SUPPORT VECTOR MACHINES & NEURAL NETWORKS

LECTURE 7 – SUPPORT VECTOR MACHINES PART # IV

A. Bi-classification

History, LSVM, Approximate LSVM, Soft LSVM, Kernel-based linear SVM, nonlinear SVM

B. Multi-classification

OVO, OVA, Twin SVM

C. Prediction

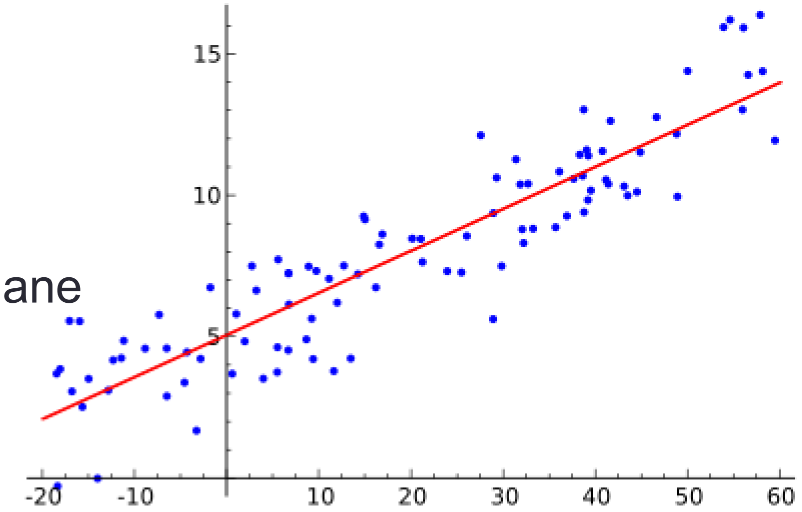
Support Vector Regression (SVR)

Regression

- Linear regression:
  - a model that assumes a linear relationship between the input variables ($\boldsymbol{x}$) and the single output variable (y) such that y can be calculated from a linear combination of the input variables ($\boldsymbol{x}$).

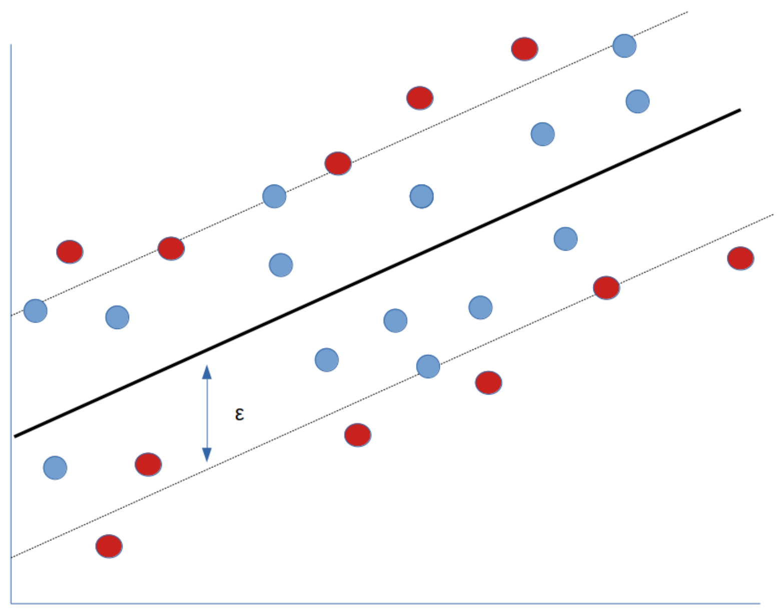
$$y = \boldsymbol{w}^T \boldsymbol{x} + b + \varepsilon$$

Fit the data to a supporting hyperplane with the minimum mean squared error.



Support vector regression (SVR)

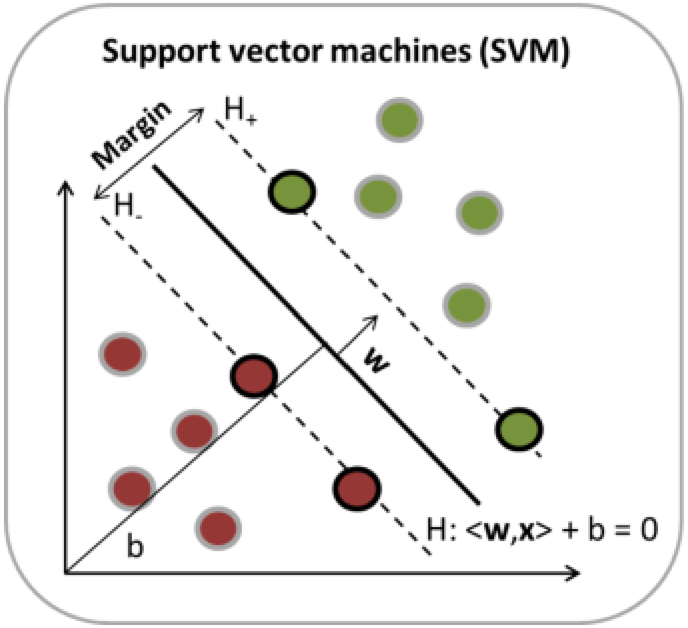
- Basic idea:
  - Find a hyperplane centering around the data by boxing as many data points as possible in a given tube around the hyperplane.

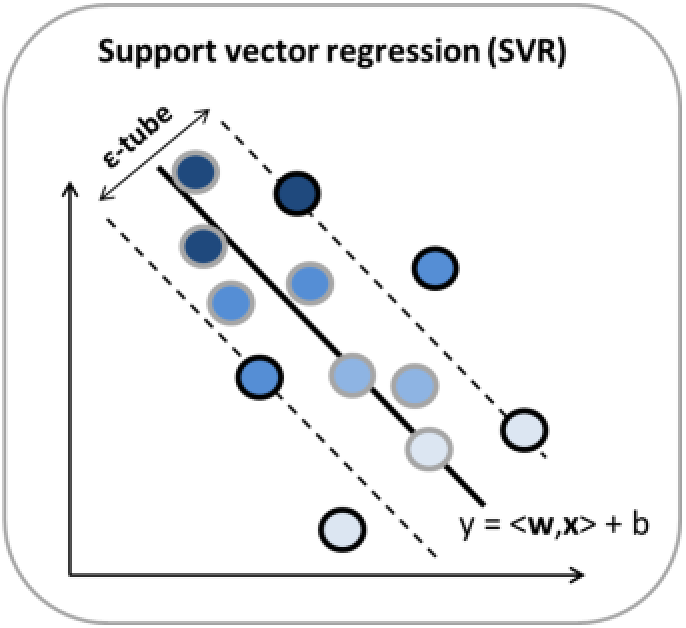


Support vector machines: classification vs. regression

- SVM: data-points in $\mathbb{R}^n$ with class babel y separate data-points apart

