} &\min_{w,b,\xi} \frac{1}{2} w^T w + C_p \sum_{i=1}^{n} \xi_i \\ \text{s.t.} \quad &\delta + \xi_i \geq y^i - (w^T x^i + b), i = 1, 2, \cdots, n, \\ &y^i - (w^T x^i + b) \geq -\delta - \xi_i, i = 1, 2, \cdots, n, \\ &\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0, \end{aligned} \tag{SVR}$$

where $\xi_i, i = 1, 2, \cdots, n$ are the errors of training points outside the insensitive tube $|y - (w^T x + b)| \leq \delta$, the given parameters $\delta, C_p > 0$ are the width of the tube and cost of training errors, respectively.

For nonlinear fitting, all training points are first mapped to a higher dimensional space by a nonlinear kernel function and then a hyperplane is found to fit the mapped points. Below is the SVR model with a commonly-used Gaussian kernel (denoted as "SVR_Gau" in this paper):

$$\min_{w,b,\xi} \frac{1}{2} w^T w + C_p \sum_{i=1}^{n} \xi_i$$

$$\text{s.t.} \quad \delta + \xi_i \geq y^i - (w^T \phi(x^i) + b), i = 1, 2, \cdots, n, \qquad \text{(SVR\_Gau)}$$

$$y^i - (w^T \phi(x^i) + b) \geq -\delta - \xi_i, i = 1, 2, \cdots, n,$$

$$\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0,$$

where $\delta, C_p > 0$ are given parameters, and $\phi : R^m \to R^d$ (where $d>m$) is the Gaussian kernel function. These SVR models won the competition 2001 organized by the EUNITE network and intrigued the research interests of the load forecasting community.

3. A Weighted Quadratic Surface SVR Model

In this section, we first introduce the vanilla model, which includes the underlying variables for electric load forecasting. Then a kernel-free QSSVR model is introduced by directly utilizing a quadratic surface to fit the training data. Finally, by incorporating the weights of training points, we propose a kernel-free WQSSVR model for effective electric load forecasting.

3.1 The Vanilla Model

Thousands of models including many various types of variables have been published in the load forecasting literature (Hong, 2010). As a frequently cited model, the following vanilla model is utilized in GEFCom2012 (Hong, Pinson, et al., 2014) to benchmark load forecasting accuracy:

$$E(y_l) = r_0 + r_1 x_{tr} + r_2 x_h + r_3 x_w + r_4 x_m + r_5 x_t + r_6 (x_t)^2 + r_7 (x_t)^3 + r_8 x_h * x_w + r_9 x_t * x_h + r_{10} (x_t)^2 * x_h + r_{11} (x_t)^3 * x_h + r_{12} x_t * x_m + r_{13} (x_t)^2 * x_m + r_{14} (x_t)^3 * x_m, \qquad \text{(vanilla)}$$

where y_l is a variable of electric loads; x_{tr} is a variable of the increasing integers on behalf of a trend of increasing loads; x_h is a vector including 24 dummy variables on behalf of 24 hours in a day; x_w is a vector including 7 dummy variables on behalf of 7 days in a week; x_m is a vector including 12 dummy variables on behalf of 12 months in a year; x_t is a variable on behalf of the temperature value. Hence, this vanilla model has totally 289 variables, which works effectively for electric load forecasting (Hong et al., 2016; Hong et al., 2014; Hong et al., 2014). In this paper, we are going to use these variables in the vanilla model as the underlying variables for the proposed weighted QSSVR model.

3.2 Quadratic surface SVR model

For nonlinear fitting of training data set $\{(x^i, y^i), i = 1, \cdots, n\}$, where $x^i = (x_1^i, x_2^i, \cdots, x_m^i) \in R^m$ and $y^i \in R$, the QSSVR model intends to find the parameters (W, b, c) of a quadratic surface

$$y = \frac{1}{2} x^T W x + b^T x + c,$$

$$W = W^T = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{12} & w_{22} & \cdots & w_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ w_{1m} & w_{2m} & \cdots & w_{mm} \end{bmatrix} \in R^{m \times m}, \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \in R^m, c \in R,$$

that fits the *n* training points without utilizing any kernel function.

Analogously to the classical SVR models, the goal of QSSVR model is to generate one "confidence interval" and then try to include the training points in this "interval" as many as possible. More specifically, we first ignore the training errors of the training points being inside the tube $| y - (0.5 x^T W x + b^T x + c) | \leq \delta$ (i.e., "confidence interval") for given δ. Then, to include the training points in this tube as many as possible, we not only maximize the geometrical margin between the upper and lower bounds of the tube, but also minimize the deviations of training points with errors larger than δ. And the geometrical margin between the upper and lower bounds of the tube can be approximated by minimizing $\sum_{i=1}^{n} || W x^i + b ||_2^2$, similar to the formulation of QSSVM in (Luo et al., 2016). Therefore, the QSSVR model can be formulated as

$$\min_{W, b, c, \xi} \sum_{i=1}^{n} || W x^i + b ||_2^2 + C_p \sum_{i=1}^{n} \xi_i$$

$$\text{s.t.} \quad \delta + \xi_i \geq y^i - (\frac{1}{2} (x^i)^T W x^i + b^T x^i + c), i = 1, 2, ..., n, \qquad \text{(QSSVR)}$$

$$y^i - (\frac{1}{2} (x^i)^T W x^i + b^T x^i + c) \geq -\delta - \xi_i, i = 1, 2, ..., n,$$

$$\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0,$$

where $\delta, C_p > 0$ are given parameters, and the constant $C_p > 0$ determines the trade-off between the geometrical margin between the bounds of the tube and the amount up to which deviations larger than δ are tolerated.

3.3 Weighted Quadratic Surface SVR Model

For electric load forecasting under data integrity attacks, the available training data set is corrupted with lots of attacked points, which are always treated as outliers or noise. In these cases, the performance of the QSSVR model may suffer the loss of load forecasting accuracy since the QSSVR model assumes that every training point makes the same contribution to the regressors. To properly address these issues, we develop the following weight function to efficiently calculate the weights of all points for characterizing their relative contributions to the regressor:

$$\beta_i = e^{-|u_i|}, i = 1, 2, ..., n$$

where $u_i = lsr_i / MED, i = 1,2,...,n$ with $lsr_i, i = 1,2,...,n$ being the absolute residuals of the training points with regard to L_1 regression and *MED* is the median absolute deviation of the residuals from their median. Hence, the weight of the training point with smaller residual is larger while that of the training point with larger residual is smaller.

Then, to reduce the contributions of attacked points to the regressor, we propose a WQSSVR model by incorporating the calculated weights $\beta_i, i = 1,...,n$ into the two terms in the objective of QSSVR since both of these two terms are related to the training points (including the attacked points) as the following:

$$\min_{W,b,c,\xi} \sum_{i=1}^{n} \beta_i \| Wx^i + b \|_2^2 + C_p \sum_{i=1}^{n} \beta_i \xi_i$$

$$\text{s.t.} \quad \delta + \xi_i \geq y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c), i = 1,2,...,n, \qquad \text{(WQSSVR)}$$

$$y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c) \geq -\delta - \xi_i, i = 1,2,...,n,$$

$$\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0,$$

where $\delta, C_p > 0$ are given parameters. Similarly, the terms $\beta_i \xi_i$ and $\beta_i \left\| Wx^i + b \right\|_2^2$ can be deemed as measuring the misclassification error ξ_i and $\left\| Wx^i + b \right\|_2^2$ (i.e., the geometrical margin between the upper and lower bounds of the "confidence interval" at point x^i) with the weight β_i, respectively. If the point x^i is more likely to be an attacked point, which indicates that x^i is less important, then the related β_i is expected to be smaller to reduce the effect of ξ_i and $\left\| Wx^i + b \right\|_2^2$ in the model (WQSSVR). Hence, the main advantage of introducing the weights into the QSSVR model is reducing the contributions of attacked points to minimize the misclassification errors and maximize the geometrical margins between the upper and lower bounds of "confidence interval". Moreover, the objective function of WQSSVR model avoids overfitting and underfitting the training data by minimizing the first regularization term and second term of misclassification errors, respectively.

As *W* is a symmetric matrix, the model (WQSSVR) can be equivalently reformulated for one smaller-sized optimization problem as the following: first define *w* be the vector formed by taking the $(m^2 + m)/2$ elements in the upper triangular part of matrix *W*, i.e.,

$$\Psi \triangleq (w_{11}, w_{12}, ..., w_{1m}, w_{22}, w_{23}, ..., w_{2m}, ..., w_{mm})^T \in R^{\frac{m^2+m}{2}}$$

Then construct an $m \times ((m^2 + m)/2)$ matrix M_i for each training point $x^i \in R^m, i = 1,2,...,n,$ as follows. For the *j*-th row of $M_i, j = 1,2,...m,$ check the elements of the vector Ψ one by one. If the *p*-th element of Ψ is w_{jk} or w_{kj} for some $k = 1,2,...m,$ then let the *p*-th element in the *j*-th row of matrix M_i be x_k^j, otherwise be 0. Afterwards, let

$$H_i \triangleq (M_i, I_{m \times m}) \in R^{m \times (\frac{m^2+m}{2} + m)}, i = 1,2,...n,$$

$$G \triangleq \sum_{i=1}^{n} \beta_i H_i^T H_i \in R^{\left(\frac{m^2+3m}{2}\right) \times \left(\frac{m^2+3m}{2}\right)},$$

$$z \triangleq (\Psi^T, b^T)^T \in R^{\frac{m^2+3m}{2}},$$

$$s_i \triangleq (\frac{1}{2}x_1^i x_1^i, ..., x_1^i x_m^i, \frac{1}{2}x_2^i x_2^i, ..., x_2^i x_m^i, ..., \frac{1}{2}x_{m-1}^i x_{m-1}^i, x_{m-1}^i x_m^i, \frac{1}{2}x_m^i x_m^i, x_1^i, x_2^i, ..., x_m^i) \in R^{\frac{m^2+3m}{2}}.$$

Then the model (WQSSVR) can be equivalently reformulated as：

$$\min_{z,c,\xi} z^T G z + C_p \sum_{i=1}^{n} \beta_i \xi_i$$

$$\text{s.t.} \quad \delta + \xi_i \geq y^i - (s_i^T z + c) \geq -\delta - \xi_i, i = 1, 2, ..., n, \qquad \text{(WQSSVR')}$$

$$\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0.$$

where $\delta, C_p > 0$ are given parameters. This WQSSVR model can be solved efficiently by a primal-dual interior-point method, especially for the large-scaled cases.

4. Theoretical Properties of WQSSVR

In this section, some theoretical properties of the WQSSVR model including the existence, uniqueness and support vector expansion of the optimal solution, are studied. We first study the solvability of the WQSSVR model as follows.

Theorem 4.1. For any given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$ and $C_p > 0$, there exists an optimal solution to the model (WQSSVR') with a finite objective value.

Proof. Take any $(\tilde{z}, \tilde{c})$ and let $\tilde{\xi}_i \triangleq \max\{0, |y^i - (s_i^T \tilde{z} + \tilde{c})| - \delta\}, i = 1, ..., n$. It is easy to see that $(\tilde{z}, \tilde{c}, \tilde{\xi}_i)$ is feasible to the model (WQSSVR'). Notice that, the objective function is continuous and the feasible domain is a closed convex set defined by linear inequalities. Moreover, for any $z \in \mathbb{R}^{\frac{m^2+3m}{2}}$ and $\xi_i \geq 0, i = 1, ..., n$, $z^T G z + C_p \sum_{i=1}^{n} \beta_i \xi_i$ $= \sum_{i=1}^{n} (\beta_i \|H_i z\|_2^2 + C_p \beta_i \xi_i) \geq 0$, which indicates that the objective value is bounded below by 0 over the feasible domain. Therefore, there exists an optimal solution to model (WQSSVR') with a finite objective value. □

Let $F^* = \{(z, c, \xi) \in \mathbb{R}^{\frac{m^2+3m}{2}} \times \mathbb{R}^1 \times \mathbb{R}^n \mid (z, c, \xi)$ is an optimal solution to the model (WQSSVR') $\}$. Then $F^* \neq \phi$ by Theorem 1. Furthermore, the next three results can be obtained.

Theorem 4.2. For any given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$ and $C_p > 0$, if *G* is positive definite, then the optimal solution of model (WQSSVR') is unique with respect to the variable *z*.

Proof. Assume that $(\hat{z}, \hat{c}, \hat{\xi}) \in F^*$, $(\bar{z}, \bar{c}, \bar{\xi}) \in F^*$ and $\hat{z} \neq \bar{z}$. For any $0 < \eta < 1$, $(\tilde{z}, \tilde{c}, \tilde{\xi}) \triangleq \eta(\hat{z}, \hat{c}, \hat{\xi}) + (1 - \eta)(\bar{z}, \bar{c}, \bar{\xi})$ is feasible to model (WQSSVR) because of the convex feasible domain. Therefore,

$$\tilde{z}^T G \tilde{z} + C_p \sum_{i=1}^{n} \beta_i \tilde{\xi}_i \geq \hat{z}^T G \hat{z} + C_p \sum_{i=1}^{n} \beta_i \hat{\xi}_i,$$

$$\tilde{z}^T G \tilde{z} + C_p \sum_{i=1}^{n} \beta_i \tilde{\xi}_i \geq \bar{z}^T G \bar{z} + C_p \sum_{i=1}^{n} \beta_i \bar{\xi}_i.$$

Multiplying the first inequality by η and the second by $(1-\eta)$, we have $\tilde{z}^T G\tilde{z} + C_p \sum_{i=1}^n \beta_i \tilde{\xi}_i \geq \eta \hat{z}^T G\hat{z} + (1-\eta)\bar{z}^T G\bar{z}$ $+C_p \sum_{i=1}^n (\eta\beta_i \hat{\xi}_i + (1-\eta)\beta_i \bar{\xi}_i)$. Equivalently, $[\eta\hat{z} + (1-\eta)\bar{z}]^T G[\eta\hat{z} + (1-\eta)\bar{z}] \geq \eta \hat{z}^T G\hat{z} + (1-\eta)\bar{z}^T G\bar{z}$, which infers that $\eta(1-\eta)(\hat{z}-\bar{z})^T G(\hat{z}-\bar{z}) \leq 0$. When G is positive definite, we have $\hat{z} - \bar{z} = 0$, which contradicts to the assumption that $\hat{z} \neq \bar{z}$. □

Therefore, for any given training data set, if *G* is positive definite, the main shape of the fitting quadratic surface is uniquely determined by the optimal solution of model (WQSSVR') with respect to the variable *z*.