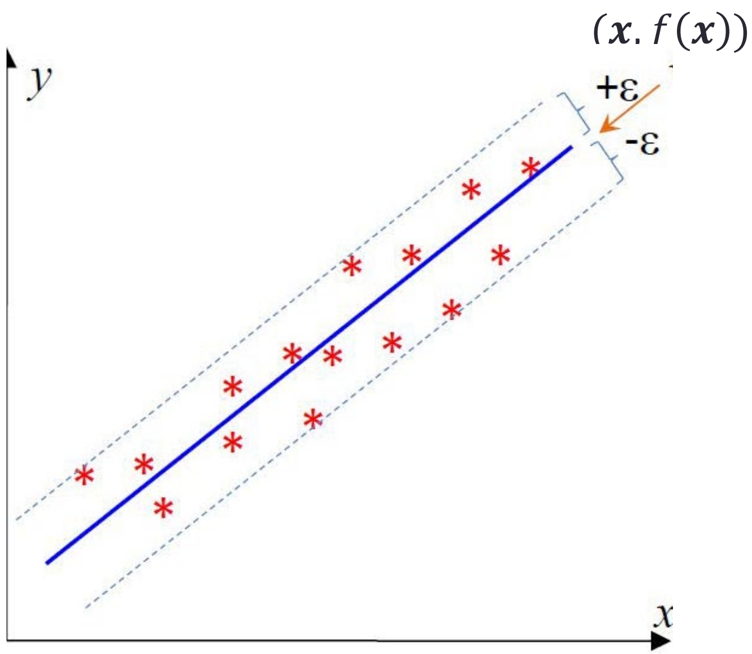
  SVR: data-points in $\mathbb{R}^{n+1}$ with data value y box data-points in a tube





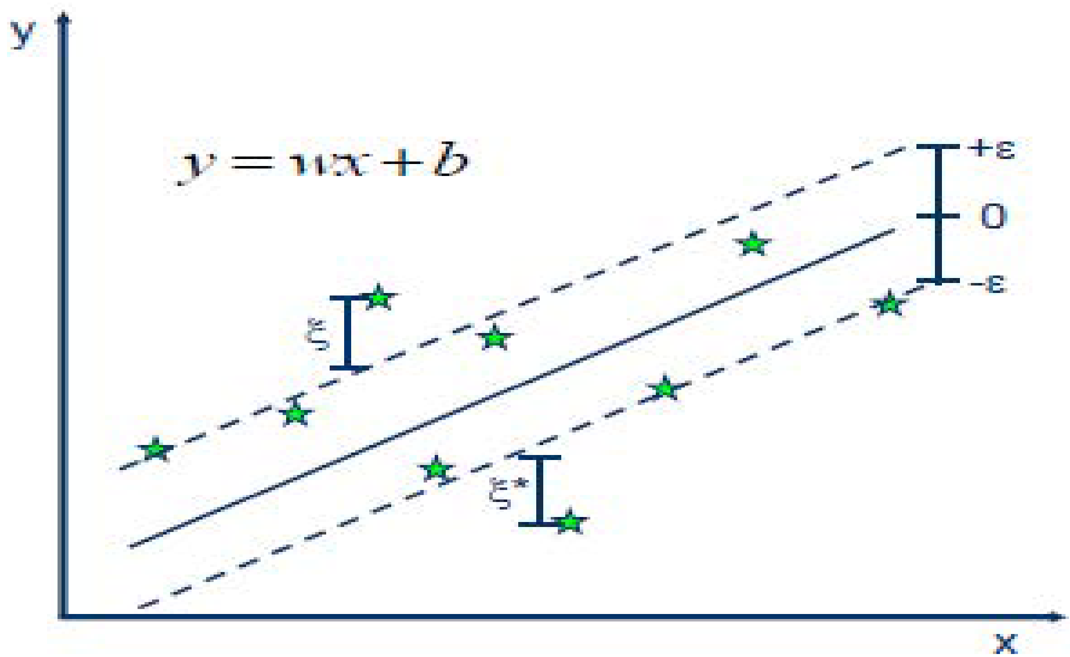
Linear support vector regression

- Problem settings:
  - Dataset $\{ (\boldsymbol{x}^i, y_i) \in \mathbb{R}^n \times \mathbb{R} \mid i = 1,2.,,,,N\}$ of N data points
  - tube tolerance $\varepsilon > 0$
  - Aim: to find affine map $f(\boldsymbol{x}) = \boldsymbol{w}^T\boldsymbol{x} + b$ with wide margin such that $\left|y_i - f\left(\boldsymbol{x}^i\right)\right| < \varepsilon,\ i = 1, \ldots, N$



Observation

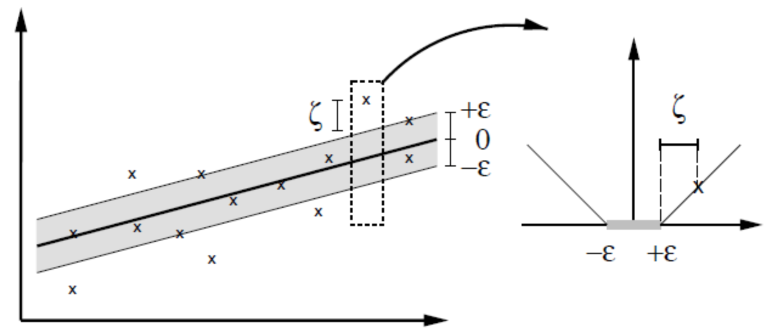
- Question: How big the box tolerance ε should be?
  - When ε (> 0) is too small, we may not be able to box all data-points in the tube.



Linear soft support vector regression

- Primal model: (For a given $C > 0$)

$$
\begin{aligned}
Min \quad & \frac{1}{2}\|\boldsymbol{w}\|_2^2 + C\sum_{i=1}^{N}\xi_i \\
\text{s.t.} \quad & y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b \le \varepsilon + \xi_i,\ i = 1, \dots, N \quad \text{(LSSVR)} \\
& y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b \ge -\varepsilon - \xi_i,\ i = 1, \dots, N \\
& \boldsymbol{w} \in \mathbb{R}^n, b \in \mathbb{R}, \boldsymbol{\xi} \in \mathbb{R}_+^N
\end{aligned}
$$



soft margin with $\varepsilon - insensitive$ loss function

Linear soft SVR - LSSVR

1. (LSSVR) is a convex quadratic program with $n+1$ free variables, N non-negative variables, and $2N$ linear inequality constraints.

2. (LSSVR) is always feasible.

3. Who are supporting vectors?

4. Any dual information?

Dual LSSVR - DLSSVR

- Lagragian

$$L(\boldsymbol{w}, b, \boldsymbol{\xi}, \boldsymbol{\alpha}, \boldsymbol{\alpha}^*, \boldsymbol{\eta}) = \frac{1}{2}\|\boldsymbol{w}\|_2^2 + C\sum_{i=1}^{N}\xi_i$$
$$- \sum_{i=1}^{N}\eta_i\xi_i - \sum_{i=1}^{N}\alpha_i\left(\varepsilon + \xi_i - y_i + \boldsymbol{w}^T\boldsymbol{x}^i + b\right)$$
$$- \sum_{i=1}^{N}\alpha_i^*\left(\varepsilon + \xi_i + y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b\right)$$

- KKT conditions

- Primal & dual feasibility

(i) $\alpha_i, \alpha_i^*, \eta_i \geq 0, i = 1, \dots, N;$

(ii) $\varepsilon + \xi_i - y_i + \boldsymbol{w}^T\boldsymbol{x}^i + b \geq 0; \varepsilon + \xi_i + y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b \geq 0;$

Dual LSSVR - DLSSVR

- Lagragian

$$L(\boldsymbol{w}, b, \boldsymbol{\xi}, \boldsymbol{\alpha}, \boldsymbol{\alpha}^*, \boldsymbol{\eta}) = \frac{1}{2}\|\boldsymbol{w}\|_2^2 + C\sum_{i=1}^{N}\xi_i$$
$$- \sum_{i=1}^{N}\eta_i\xi_i - \sum_{i=1}^{N}\alpha_i\left(\varepsilon + \xi_i - y_i + \boldsymbol{w}^T\boldsymbol{x}^i + b\right)$$
$$- \sum_{i=1}^{N}\alpha_i^*\left(\varepsilon + \xi_i + y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b\right)$$