Theorem 4.3. For any given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$ and $C_p > 0$, if *G* is positive definite, then there exist constants $\underline{c}$ and $\bar{c}$ such that $\underline{c} \leq c \leq \bar{c}$, for any $(z, c, \xi) \in F^*$.

Proof. Let $(\hat{z}, \hat{c}, \hat{\xi}) \in F^*$. When *G* is positive definite, by Theorem 4.2, $\hat{z}$ is uniquely determined and, for each $(z, c, \xi) \in F^*$, we have $z = \hat{z}$ and $z^T Gz + C_p \sum_{i=1}^n \beta_i \xi_i = \hat{z}^T G\hat{z} + C_p \sum_{i=1}^n \beta_i \hat{\xi}_i$. Consequently, $\sum_{i=1}^n \beta_i \xi_i = \sum_{i=1}^n \beta_i \hat{\xi}_i$ $\triangleq \bar{\eta}$, which is uniquely determined. Since $\beta_i, \xi_i \geq 0$ for any i, we have $\beta_i \xi_i \leq \sum_{i=1}^n \beta_i \xi_i = \bar{\eta}$. Therefore, $c \leq y^i - s_i^T z + \delta + \xi_i \leq y^i - s_i^T \hat{z} + \delta + \bar{\eta} / \beta_i$ and $c \geq y^i - s_i^T z - \delta - \xi_i \geq y^i - s_i^T \hat{z} - \delta - \bar{\eta} / \beta_i$.

Let $\bar{c} = \min_{\{i=1,\cdots,n\}} \{y^i - s_i^T \hat{z} + \delta + \bar{\eta} / \beta_i\}$, $\underline{c} = \max_{\{i=1,\cdots,n\}} \{y^i - s_i^T \hat{z} - \delta - \bar{\eta} / \beta_i\}$, then we have $\underline{c} \leq c \leq \bar{c}$. □

Notice that, if the matrix *G* in model (WQSSVR') is only positive semi-definite, we can always append a perturbation such that the matrix $G + \varepsilon I$ ($\varepsilon > 0$, I is the identity matrix) becomes positive definite. Then, consider the following perturbed model:

$$\min_{z,c,\xi} z^T (G + \varepsilon I) z + C_p \sum_{i=1}^n \beta_i \xi_i$$

$$\text{s.t.} \quad \delta + \xi_i \geq y^i - (s_i^T z + c) \geq -\delta - \xi_i, i = 1, 2, ..., n, \qquad \text{(WQSSVR-eps)}$$

$$\xi = (\xi_1, \xi_2, ..., \xi_n)^T \geq 0.$$

Similar to the proof of Theorem 4.1, it is easy to verify that the model (WQSSVR-eps) has at least one optimal solution with a finite optimal value. Let $(z^\varepsilon, c^\varepsilon, \xi^\varepsilon)$ be an optimal solution of model (WQSSVR-eps), then the model (WQSSVR') and its perturbed model (WQSSVR-eps) can be related by the next two results.

Lemma 4.4. For any given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$ and $C_p > 0$, if the optimal value of model (WQSSVR') is *v* and the optimal value of model (WQSSVR-eps) is v_ε, for given $\varepsilon > 0$, then $v_\varepsilon \to v$ as $\varepsilon \to 0$.

Proof. Let $(\tilde{z}, \tilde{c}, \tilde{\xi}) \in F^*$. If $\|\tilde{z}\| \neq 0$, for $(z^\varepsilon, c^\varepsilon, \xi^\varepsilon)$ and any $\delta > 0$, there exists $\varepsilon_0 \triangleq \dfrac{\eta}{(\tilde{z}^T)(\tilde{z})}$ such that when $0 < \varepsilon < \varepsilon_0$, $v \leq (z^\varepsilon)^T Gz^\varepsilon + C_p \sum_{i=1}^n \beta_i \xi_i^\varepsilon \leq v_\varepsilon \leq \tilde{z}^T (G + \varepsilon I)\tilde{z} + C_p \sum_{i=1}^n \beta_i \tilde{\xi}_i = v + \varepsilon(\tilde{z})^T (\tilde{z}) < v + \eta$, i.e., $|v_\varepsilon - v| < \delta$.

If $\|\tilde{z}\| = 0$, by the expression $v \leq (z^\varepsilon)^T Gz^\varepsilon + C_p \sum_{i=1}^n \beta_i \xi_i^\varepsilon \leq v_\varepsilon \leq \tilde{z}^T (G + \varepsilon I)\tilde{z} + C_p \sum_{i-1}^n \beta_i \tilde{\xi}_i = v + \varepsilon(\tilde{z})^T (\tilde{z}) = v$, which infers that $v = v_\varepsilon$. Hence, $v_\varepsilon \to v$ as $\varepsilon \to 0$. □

Remark. For any given $C_p > 0$ and $0 < \varepsilon_1 < \varepsilon_2$, we have $v_{\varepsilon_1} \le (z^{\varepsilon_2})^T G z^{\varepsilon_2} + \varepsilon_1 (z^{\varepsilon_2})^T (z^{\varepsilon_2}) + C_p \sum_{i=1}^n \beta_i \xi_i^{\varepsilon_2} < (z^{\varepsilon_2})^T G z^{\varepsilon_2} + \varepsilon_2 (z^{\varepsilon_2})^T (z^{\varepsilon_2}) + C_p \sum_{i=1}^n \beta_i \xi_i^{\varepsilon_2} = v_{\varepsilon_2}$. Therefore, the sequence $\{v_\varepsilon\}$ monotonically decreases to v as $\varepsilon \searrow 0$.

Theorem 4.5. For any given training data set $\{(x^i, y^i), i = 1, \cdots, n\}$ and $C_p > 0$, if the sequence $\{(z^\varepsilon, c^\varepsilon, \xi^\varepsilon)\}$ converges to (z^0, c^0, ξ^0) as $\varepsilon \to 0$, then $(z^0, c^0, \xi^0) \in F^*$ and $(z^0)^T z^0 \le z^T z$, for any $(z, c, \xi) \in F^*$.

Proof. While $\{(z^\varepsilon, c^\varepsilon, \xi^\varepsilon)\} \to (z^0, c^0, \xi^0)$ as $\varepsilon \to 0$, it is easy to verify that (z^0, c^0, ξ^0) is feasible to model (WQSSVR'). By Lemma 4.4, $v_\varepsilon \to v$ as $\varepsilon \to 0$. Then we have $(z^0, c^0, \xi^0) \in F^*$. For any $\varepsilon > 0$ and any $(z, c, \xi) \in F^*$, it should be noted that (z, c, ξ) is feasible to model (WQSSVR-eps). Hence, we have

$$(z^\varepsilon)^T (G + \varepsilon I) z^\varepsilon + C_p \sum_{i=1}^n \beta_i \xi_i^\varepsilon = (z^\varepsilon)^T G z^\varepsilon + \varepsilon (z^\varepsilon)^T z^\varepsilon + C_p \sum_{i=1}^n \beta_i \xi_i^\varepsilon \le z^T (G + \varepsilon I) z + C_p \sum_{i=1}^n \beta_i \xi_i = z^T G z + \varepsilon z^T z + C_p \sum_{i=1}^n \beta_i \xi_i$$

Since $(z, c, \xi) \in F^*$, we have $z^T G z + C_p \sum_{i=1}^n \xi_i \le (z^\varepsilon)^T G z^\varepsilon + C_p \sum_{i=1}^n \xi_i^\varepsilon$. Consequently, $(z^\varepsilon)^T z^\varepsilon \le (z)^T z$ for any $\varepsilon > 0$. Hence, as $\varepsilon \to 0, (z^0)^T z^0 \le (z)^T z$ for any $(z, c, \xi) \in F^*$. □

Generally speaking, for a training data set with *G* being positive semi-definite only, the perturbed model (WQSSVR-eps) with a sufficiently small $\varepsilon > 0$ can be solved to generate a fitting quadratic surface for regression. Therefore, without loss of generality, *G* is supposed to be positive definite in the model (WQSSVR').

Moreover, we can formulate the dual problem of model (WQSSVR') as follows. First, the Lagrangian function is written as below by introducing three groups of dual variables $\alpha_i, \hat{\alpha}_i, \mu_i \ge 0, i = 1, \cdots, n$:

$$L(z, c, \xi, \alpha, \hat{\alpha}, \mu) = z^T G z + C_p \sum_{i=1}^n \beta_i \xi_i + \sum_{i=1}^n \alpha_i \left(s_i^T z + c - y^i - \delta - \xi_i \right) + \sum_{i=1}^n \hat{\alpha}_i \left(y^i - s_i^T z - c - \delta - \xi_i \right) - \sum_{i=1}^n \mu_i \xi_i \quad (1)$$

the first-order partial derivative of Lagrangian function be 0, the following formulas can be obtained:

$$\frac{\partial L}{\partial z} = 0 \Rightarrow z = \frac{1}{2} \sum_{i=1}^n (\hat{\alpha}_i - \alpha_i) G^{-1} s_i,$$

$$\frac{\partial L}{\partial c} = 0 \Rightarrow \sum_{i=1}^n (\hat{\alpha}_i - \alpha_i) = 0,$$

$$\frac{\partial L}{\partial \xi} = 0 \Rightarrow C_p \beta_i = \hat{\alpha}_i + \alpha_i + \mu_i.$$

Finally, after replacing the corresponding variables in the formula (1) with the above formulas, the dual problem of model (WQSSVR') can be formulated as the following:

$$\max \sum_{i=1}^n \left[(\hat{\alpha}_i - \alpha_i) y^i - \varepsilon (\hat{\alpha}_i + \alpha_i) \right] - \frac{1}{4} \left(\sum_{i=1}^n (\hat{\alpha}_i - \alpha_i) s_i \right)^T G^{-1} \left(\sum_{i=1}^n (\hat{\alpha}_i - \alpha_i) s_i \right)$$

$$\text{s.t.} \quad \sum_{i=1}^n (\hat{\alpha}_i - \alpha_i) = 0, \qquad \text{(D-WQSSVR')}$$

$$0 \le \alpha_i + \hat{\alpha}_i \le C_p \beta_i.$$

Both of models (WQSSVR') and (D-WQSSVR') are convex linearly constrained quadratic programming problems, no duality gap exists. Hence, the optimal conditions for these models are:

$$\begin{aligned} \alpha_i(s_i^T z + c - y^i - \delta - \xi_i) &= 0 \\ \hat{\alpha}_i(y^i - s_i^T z - c - \delta - \xi_i) &= 0 \\ \left(C_p\beta_i - \alpha_i - \hat{\alpha}_i\right)\varepsilon_i &= 0 \\ \alpha_i \cdot \hat{\alpha}_i &= 0 \end{aligned} \tag{2}$$

From these KKT conditions, it should be noted that either α_i or $\hat{\alpha}_i$ would be 0 for all training points, and $\alpha_i = \hat{\alpha}_i = 0$ for all training points falling within the tube. Moreover, these above optimal conditions can be solved to obtain the optimal solutions (z^*, c^*, ξ^*) and $(\alpha_i^*, \hat{\alpha}_i^*, i = 1, \cdots, n)$ of models (WQSSVR') and (D-WQSSVR'), respectively. Then the following results can be obtained by Lagrangian duality theory:

$$z^* = \frac{1}{2}\sum_{i=1}^{n}\left(\hat{\alpha}_i^* - \alpha_i^*\right)G^{-1}s_i \tag{3}$$

Hence, from the optimal conditions (2) and formula (3), only the training points falling outside the tube (i.e., either α_i^* or $\hat{\alpha}_i^*$ would be non-zero) contribute to the shape of fitting quadratic surface (i.e., given by z^*) so that these points are called the support vectors. Moreover, by utilizing any support vector (e.g. the *j*-th training point), the intercept parameter can be calculated as the following:

$$c^* = y_j + \delta - \frac{1}{2}\sum_{i=1}^{n}\left(\hat{\alpha}_i^* - \alpha_i^*\right)G^{-1}s_i^T s_j. \tag{4}$$

Therefore, from formulas (3) and (4), the optimal solution of model (WQSSVR') is the expansion of support vectors. Then the regression quadratic surface obtained by the WQSSVR model is mainly determined by the support vectors, and less affected by outliers and noise (i.e., attacked points) from another perspective.

5. Numerical Experiments & Results

In this section, the setups of numerical experiments are first introduced and then the numerical results of five tested load forecasting models are shown.

5.1 Setups of Computational Experiments

The data used in this section is from GEFCom2012 (Hong, Pinson, et al., 2014). The entire data for the load forecasting track includes 3.5 years of hourly load and temperature information for 21 zones, where the hourly loads in Z_{21} are the sum of those in the other 20 zones. Following the practices reported in (Hong, Pinson, et al., 2014; Hong & Wang, 2014), we picked two years (2005-2006) and one year (2007) of hourly load and temperature information as the training and testing periods, respectively. In general, the benchmark vanilla model is effective for

forecasting the electric loads in the residential zones, which represent the majority zones of GEFCom2012 data excluding zones 4 and 9.

In this paper, for fair comparisons, the IRLS model with bisquare function (denoted as 'IRLS_bis'), L_1 regression (denoted as 'L_1'), MLR, SVR_Gau and WQSSVR models share exactly the same variables as described in the vanilla model. All numerical experiments in this paper are performed using MATLAB (R2019a) software on a desktop equipped with an Intel Xeon Processor 2.99 GHz CPU, 31.3GB usable RAM and Microsoft Windows 10 Enterprise. The IRLS_bis, L_1, MLR, SVR_Gau and WQSSVR models are implemented using the modules "robustfit", "linprog", "robustfit", "fitrsvm", and "quadprog" of MATLAB, respectively. Moreover, to tune the parameter C_p for WQSSVR model, we have divided the training data set into three equivalent parts, and then respectively utilized the first two parts and last part as the pre-training data and validation data to select C_p in $\{2^{28}, 2^{29},...,2^{36},2^{37}\}$, and the δ value is determined by utilizing the absolute residuals of points with regard to L_1 regression.