- KKT conditions

Stationarity

(iii) $\nabla_{\boldsymbol{w}}L = \boldsymbol{w} - \sum_{i=1}^{N}(\alpha_i - \alpha_i^*)\boldsymbol{x}^i = 0;$

(iv) $\nabla_b L = \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0;$

(v) $\nabla_{\xi_i} L = C - \eta_i - (\alpha_i + \alpha_i^*) = 0;$

$\Longrightarrow \eta_i = C - (\alpha_i + \alpha_i^*) \geq 0$ and $0 \leq \alpha_i + \alpha_i^* \leq C$

Dual soft support vector regression -DLSSVR

- Dual model:

$$
\begin{aligned}
Max \quad & -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\alpha_i - \alpha_i^*) < \boldsymbol{x}^i, \boldsymbol{x}^j > (\alpha_j - \alpha_j^*) \\
& -\varepsilon \sum_{i=1}^{N}(\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i (\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0 \qquad \text{(DLSSVR)} \\
& 0 \le \alpha_i + \alpha_i^* \le C, \alpha_i \ge 0, \alpha_i^* \ge 0, i = 1, \dots, N
\end{aligned}
$$

*Depending on $y_i > \boldsymbol{w}^T \boldsymbol{x}^i + b$, or $y_i < \boldsymbol{w}^T \boldsymbol{x}^i + b$, at least one of α_i or α_i^* = 0. So we have

$$
\begin{aligned}
Max \quad & -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\alpha_i - \alpha_i^*) < \boldsymbol{x}^i, \boldsymbol{x}^j > (\alpha_j - \alpha_j^*) \\
& -\varepsilon \sum_{i=1}^{N}(\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i (\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0 \qquad \text{(DLSSVR)} \\
& 0 \le \alpha_i \le C, \; 0 \le \alpha_i^* \le C, i = 1, \dots, N
\end{aligned}
$$

Dual soft support vector regression -DLSSVR

- Observations:

1. (DLSSVR) is a convex quadratic program with $2N$ bounded variables and 1 linear equality constraint.

2. (DLSSVR) is independent of the size of n, which is absolved in the inner product of $(\boldsymbol{x}^i)^T\boldsymbol{x}^j =< \boldsymbol{x}^i, \boldsymbol{x}^j >$.

DLSSVR

- Dual-to-primal conversion:
- KKT (iii) say that

$$\nabla_{\boldsymbol{w}} L = \boldsymbol{w} - \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) \boldsymbol{x}^i = 0.$$

Hence,

$$\boldsymbol{w} = \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) \boldsymbol{x}^i \quad \text{and}$$

$$f(\boldsymbol{x}) = \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) < \boldsymbol{x}^i, \boldsymbol{x} > + b$$

* This is called a “support vector expansion” of $f(\boldsymbol{x})$.

* What is b ?

DLSSVR

- KKT conditions: Complementary slackness:

  (vi) $\alpha_i\left(\varepsilon + \xi_i - y_i + \boldsymbol{w}^T \boldsymbol{x}^i + b\right) = 0$

  (vii) $\alpha_i^*\left(\varepsilon + \xi_i + y_i - \boldsymbol{w}^T \boldsymbol{x}^i - b\right) = 0$

  (viii) $\eta_i \xi_i = (C - (\alpha_i + \alpha_i^*))\ \xi_i = 0$

Observations:

1. Depend on $y_i > \boldsymbol{w}^T \boldsymbol{x}^i + b$, or $y_i < \boldsymbol{w}^T \boldsymbol{x}^i + b$,

   at least one of α_i or $\alpha_i^* = 0$.

2. When data-point $\left(\boldsymbol{x}^i, y_i\right)$ is in the tube

   $$\left|y_i - \left(\boldsymbol{w}^T \boldsymbol{x}^i + b\right)\right| < \varepsilon \Rightarrow \alpha_i = 0 \text{ and } \alpha_i^* = 0.$$

DLSSVR

- KKT conditions: Complementary slackness:

(vi) $\alpha_i\left(\varepsilon + \xi_i - y_i + \boldsymbol{w}^T\boldsymbol{x}^i + b\right) = 0$

(vii) $\alpha_i^*\left(\varepsilon + \xi_i + y_i - \boldsymbol{w}^T\boldsymbol{x}^i - b\right) = 0$

(viii) $\eta_i\xi_i = (C - (\alpha_i + \alpha_i^*))\ \xi_i = 0$

Observations:

3. When data-point $\left(\boldsymbol{x}^i, y_i\right)$ is outside of the tube,

$$\left|y_i - \left(\boldsymbol{w}^T\boldsymbol{x}^i + b\right)\right| > \varepsilon \Rightarrow \xi_i > 0 \Rightarrow \alpha_i = C \text{ or } \alpha_i^* = C.$$

4. $\alpha_i \in (0, C)$ or $\alpha_i^* \in (0, C)$ happens only when $\left(\boldsymbol{x}^i, y_i\right)$ lies on the tube

$$\left|y_i - \left(\boldsymbol{w}^T\boldsymbol{x}^i + b\right)\right| = \varepsilon$$

$\Rightarrow$ either $y_i - (\boldsymbol{w}^T\boldsymbol{x}^i + b) = \varepsilon \Rightarrow b = \varepsilon - y_i + \boldsymbol{w}^T\boldsymbol{x}^i$, when $\alpha_i \in (0, C)$

or $y_i - (\boldsymbol{w}^T\boldsymbol{x}^i + b) = -\varepsilon \Rightarrow b = -\varepsilon - y_i + \boldsymbol{w}^T\boldsymbol{x}^i$, when $\alpha_i^* \in (0, C)$

5. Supporting vectors are indeed sparse!

DLSSVR

- Dual-to-primal conversion:
- KKT (iii) say that

$$\nabla_{\boldsymbol{w}} L = \boldsymbol{w} - \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) \boldsymbol{x}^i = 0.$$

Hence,

$$\boldsymbol{w} = \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) \boldsymbol{x}^i$$

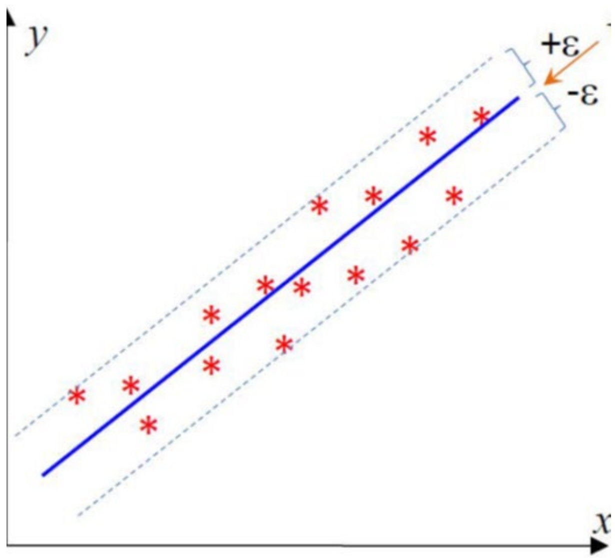
$$b = \begin{pmatrix} \varepsilon - y_i + \boldsymbol{w}^T \boldsymbol{x}^i, & \text{if } \alpha_i \in (0, C) \\ -\varepsilon - y_i + \boldsymbol{w}^T \boldsymbol{x}^i, & \text{if } \alpha_i^* \in (0, C) \end{pmatrix}$$