5.2 Benchmarking Performance without Data Integrity Attacks

Table I records the mean absolute percentage error (MAPE) values of all five models without data integrity attacks, in case other researchers may find them useful for the benchmarking purpose. It should be noted that, a smaller MAPE value indicates the more accurate load forecasts yielded by the related model. Overall, the MLR and SVR_Gau models produce the most and least accurate load forecasts among all five models, respectively. The performance of WQSSVR is as close as that of L_1 regression or IRLS_bis model in terms of load forecasting accuracy. Since the results at low level zones do not add much information nor change our final conclusions and findings, we first focus on the aggregated zone Z_{21} for experiments of electric load forecasting under data intergrity attacks to avoid verbose presentation.

Zone	IRLS_bis	L_1	MLR	SVR_Gau	WQSSVR
21	5.30	5.33	**5.22**	6.31	5.29
1	7.08	7.08	7.01	8.34	**6.93**
2	5.56	**5.52**	5.62	7.39	5.59
3	5.56	**5.52**	5.62	7.39	5.59
5	9.69	**9.64**	9.88	10.51	9.69
6	5.56	**5.53**	5.55	7.24	5.59
7	5.56	**5.52**	5.62	7.46	5.60
8	7.59	7.59	7.50	8.74	**7.39**
10	6.70	6.79	6.70	9.53	**6.64**
11	7.97	8.20	7.70	9.63	**7.64**
12	6.95	6.99	**6.78**	8.35	7.31
13	7.48	7.44	**7.39**	8.11	7.54
14	9.41	9.40	**9.38**	10.52	9.92
15	**7.38**	7.40	7.44	7.96	7.76
16	8.13	**8.11**	8.12	9.10	8.23
17	5.31	5.30	**5.26**	6.93	5.32
18	6.77	6.73	**6.72**	7.71	6.75
19	7.88	**7.87**	7.90	8.86	7.94
20	5.73	5.68	5.74	7.44	**5.66**
Avg	7.02	7.02	**7.00**	8.40	7.06

4	**15.83**	15.89	16.08	15.86	15.90
9	164.05	153.48	**139.16**	157.52	159.93

Table I: MAPE (%) of hourly load forecast without data attacks

5.3 Data Integrity Attacks Targeting Economic Losses

When the values of the majority part of the load history are increased, the load forecasts would most likely be higher than the nominal loads. These over-forecasts may cost power companies unnecessary expenses on the generation of unused electricity, the infrastructure upgrade and maintenance. Moreover, the over-forecasts may results in an excess of spinning reserves and probably unnecessary start-ups of peaking and cycling units, which reduce the overall economic efficiency. In this subsection, the data integrity attack on the training dataset targeting economic losses is simulated as follows: *k%* of all observations are randomly picked with their electric loads being deliberately increased by *p%* to make these selected observations become outliers.

Using the training dataset (years of 2005 and 2006) under the simulated data integrity attack targeting economic losses, we estimate the parameters of the regressors via all five models. The original testing dataset (year of 2007) is used to calculate the mean absolute percentage error (MAPE) values of all five models. To comprehensively evaluate the performance of all five models, we have conducted three groups of numerical experiments under normally-distributed or uniformly-distributed data attacks as the following: 1) vary k from 40 to 90 with the increment of 10, *p%* is generated by the normal distribution $N(\mu,\sigma^2)$, where μ is varied from 0.25 to 0.75 with the increment of 0.25 and σ is 0.5; 2) k is 70, *p%* is generated by the normal distribution $N(\mu,\sigma^2)$, where μ is 0.5 and σ is varied from 0.25 to 1.5 with the increment of 0.25; 3) k is 70, *p%* is generated by the uniform distribution $U(a,b)$. For each (k, p) pair, we repeat the test with randomly selected *k%* observations for 10 times.

For each model tested in the three groups of experiments, the averages of MAPE values of 10 experiments are reported in Tables II, III and IV, respectively. From these three tables, we have the following observations: 1) For most tested numerical experiments, the WQSSVR model produces more accurate forecasts than the other four models, especially for large k and large mean of p. That's mainly because that the relative importance (i.e., weights) of attacked points are greatly reduced in WQSSVR model, which mainly utilizes the information of normal points. 2) For small-scaled data attacks (such as k=40) or small mean of p% (such as $N(0.25,0.5^2)$, $U(-0.9,0.9)$, and so forth), the L_1 regression and IRLS_bis models perform well. Similar observations can be found in (Jian Luo et al., 2019). However, as k increases or the mean of p increases, the WQSSVR model shows increasing dominance over other tested models. 3) From Table III, as the standard deviation of normally-distributed data attacks increases, the advantage of WQSSVR model over L_1 regression becomes less and less obvious. That's mainly because the ratio of training points with reduced loads increases to be closer to the ratio of training points with increased loads so that the performance of L_1 regression is improved greatly. 4) From Table IV, as the mean of uniformly-distributed data attacks increases (i.e., the ratio of the number of points with increased loads to that of points with decreased loads increases as the following: 5/5, 6/4, 7/3, 8/2, 9/1, 10/0), the WQSSVR model shows the increasing advantage over other four models.

	k \ *p%*	*N(0.25,0.5²)*	*N(0.5,0.5²)*	*N(0.75,0.5²)*
IRLS_bis		5.23	5.23	**5.24**
L_1		**5.16**	**5.19**	5.50
MLR	40	9.23	17.41	27.50
SVR_Gau		6.39	6.91	8.45
WQSSVR		5.28	5.27	5.31
IRLS_bis		5.46	10.44	28.22
L_1		**5.24**	5.97	9.63
MLR	50	11.03	22.66	35.01
SVR_Gau		6.84	8.87	14.27
WQSSVR		5.34	**5.60**	**5.84**
IRLS_bis		7.90	21.93	38.60
L_1		**5.47**	10.35	25.27
MLR	60	13.29	27.36	42.27
SVR_Gau		7.66	12.93	25.13
WQSSVR		5.64	**5.81**	**11.97**
IRLS_bis		11.84	29.19	46.26
L_1		6.80	20.56	41.61
MLR	70	15.22	32.52	48.59
SVR_Gau		9.12	19.77	38.45
WQSSVR		**5.86**	**9.58**	**26.00**
IRLS_bis		15.96	35.27	56.23
L_1		10.67	31.18	57.01
MLR	80	17.89	37.20	57.55
SVR_Gau		11.87	28.73	51.86
WQSSVR		**7.96**	**19.28**	**47.90**
IRLS_bis		19.02	40.97	63.60
L_1		16.10	39.62	64.38
MLR	90	19.76	41.98	64.19
SVR_Gau		15.84	37.25	**60.69**
WQSSVR		**12.39**	**32.14**	62.97