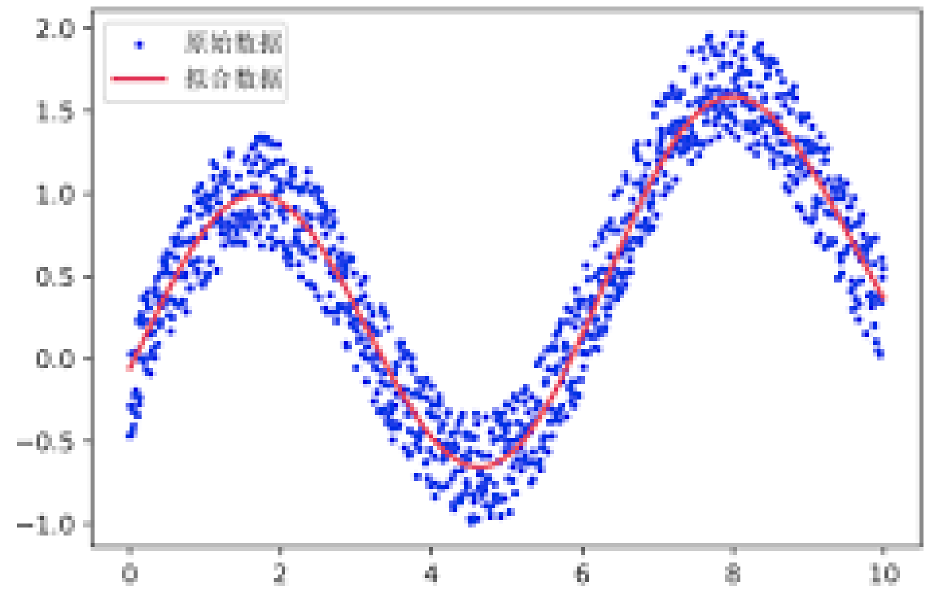
and DLSSVR prediction is

$$f(\boldsymbol{x}) = \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) < \boldsymbol{x}^i, \boldsymbol{x} > + b$$

SVM-based nonlinear regression

- From linear to nonlinear regression





Kernel-based linear soft SVR

- Use a *feature map* $\phi(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R}^l \ (l \geq n)$ to transform the problem to a higher dimensional space for linear separability.

- Primal model: (For a given $C > 0$)

$$Min \quad \frac{1}{2}\|\boldsymbol{w}\|_2^2 + C\sum_{i=1}^{N}\xi_i$$

s.t. $y_i - \boldsymbol{w}^T\phi(\boldsymbol{x}^i) - b \leq \varepsilon + \xi_i, \ i = 1, \dots, N$ (KLSSVR)

$$y_i - \boldsymbol{w}^T\phi(\boldsymbol{x}^i) - b \geq -\varepsilon - \xi_i, \ i = 1, \dots, N$$

$$\boldsymbol{w} \in \mathbb{R}^l, b \in \mathbb{R}, \boldsymbol{\xi} \in \mathbb{R}_+^N$$

* Dimensionality changes from n to l.

Dual kernel-based linear soft support vector regression

- Dual model:

$$
\begin{aligned}
Max \quad & -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\alpha_i - \alpha_i^*) < \phi(\boldsymbol{x}^i), \phi(\boldsymbol{x}^j) > (\alpha_j - \alpha_j^*) \\
& -\varepsilon\sum_{i=1}^{N}(\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i\,(\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0 \qquad \text{(DKLSSVR)} \\
& 0 \le \alpha_i \le C, 0 \le \alpha_i^* \le C, i = 1, \dots, N
\end{aligned}
$$

*(DKLSSVR) is a convex quadratic program with $2N$ bounded variables and 1 linear equality constraint.

*(DKLSSVR) is independent of the size of n, which is absolved in the inner product of $\phi(\boldsymbol{x}^i)^T\phi(\boldsymbol{x}^j) =< \phi(\boldsymbol{x}^i), \phi(\boldsymbol{x}^j) >$.

Kernel-based linear soft SVR

- Knowing an admissible kernel (Mercer's condition)
  $K = (k(x, x'))$ with $k(x, x') = \phi(x)^T \phi(x')$ rather than the feature mapping $\phi(x)$ explicitly, we have a kernel-based LSSVR for nonlinear regression:

$$
\begin{aligned}
Max \quad & -\frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} (\alpha_i - \alpha_i^*) k(\boldsymbol{x}^i, \boldsymbol{x}^j) (\alpha_j - \alpha_j^*) \\
& -\varepsilon \sum_{i=1}^{N} (\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i (\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) = 0 \qquad \text{(DKLSSVR)} \\
& 0 \le \alpha_i \le C, 0 \le \alpha_i^* \le C, i = 1, \dots, N
\end{aligned}
$$

DLSSVR vs. DKLSSVR

- Same structure, same complexity:

$$
\begin{aligned}
Max \quad & -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\alpha_i - \alpha_i^*)k(\boldsymbol{x}^i, \boldsymbol{x}^j)\,(\alpha_j - \alpha_j^*) \\
& \qquad -\varepsilon\sum_{i=1}^{N}(\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i\,(\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0 \qquad \text{(DKLSSVR)} \\
& 0 \le \alpha_i \le C, 0 \le \alpha_i^* \le C, i = 1, \dots, N
\end{aligned}
$$

$$
\begin{aligned}
Max \quad & -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\alpha_i - \alpha_i^*) < \boldsymbol{x}^i, \boldsymbol{x}^j > (\alpha_j - \alpha_j^*) \\
& \qquad -\varepsilon\sum_{i=1}^{N}(\alpha_i + \alpha_i^*) + \sum_{i=1}^{N} y_i\,(\alpha_i - \alpha_i^*) \\
\text{s.t.} \quad & \sum_{i=1}^{N}(\alpha_i - \alpha_i^*) = 0 \qquad \text{(DLSSVR)} \\
& 0 \le \alpha_i \le C, 0 \le \alpha_i^* \le C, i = 1, \dots, N
\end{aligned}
$$

Support vector expansion of KLSSVR

- For KLSSVR

$$\boldsymbol{w} = \sum_{i=1}^{N}(\alpha_i - \alpha_i^*)\phi(\boldsymbol{x}^i)$$

$$b = \begin{cases} \varepsilon - y_i + \boldsymbol{w}^T\boldsymbol{x}^i, \text{ if } \alpha_i \in (0, C) \\ -\varepsilon - y_i + \boldsymbol{w}^T\boldsymbol{x}^i, \text{if } \alpha_i^* \in (0, C) \end{cases}$$

KLSSVR Prediction:

$$f(\boldsymbol{x}) = \sum_{i=1}^{N}(\alpha_i - \alpha_i^*)\phi(\boldsymbol{x}^i)^{\boldsymbol{T}}\phi(\boldsymbol{x}) + b$$

or

$$f(\boldsymbol{x}) = \sum_{i=1}^{N}(\alpha_i - \alpha_i^*)k(\boldsymbol{x}^i, \boldsymbol{x}) + b$$

A case study of electric load forecasting for smart grids

References:

*Co-authors: **Jian Luo, Tao Hong, S-C Fang, Zheming Gao**

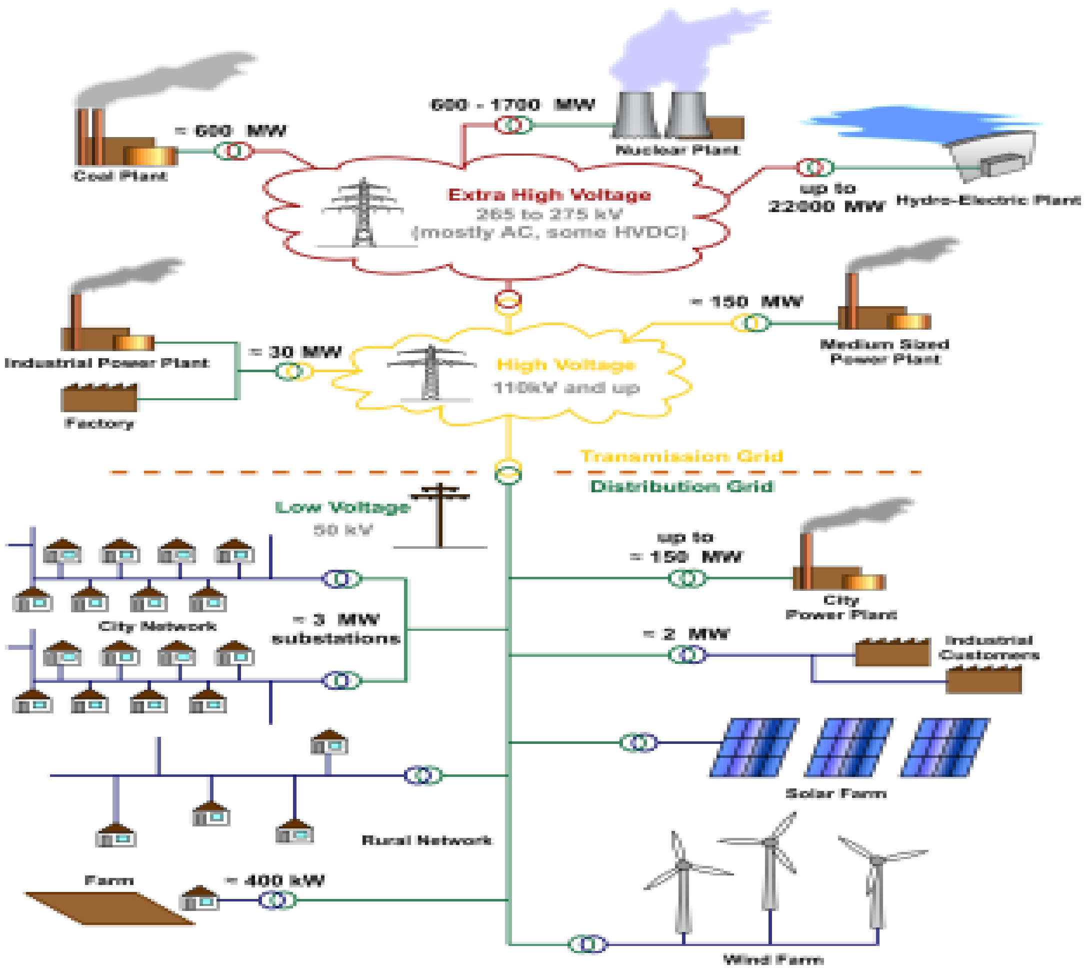
1. Benchmarking robustness of load forecasting models under data integrity attacks. International Journal of Forecasting, 2018.
2. Robust regression for load forecasting. IEEE Transactions on Smart Grid, 2019.
3. A robust support vector regression model for electric load forecasting, International Journal of Forecasting. 2022.

Background knowledge

Load forecasts are widely used across all segments of various industries. Accurate load forecasting is crucial to the excellence of system operations and planning.

- Electric load forecasting is an essential part of business operations in the energy industry. Under-forecasting may cause the undesired "blackouts" while over-forecasting usually leads to an economic losses.
- Various load forecasting methods and techniques have been adopted and tested.
- With the growing concerns about cybersecurity including malicious data manipulations, an emerging topic is to develop robust load forecasting models.
- We report a series of works building robust SVR models to forecast the electricity demand under data integrity attacks.

Electricity Networks



Power Grids

- An **electrical grid** is an interconnected network for electricity delivery from producers to consumers. Electrical grids vary in size and can cover whole countries or continents. It consists of

  - power stations often located near energy and away from heavily populated areas;

  - electrical substations to step voltage up or down;

  - electric power transmission to carry power long distances;

  - electric power distribution to individual customers, where voltage is stepped down again to the required service voltage(s).

Power Grids

https://en.wikipedia.org/wiki/Smart_grid

Evolution:

Characteristics of a traditional system (left) versus the smart grid (right)

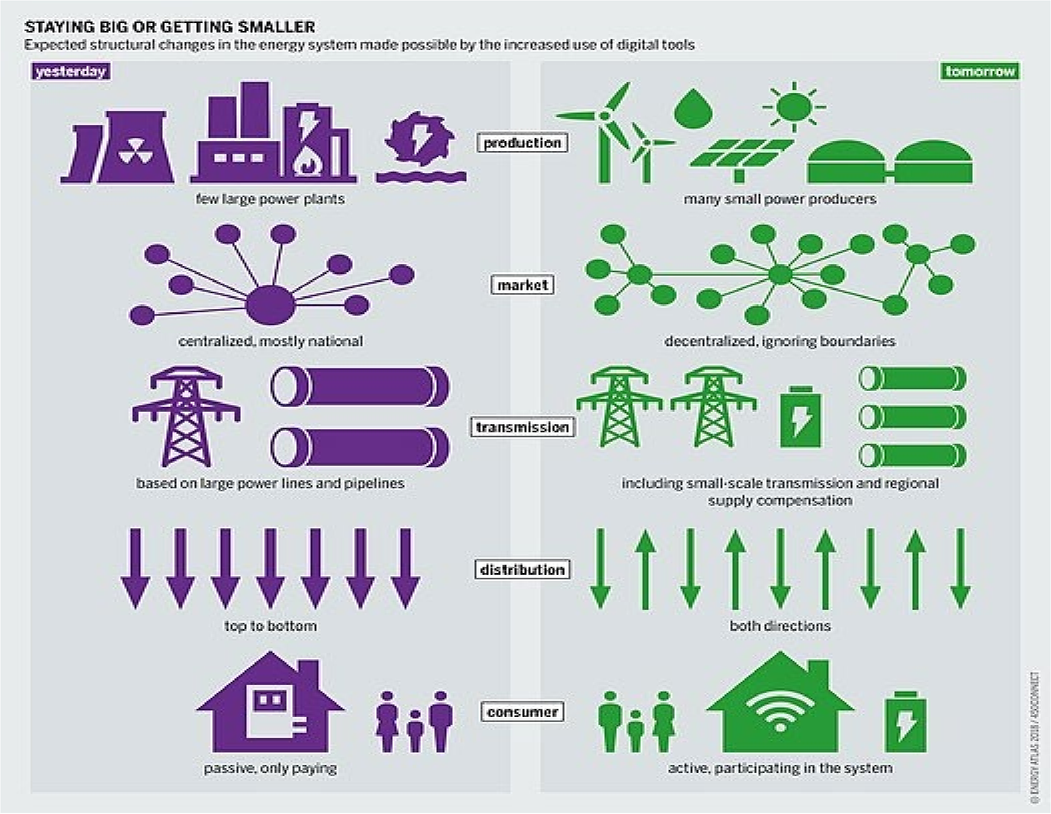
Producers: large to small

Market: central to distributed

Transmission: fixed to regional

Distribution: one-way to two-way

Customers: passive to active



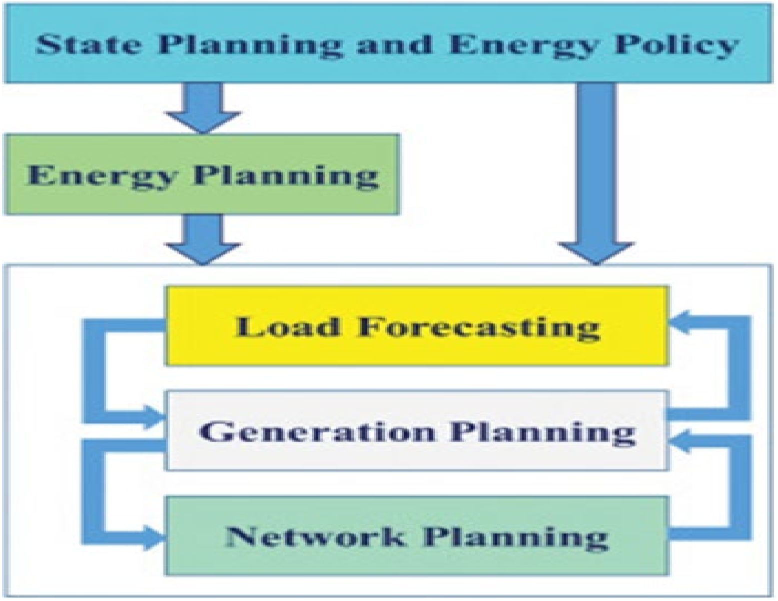
Smart Grids

- The smart grid would be an enhancement of the 20th century electrical grid, using two-way communications and distributed "intelligent devices". Two-way flows of electricity and information could improve the delivery network.