Table II: Forecast error in MAPE (%) under normally-distributed data attacks

	k \ *p%*	*N(0.5,0.25²)*	*N(0.5,0.5²)*	*N(0.5,0.75²)*	*N(0.5,1²)*	*N(0.5,1.25²)*	*N(0.5,1.5²)*
IRLS_bis		31.50	29.19	25.72	23.27	23.73	23.74
L_1		31.77	20.56	13.08	9.53	7.97	6.82
MLR	70	32.43	32.52	32.12	31.40	33.37	32.30
SVR_Gau		28.52	19.77	16.31	14.26	14.80	15.05
WQSSVR		**28.25**	**9.58**	**7.03**	**6.70**	**6.64**	**6.59**

Table III: Forecast error in MAPE (%) under normally-distributed data attacks targeting economic losses

	k \ *p%*	*U(-0.9,0.9)*	*U(-0.72,1.08)*	*U(-0.54,1.26)*	*U(-0.36,1.44)*	*U(-0.18,1.62)*	*U(0,1.8)*
IRLS_bis		7.06	9.45	19.04	31.52	44.34	58.25
L_1		**5.58**	**5.61**	8.25	16.73	30.51	49.05
MLR	70	6.91	11.13	23.04	34.76	46.89	60.14
SVR_Gau		9.79	8.50	11.24	18.26	31.21	46.38
WQSSVR		6.79	6.86	**6.13**	**7.37**	**13.32**	**27.07**

Table IV: Forecast error in MAPE (%) under uniformly-distributed data attacks targeting economic losses

Figures 1 and 2 depict the hourly load profiles for two representative weeks under data integrity attacks with k =

70 and *p%* following $N(0.5,0.5^2)$, respectively. One week is in the Summer of year 2006 (a training year) while the other week is in the Winter of year 2007 (a testing year). In Figure 1, the curve representing the weights of all data points for WQSSVR model is plotted. We can observe that the smaller weights are assigned to the attacked observations with larger perturbation magnitude (i.e., outliers or noise). In Figure 2, the corresponding load forecasts of tested five models are shown. From this figure, we can observe that all five models are more or less over predicting the actual load for the testing period, due to the data integrity attacks targeting economic losses. And the forecasts provided by the WQSSVR model, is much closer to the actual load than the forecasts provided by other four models.

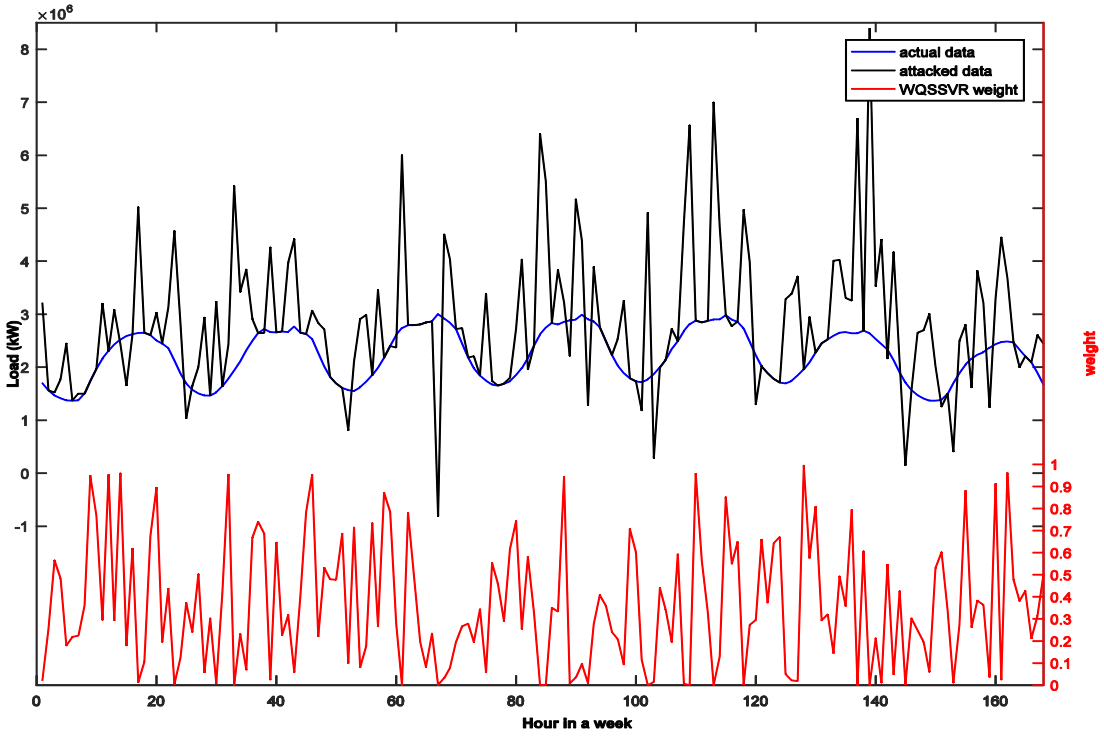

Figure 1: Hourly load profile (2006/7/30-2006/8/5) and data weights for WQSSVR under data integrity attacks targeting economic losses

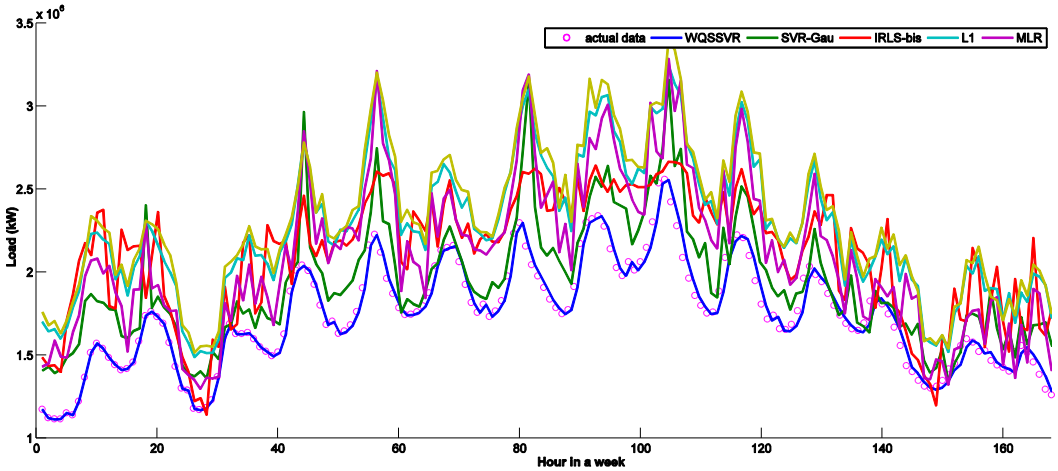

Figure 2: Forecasted (2007/1/7-2007/1/13) hourly load profile under data integrity attacks targeting economic losses

5.4 Data Integrity Attacks Targeting System Blackouts

While increasing the historical load may result in over-forecasts, decreasing the historical load may lead to the under-forecasts so that the insufficient capacity expansion in the generation, transmission and distribution systems may happen, which always leads to worse reliability indices, increases the risk for brownouts or even blackouts.

Following Section 5.3, we can create a different type of data integrity attacks targeting system blackouts by randomly picking *k%* of the observed load data in the training period and then decreasing them by *p%* to make these selected observations anomalies. Two groups of numerical experiments under such data integrity attacks are conducted as the following: 1) let k = 40, and vary *p%* from 10% to 90% with the increment of 10%. 2) let k = 40, *p%* is generated by the uniform distribution *U(a,b)*. For each (k, p) pair, we repeat the test with randomly selected *k%* observations for 10 times. Here we primarily conduct representative experiments to avoid verbose presentation.