- Research and practice are mainly focused on three systems of a smart grid – the infrastructure system, the management system, and the protection system.

Electric Load Forecast

The electric load forecasting (ELF) is indispensable procedure for the planning of power system industry, which plays an essential role in the scheduling of electricity and the management of the power system (PSM).



Electric Load Forecasting

- Forecasting horizons:
  - Long-term, intermediate-term, short-term
  - Yearly, monthly, weekly, hourly, per minute, per second

- Factors: time, weather, social behavior, etc.
  and compounding factors

Electric load forecasting factors

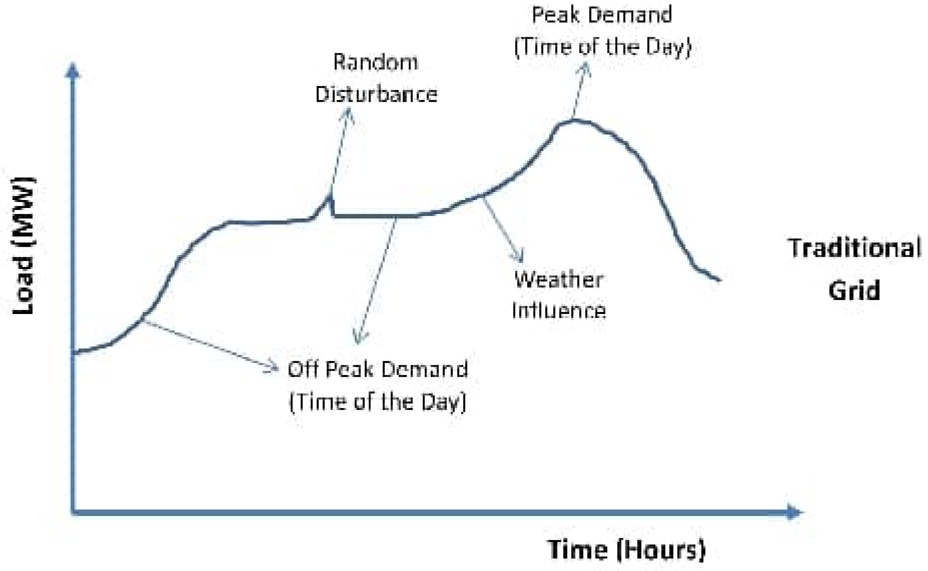


Image: energycentral.com

- Vanilla model has a total of 289 variables, which works effectively for electric load forecasting, (Hong & Fan, 2016; Hong, Pinson, & Fan, 2014; Hong, Wilson, & Xie, 2014).

Electric load forecasting methods

- Available models:
  - using statistical or AI techniques on historical data of load and its affecting factors:

    (1) AI methods (ANN, Fuzzy Logic)

    (2) Parametric mathematical models
    - regression methods
    - time-series prediction methods
    - gray dynamic methods

Commonly used electric load forecasting models

- Multiple linear regression (MLR) (Papalexopoulos et al., 1990)
- Artificial neural networks (ANN) (Hippert et al., 2001)
- Support vector regression (SVR) (Chen et al., 2004)
- Fuzzy interaction regression (FIR) (Hong & Wang, 2014)

- Expected performance: $about\ 95\%\ accuracy$ for industrial practice

Multiple linear regression (MLR)

- Basic MLR Model:

Data $\{(\boldsymbol{x}^i, y^i)\}$, $\boldsymbol{x}^i \in \mathbb{R}^{289}$, $y^i \in \mathbb{R}^+, n =$ # data points

$$min_{\beta \in \mathbb{R}^{289}, \beta_0 \in \mathbb{R}} \sum_{i=1}^{n} \left(y^i - \left(\beta^T x^i + \beta_0\right)\right)^2$$

Support vector regression (SVR)

- Basic SVR Model: ($C, \delta \geq 0$ are given)

$$\min_{\beta \in \mathbb{R}^{289}, \beta_0 \in \mathbb{R}, \varepsilon \in \mathbb{R}^n} \frac{1}{2}\beta^T \beta + C \sum_{i=1}^{n} \varepsilon_i^2$$

$$\text{s.t.} \quad \delta + \varepsilon_i \geq y^i - \left(\beta^T x^i + \beta_0\right) \geq -\delta - \varepsilon_i, \; \varepsilon_i \geq 0.$$
$$i = 1, \ldots, n,$$

Artificial neural network (ANN)

- Basic ANN Model:

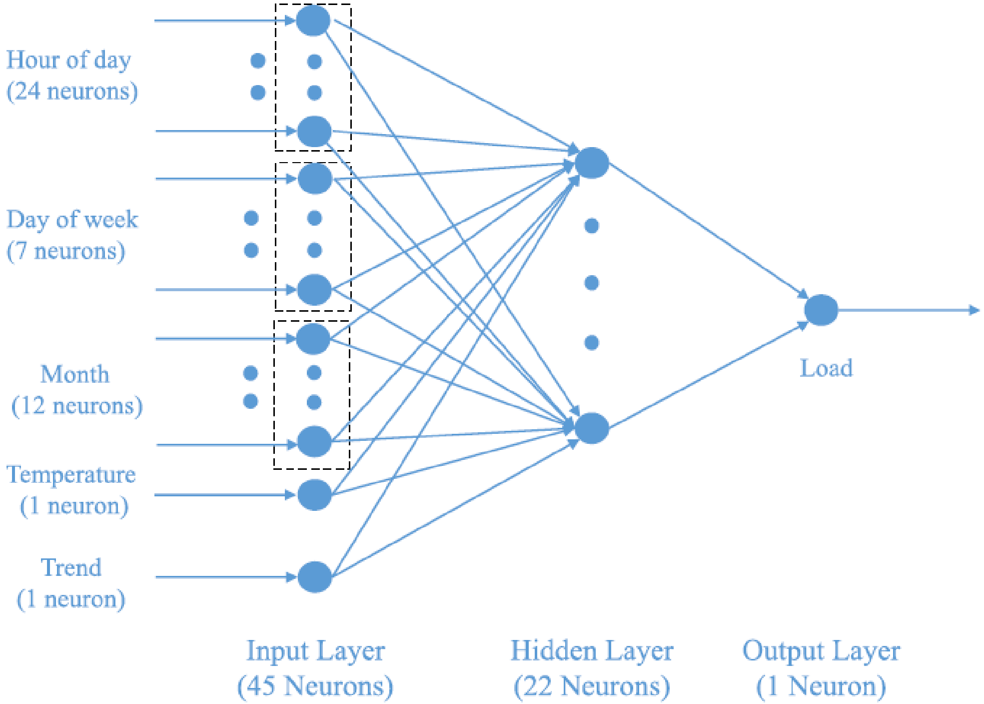


Fig. 1. The architecture of the ANN model.