For each model tested in the two groups of experiments, the averages of MAPE values of 10 experiments are reported in Tables V and VI, respectively. From these two tables, we have the following similar observations: 1) For most tested numerical experiments, the WQSSVR model produces more accurate forecasts than other tested models, especially for large mean of p. 2) From Table VI, as the mean of p increases (i.e., the ratio of the number of points with decreased loads to that of points with increased loads increases as the following: 5/5, 6/4, 7/3, 8/2, 9/1, 10/0), the WQSSVR model shows the increasing advantage over other four models.

	k \ *p%*	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
IRLS_bis		6.97	9.77	13.08	16.62	20.37	23.88	27.53	31.18	34.83
L_1		6.64	7.40	7.63	7.82	8.05	8.15	8.30	8.45	8.59
MLR	40	6.97	9.90	13.36	17.04	20.93	24.59	28.38	32.17	35.97
SVR_Gau		8.50	10.76	12.17	13.34	14.70	16.00	17.87	19.38	20.54
WQSSVR		**6.37**	**6.88**	**6.17**	**6.12**	**6.22**	**6.23**	**6.56**	**6.73**	**6.89**

Table V: Forecast error in MAPE (%) under various levels of data integrity attacks targeting system blackouts

	k \ *p%*	*U(-0.5,0.5)*	*U(-0.4,0.6)*	*U(-0.3,0.7)*	*U(-0.2,0.8)*	*U(-0.1,0.9)*	*U(0,1)*
IRLS_bis		5.88	8.64	14.04	20.60	28.01	34.88
L_1		**5.47**	**6.30**	8.29	12.86	20.84	29.63
MLR	70	5.84	9.40	15.54	22.02	29.21	35.81
SVR_Gau		7.58	9.32	12.21	16.95	23.91	32.13
WQSSVR		6.29	6.37	**6.21**	**7.66**	**11.38**	**18.61**

Table VI: Forecast error in MAPE (%) under uniformly-distributed data attacks targeting system blackouts

6. Discussion

In this section, we further test the load forecasting models on different datasets under uniformly-distributed data attacks targeting system blackouts. We then analyze the robustness of the proposed WQSSVR model, and discuss other possible attacks.

6.1 Different Data Sets under Uniformly-Distributed Data Attacks Targeting System Blackouts

To further test the proposed WQSSVR model on other data sets (from other zones in GEFCom2012) under data attacks, we first simulate the uniformly-distributed data integrity attacks targeting system blackouts as the following: The percentage of the attacked observations in the training data is fixed to be 70%, i.e., $k = 70$; ten test cases are created by decreasing the magnitude of randomly-selected load values by p%, where p% is generated following a uniform distribution $U(-0.2, 0.8)$. Then the five load forecasting models are tested on these data sets and the computational results are recorded in Table VII.

Moreover, we simulate the similar uniformly-distributed data integrity attacks targeting system blackouts for the load data sets of all 9 zones in ISONE (publicly available from its website *http://www.iso-ne.com/isoexpress /web/reports*) by setting k to be 70 and generating p% following the uniform distribution $U(-0.2, 0.8)$. Similarly, the load forecasting models are tested on these data sets and the results are recorded in Table VIII. Notice that, in ISONE data, two years (2013-2014) and one year (2015) of hourly load and dry bulb temperature information are selected as the training and testing periods, respectively, and the hourly loads in the ninth zone are the sum of those in the other 8 zones. From Tables VII and VIII, we can have the observations similar as the ones in Section 5.

Zone	IRLS_bis	L_1	MLR	SVR_Gau	WQSSVR
1	19.97	13.97	21.51	19.56	**8.63**
2	20.96	13.46	22.30	17.57	**7.79**
3	20.96	13.22	22.30	17.60	**8.07**
5	15.82	11.32	17.23	15.07	**10.11**
6	20.68	13.11	22.05	17.43	**7.77**
7	20.96	13.18	22.30	17.57	**7.89**
8	22.58	15.74	23.98	19.62	**8.84**
10	22.59	15.27	23.88	18.84	**10.05**
11	23.90	17.26	25.33	21.25	**8.26**
12	21.26	15.08	22.80	19.65	**11.70**
13	18.62	**13.31**	19.96	16.77	14.24
14	19.62	**15.81**	20.66	19.23	18.42
15	20.31	14.88	21.60	16.52	**13.74**
16	20.61	15.54	22.08	18.86	**12.11**
17	19.88	12.64	21.46	17.56	**7.02**
18	20.37	14.49	21.81	18.21	**9.48**
19	19.64	15.01	21.07	18.71	**11.81**
20	21.18	13.99	22.60	17.95	**9.56**
4	22.54	17.26	23.89	21.36	**16.35**
9	117.00	111.85	117.56	124.94	**110.11**

Table VII: MAPE (%) of zones from GEFCom 2012 under data attacks targeting system blackouts

Zone	IRLS_bis	L_1	MLR	SVR_Gau	WQSSVR
WCMASS	19.17	11.48	20.46	14.38	**8.84**
VT	20.52	12.35	21.82	13.97	**8.73**
SEMASS	19.91	12.46	21.35	13.58	**10.46**
RI	19.80	12.44	21.23	13.81	**11.78**
NH	19.90	12.54	21.18	16.00	**10.61**
NEMASS	20.11	11.99	21.51	14.24	**9.16**
ME	16.25	8.30	17.82	13.14	**5.10**

CT	20.80	12.94	22.24	14.55	**9.38**
Aggregate	17.64	9.41	19.06	13.18	**4.86**

Table VIII: MAPE (%) of zones from NEISO under data attacks targeting system blackouts

6.2 Robustness and Future Research

In these computational experiments, the normally-distributed or uniformly-distributed data integrity attacks have been tested against the load data in three dimensions, i.e., the percentage (k%) of load data being perturbed maliciously, the mean (μ%) and standard deviation (σ%) of the perturbation magnitude (p%), and the type of data attacks (targeting economic losses or system blackouts). We ranked the overall performance of five tested load forecasting models under data integrity attacks from the most accurate one to the least accurate one as: WQSSVR, L_1 regression, SVR_Gau, IRLS_bis and MLR. Notice that, under no data integrity attacks, the overall performance of WQSSVR, L_1 regression, IRLS_bis and MLR models is close with each other while SVR_Gau produces the least accurate load forecasts.

Besides the detailed robustness analysis of IRLS_bis, L_1 regression and MLR models mentioned in (Luo et al., 2019), several observations about the robustness of these tested models can be made: 1) On average, the WQSSVR model is the most robust one among all five models, mainly because it respectively assign small and large weights to attacked and normal points after calculating the ℓ_1–normed residuals of all points, which greatly reduces the impact of attacked points. 2) The L_1 regression and SVR_Gau models are more robust than IRLS_bis and MLR models, largely because the L_1 regression and SVR_Gau models utilize ℓ_1–norm (instead of ℓ_2–norm in the other two models) to measure the fitting errors. 3) L_1 regression outperforms the SVR_Gau model no matter the load data is under data integrity attacks or not, largely because the SVR_Gau model becomes overfitted by utilizing the vanilla model of 289 variables to predict the electric loads.