Fuzzy interaction regression (FIR)

- Basic FIR Model: (h is a given parameter)

$$\min_{\beta\in\mathbb{R}^{289},\beta_0\in\mathbb{R},c\in\mathbb{R}^{289},c_0\in\mathbb{R}} \sum_{i=1}^{n} \left(c^T \left|x^i\right| + c_0\right)$$

$$\begin{aligned}\text{s.t. } |1-h|\left(c^T\left|x^i\right|+c_0\right) &\geq y^i - \left(\beta^T x^i + \beta_0\right)\\ &\geq -|1-h|\left(c^T\left|x^i\right|+c_0\right)\end{aligned}$$

$$i = 1, \ldots, n, \quad c_j \geq 0, \quad j = 0, 1, \ldots, 289,$$

Cyber attacks

- A cyberattack is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices. Wikipedia

Cyber Attacks

- Cybersecurity currently presents a serious challenge to the resilience of power grids (Ericsson, 2010).
- The cyber attack on Ukraine's power grid (Perez, 2016), for instance, was a real threat to people's daily lives. Several other cyber attacks on power systems were discussed in (Hong & Hofmann, 2021).
- Data integrity attack is one form of cyber attacks. Hackers may access the supposedly protected data sets and inject misleading information to the historical load in a way such that the manipulations may not be easily detected by conventional operational practices.

Load Forecasting under data integrity attacks

- Important issues:
  - Deadly operational cost:
    Under-capacity - Brownout, Blackout
  - Unnecessary economic loss:
    Over-capacity
- Challenge: Robustness

- Question: *How good are the commonly used electric load forecasting models?*

Benchmarking Dataset

- GEFCom2012 (Hong et al., 2014): a widely used Electric Load Forecasting dataset.
  - Includes 4.5 years of hourly load and temperature information for a US utility with 21 zones ($Z_1, \ldots, Z_{21}$).
  - The load in Z_{21} is the sum of the other 20 zones.
  - Data of 3 full calendar years (2005–2007) are taken for an empirical study.
  - Data of (2005 and 2006) are used as the training data.
  - Data of (2007) is used as the test data for benchmarking.

Computational Experiments

- In each experiment:
  - $k\%$ of data points are randomly selected
  - Load of each selected point is injected a noise (increase or decrease) by $p\%$.
  - p is specified by a
    - -- number,
    - -- normal distribution $N(\mu, \sigma^2)$, or
    - -- uniform distribution $U(a, b) = (\mu - \sigma, \mu + \sigma)$
- Major metric:

  $MAPE$ = mean absolute % error $= \frac{100\%}{n} \sum_{t=1}^{n} \left| \frac{A_t - F_t}{A_t} \right|$

  $RMSE = \text{root mean square error}$

Implementation

- Computational platform:

MATLAB modules used in the implementation.

Model	MATLAB module
MLR	robustfit
ANN	Neural network toolbox
SVR	quadprog
FIR	linprog

Benchmarking w/o data integrity attack

- Baseline: $MLR \geq SVR \gg FIR \geq ANN$

MAPEs (%) of hourly load forecasts in 2007 without data integrity attacks.

	Zone	MLR	ANN	SVR	FIR
Aggregated zone	21	**5.22**	5.69	5.23	5.54
Regular zone	1	**7.01**	8.88	7.02	8.14
	2	5.62	5.99	**5.61**	6.36
	3	5.62	6.19	**5.61**	6.36
	5	**9.88**	10.80	9.93	13.11
	6	**5.55**	6.34	**5.55**	6.20
	7	5.62	6.15	**5.61**	6.36
	8	7.50	8.57	**7.47**	8.40
	10	**6.70**	7.39	6.75	7.80
	11	**7.70**	9.46	7.75	8.05
	12	**6.78**	8.45	6.88	7.77
	13	**7.39**	9.46	7.40	8.35
	14	**9.38**	11.08	9.48	10.76
	15	**7.44**	9.36	7.47	8.27
	16	**8.12**	9.74	8.24	9.65
	17	**5.26**	6.41	5.27	5.83
	18	**6.72**	7.79	6.77	7.27
	19	**7.90**	10.28	7.96	8.78
	20	**5.74**	6.67	5.75	6.45
Special zone	4	16.08	17.72	**16.06**	19.72
	9	139.16	128.82	140.04	**110.66**

Benchmarking with $N(\mu, \sigma^2)$ attack

- Average MAPEs (%) under normally-distributed data attacks with varying amounts of injected data.

	μ \ k	$\sigma = 50$					$\sigma = 100$				
		10	20	30	40	50	10	20	30	40	50
MLR	0	5.49	5.76	6.01	6.24	6.44	6.23	7.09	7.90	8.59	9.18
ANN		6.62	7.52	8.13	8.96	9.32	8.88	10.82	12.67	13.79	14.62
SVR		**5.48**	**5.73**	**5.97**	**6.18**	**6.36**	**6.16**	**6.97**	**7.72**	**8.37**	**8.91**
FIR		21.25	21.02	19.74	19.37	18.53	41.63	40.58	38.24	37.77	36.24
MLR	10	5.36	5.63	5.99	6.41	6.96	6.12	7.00	7.92	8.76	9.67
ANN		6.36	7.48	8.31	8.84	10.02	8.90	11.00	12.55	13.96	14.89
SVR		**5.34**	**5.60**	**5.94**	**6.34**	**6.88**	**6.05**	**6.87**	**7.73**	**8.52**	**9.40**
FIR		22.22	21.94	20.40	20.77	20.06	42.37	41.25	38.20	38.60	37.15
MLR	20	5.36	5.95	6.87	8.03	9.60	6.12	7.27	8.62	10.00	11.70
ANN		6.59	7.82	9.08	10.63	12.18	8.66	11.16	12.99	14.77	16.65
SVR		**5.34**	**5.92**	**6.82**	**7.96**	**9.54**	**6.04**	**7.14**	**8.44**	**9.77**	**11.47**
FIR		25.76	25.70	24.07	25.16	24.65	44.46	43.27	39.75	41.16	39.81
MLR	30	5.49	6.69	8.49	10.70	13.54	6.23	7.88	9.93	12.14	14.94
ANN		6.83	8.38	10.42	12.66	15.18	8.99	11.75	13.91	16.41	18.46
SVR		**5.47**	**6.65**	**8.43**	**10.65**	**13.50**	**6.15**	**7.75**	**9.76**	**11.95**	**14.77**
FIR		30.98	31.70	30.25	31.69	31.78	47.97	46.67	43.25	45.24	43.77
MLR	40	5.75	7.78	10.62	13.99	18.05	6.46	8.80	11.73	14.96	18.96
ANN		7.31	9.68	12.15	15.23	19.25	9.33	12.36	15.25	18.28	21.36
SVR		**5.72**	**7.74**	**10.57**	**13.94**	**18.03**	**6.37**	**8.67**	**11.58**	**14.80**	**18.85**
FIR		37.91	38.89	37.99	39.94	39.67	52.27	51.11	48.32	50.65	49.34

Benchmark with $U(\mu-\sigma, \mu+\sigma)$ attack

- T

Forecast error in MAPEs (%) under uniformly-distributed data attacks.