These types of data integrity attacks in this paper only represent a small portion of potential attacks that a load forecasting system may encounter. Other types of data integrity attacks (such as data integrity attacks on weather data, peak periods, and so forth) need to be further investigated. All existing methods, including the proposed WQSSVR model, may not perform well in face of other cyberattacks such as the data attacks on the temperature and dates. This study paves a way to further research on anti-attack methods for electric load forecasting. Moreover, this paper focuses on robust machine learning models, which can be utilized for load forecasting with or without data attacks. Another approach to addressing data integrity attacks would involve detecting attacks, identifying attacked data, cleansing and recovering attacked data, and finally electric load forecasting. Hence, the anomaly detection and similar methods can be incorporated with the robust WQSSVR model to improve the load forecasting accuracy.

7. Conclusions

In this paper, the data integrity attacks on the historical load data has been addressed from three perspectives, namely, the percentage (k%) of data being perturbed, the magnitude (p%) of the normally-distributed or uniformly-distributed perturbation, and the type of data attacks (targeting economic losses or system blackouts). Under these

types of data integrity attacks, we show that the robust load forecasting models including the L_1 regression, IRLS and SVR with Gaussian kernel may easily fail to provide reliable load forecasts under large-scaled data integrity attacks (i.e., $k \geq 40$), while the proposed WQSSVR model is capable of producing much more accurate and robust load forecasts. Especially when more observations (such as 70% of whole dataset) are attacked with a large mean of perturbation magnitude, the WQSSVR model demonstrates much stronger robustness than other electric load forecasting models. The computational results indicate that the load forecasting MAPE provided by the WQSSVR model remains under 10% even with 70% of the historical load data being maliciously decreased by 30% on average or increased by 50% on average. This study may lead to the investigation of new theory and methodologies for load forecasting under other types of data integrity attacks.

References

Akouemo, H. N., & Povinelli, R. J. (2016). Probabilistic anomaly detection in natural gas time series data. *International Journal of Forecasting*, *32*(3), 948–956.

Arora, S., & Taylor, J. W. (2018). Rule-based autoregressive moving average models for forecasting load on special days: a case study for France. *European Journal of Operational Research*, *266*(1), 259–268.

Bessec, M., & Fouquau, J. (2018). Short-run electricity load forecasting with combinations of stationary wavelet transforms. *European Journal of Operational Research*, *264*(1), 149–164.

Ceperic, E., Ceperic, V., & Baric, A. (2013). A strategy for short-term load forecasting by support vector regression machines. *IEEE Transactions on Power Systems*, *28*, 4356–4364.

Charlton, N., & Singleton, C. (2014). A refined parametric model for short term load forecasting. *International Journal of Forecasting*, *30*(2), 364–368.

Chen, B.-J., Chang, M.-W., & Lin, C.-J. (2004). Load forecasting using support vector machines: a study on EUNITE competition 2001. *IEEE Transactions on Power Systems*, *19*(4), 1821–1830.

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, *20*, 273–297.

Ericsson, G. N. (2010). Cyber security and power system communicationessential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, *25*(3), 1501–1507.

Hahn, H., Meyer-Nieberg, S., & Pickl, S. (2009). Electric load forecasting methods: tools for decision making. *European Journal of Operational Research*, *199*(3), 902–907.

Hippert, H. S., Pedreira, C. E., & Souza, R. C. (2001). Neural networks for short-term load forecasting: a review and evaluation. *IEEE Transactions on Power Systems*, *16*(1), 44–55.

Hong, T. (2010). *Short Term Electric Load Forecasting*. North Carolina State University.

Hong, T., & Fan, S. (2016). Probabilistic electric load forecasting: a tutorial review. *International Journal of Forecasting*, *32*(3), 914–938.

Hong, T., Pinson, P., & Fan, S. (2014). Global energy forecasting competition 2012. *International Journal of Forecasting*, *30*(2), 357–363.

Hong, T., Pinson, P., Fan, S., Zareipour, H., Troccoli, A., & Hyndman, R. J. (2016). Probabilistic energy forecasting: Global Energy Forecasting Competition 2014 and beyond. *International Journal of Forecasting*, *32*(3), 896–913.

Hong, T., & Wang, P. (2014). Fuzzy interaction regression for short term load forecasting. *Fuzzy Optimization and Decision Making*, *13*(1), 91–103.

Hong, T., Wilson, J., & Xie, J. (2014). Long term probabilistic load forecasting and normalization with hourly information. *IEEE Transactions on Smart Grid*, *5*(1), 456–462.

Luo, J., Fang, S.-C., Deng, Z., & Guo, X. (2016). Soft quadratic surface support vector machine for binary classification. *Asia-Pacific Journal of Operational Research*, *33*(6), 1650046.

Luo, J., Hong, T., & Yue, M. (2018). Real-time anomaly detection for very short-term load forecasting. *Journal of Modern Power System and Clean Energy*, 6(2), 235–243.

Luo, J., Hong, T., & Fang, S.-C. (2018). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting*, *34*(1), 89–104.

Luo, J., Hong, T., & Fang, S.-C. (2019). Robust regression for load forecasting. *IEEE Transactions on Smart Grid*, *10*(5), 5397–5404.

Luo, J., Yan, X., & Tian, Y. (2020). Unsupervised quadratic surface support vector machine with application to credit risk assessment. *European Journal of Operational Research*, *280*(3), 1008–1017.

Nazemi, A., Heidenreich, K., & Fabozzi, F. J. (2018). Improving corporate bond recovery rate prediction using multi-factor support vector regressions. *European Journal of Operational Research*, *271*(2), 664–675.

Nystrup, P., Lindström, E., Pinson, P., & Madsen, H. (2020). Temporal hierarchies with autocorrelation for load forecasting. *European Journal of Operational Research*, *280*(3), 876–888.

Perez, E. (2016). *First on CNN: U.S. investigators find proof of cyberattack on Ukraine power grid*.

Rendon-Sanchez, J. F., & Menezes, L. M. d. (2019). Structural combination of seasonal exponential smoothing forecasts applied to load forecasting. *European Journal of Operational Research*, *275*(3), 916–924.

Tian, Y., Sun, M., Deng, Z., Luo, J., & Li, Y. (2017). A new fuzzy set and non-kernel SVM approach for mislabeled binary classification with applications. *IEEE Transactions on Fuzzy Systems*.

Vapnik, V., & Lerner, A. (1963). Pattern recognition using generalized portrait method. *Automation and Remote Control*, *24*, 774–780.

Vapnik, V. N. (1995). *The Nature of Statistical Learning Theory*. Springer-Verlag New York, Inc.

Weron, R. (2006). *Modeling and Forecasting Electricity Loads and Prices: A Statistical Approach*. John Wiley & Sons.

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), 1012–1016.

Yao, X., Crook, J., & Andreeva, G. (2015). Support vector regression for loss given default modelling. *European Journal of Operational Research*, *240*(2), 528–538.

Yue, M., Hong, T., & Wang, J. (2019). Descriptive analytics-based anomaly detection for cybersecure load forecasting. *IEEE Transactions on Smart Grid*, *10*(6), 5964–5974.