	μ \ k	10	20	30	40	50
MLR	0	5.45	5.67	5.93	6.19	6.43
ANN		6.64	7.37	8.16	9.23	9.77
SVR		**5.45**	**5.64**	**5.88**	**6.11**	**6.34**
FIR		11.25	12.03	10.09	10.16	10.98
MLR	10	5.34	5.54	5.86	6.32	6.82
ANN		6.63	7.59	8.30	9.05	10.44
SVR		**5.34**	**5.51**	**5.78**	**6.23**	**6.71**
FIR		13.85	14.09	13.10	13.10	13.40
MLR	20	5.37	5.88	6.70	7.92	9.37
ANN		6.73	7.79	9.00	10.34	12.37
SVR		**5.36**	**5.83**	**6.61**	**7.84**	**9.28**
FIR		19.61	20.46	20.61	21.26	21.91
MLR	30	5.53	6.64	8.31	10.61	13.27
ANN		6.87	8.66	10.59	12.86	15.16
SVR		**5.49**	**6.59**	**8.23**	**10.55**	**13.22**
FIR		28.73	29.41	29.92	30.76	31.56
MLR	40	5.81	7.75	10.45	13.90	17.77
ANN		7.29	9.79	12.26	15.44	18.90
SVR		**5.79**	**7.70**	**10.39**	**13.86**	**17.69**
FIR		36.69	39.02	39.75	40.60	41.51

Lessons learned

- 1. Without data integrity attack:

  $$MLR \geq SVR \gg FIR > ANN$$

  With data integrity attack

  $$SVR \geq MLR \gg ANN > FIR$$

- 2. All 4 representative load forecasting models are working well, but they fail to generate robust forecasts $(MAPE > 10\%)$ under severe data integrity attack $(k\% > 30\%)$.

- 3. There is a need for more robust models for electric load forecasting.

Enhancing robustness

- Two basic ideas for investigation:

  (1) weighting the l_2-norm of all residuals;

  (2) changing the penalty function of errors from

  l_2-norm to l_1-norm.

- Three robust regression models for load forecasting:

  - two are based on iteratively re-weighted least squares (IRLS);

  - one is l_1-norm based penalty.

Robust electric load foresting models

- $IRLS_{bis} and\ IRLS_{\log}$

$$\min_{w \in R^{289}, b \in R} \sum_{i=1}^{n} r_i^2 (y^i - w^T x^i - b)^2, \tag{2}$$

where the weights $\{r_i, i = 1, \ldots, n\}$ are determined by utilizing the regression residuals from last iteration. Generally speaking, to stay robust, an observation with smaller (and larger) residual is assigned with a smaller (and larger) weight.

- *piecewise "bi-square"* weight function

$$r_i = \begin{cases} 0, & \text{if} |u_i| \geq 1, \\ (1 - u_i^2)^2, & \text{if} |u_i| < 1, \end{cases}$$

- *continuous "logistic"* weight function

$$r_i = \tan(u_i)/u_i, \qquad u_i = res_i/(tune \cdot s \cdot \sqrt{1-h})$$

Robust electric load forecasting models

- l_1-regression model (L_1)

$$\min_{w \in R^{289}, b \in R, \varepsilon \in R^n} \sum_{i=1}^{n} \varepsilon_i$$

$$s.t. \varepsilon_i \geq y^i - (w^T x^i + b) \geq -\varepsilon_i, \varepsilon_i \geq 0, i = 1, 2, \ldots, n$$

Implementations

- Six models for benchmarking

MATLAB MODULES USED IN THE IMPLEMENTATION

Model	MATLAB Module
IRLS_bis	robustfit with defaulted "wfun" input
IRLS_log	robustfit with "wfun" input "logistic"
L_1	linprog
MLR	robustfit with "wfun" input "ols"
ANN	Neural Network Toolbox
SVR	quadprog

Benchmarking w/o data integrity attack

MAPE (%) OF HOURLY LOAD FORECAST IN 2007

Zone	IRLS_bis	IRLS_log	L_1	MLR	ANN	SVR
21	5.30	5.27	5.33	**5.22**	5.69	5.23
1	7.08	7.03	7.08	**7.01**	8.88	7.02
2	5.56	5.56	**5.52**	5.62	5.99	5.61
3	5.56	5.56	**5.52**	5.62	6.19	5.61
5	9.69	9.67	**9.64**	9.88	10.80	9.93
6	5.56	5.54	**5.53**	5.55	6.34	5.55
7	5.56	5.56	**5.52**	5.62	6.15	5.61
8	7.59	7.56	7.59	7.50	8.57	**7.47**
10	**6.70**	6.73	6.79	**6.70**	7.39	6.75
11	7.97	7.94	8.20	**7.70**	9.46	7.75
12	6.95	6.91	6.99	**6.78**	8.45	6.88
13	7.48	7.46	7.44	**7.39**	9.46	7.40
14	9.41	9.39	9.40	**9.38**	11.08	9.48
15	**7.38**	7.39	7.40	7.44	9.36	7.47
16	8.13	**8.11**	**8.11**	8.12	9.74	8.24
17	5.31	5.29	5.30	**5.26**	6.41	5.27
18	6.77	6.74	6.73	**6.72**	7.79	6.77
19	7.88	7.88	**7.87**	7.90	10.28	7.96
20	5.73	5.71	**5.68**	5.74	6.67	5.75
Avg	7.017	7.002	7.017	**6.996**	8.278	7.029
4	**15.83**	15.90	15.89	16.08	17.72	16.06
9	164.05	152.10	153.48	139.16	**128.82**	140.04

Benchmarking with data integrity attack

- Similar results for attack targeting economic loss

Forecast Error in MAPE (%) / RMSE (10^5) Under Various Levels of Data Integrity Attacks Targeting System Blackouts

	k \ p	10	20	30	40	50	60	70	80	90
IRLS_bis	10	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		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
IRLS_bis	20	5.84/1.34	6.03/1.36	**5.42/1.23**	**5.28/1.21**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**
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		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
IRLS_bis	30	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		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	11.03/2.54	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		6.43/1.46	8.29/1.82	10.70/2.24	13.33/2.70	16.08/3.16	19.03/3.67	21.70/4.14	24.54/4.62	27.38/5.12
IRLS_bis	40	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**	**8.15/2.01**	**8.30/2.11**	**8.45/2.28**	**8.59/2.36**
MLR		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

Benchmarking with data integrity attack

FORECAST ERROR IN MAPE (%) / RMSE (10^5) UNDER VARIOUS LEVELS OF DATA INTEGRITY ATTACKS TARGETING SYSTEM BLACKOUTS

	k \ p	10	20	30	40	50	60	70	80	90
IRLS_bis	10	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		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
IRLS_bis	20	5.84/1.34	6.03/1.36	**5.42/1.23**	**5.28/1.21**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**	**5.27/1.20**
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		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
IRLS_bis	30	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		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	11.03/2.54	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		6.43/1.46	8.29/1.82	10.70/2.24	13.33/2.70	16.08/3.16	19.03/3.67	21.70/4.14	24.54/4.62	27.38/5.12
IRLS_bis	40	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**	**8.15/2.01**	**8.30/2.11**	**8.45/2.28**	**8.59/2.36**
MLR		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

Lessons learned

- Both idea of "weighted loss" and "l_1 norm" work.

RANKINGS OF THE OVERALL ACCURACY OF THE FORECASTING MODELS

Model	Without data integrity attacks	With data integrity attacks
IRLS_bis	3	2
IRLS_log	4	3
L_1	2	1
MLR	1	5
ANN	6	6
SVR	5	4

- Question: *How about developing a robust SVR ?*

Robust support vector regression

- Linear SVR
- Linear SVR with Kernel
- Quadratic surface SVR (QSSVR)
- Robust weighted QSSVR

Robust SVR for electric load forecating

- Linear SVR (Chen *et al*. 2004)

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

$$\begin{aligned} s.t.\quad & \delta + \xi_i \geq y^i - (w^T x^i + c), i = 1, 2, \ldots, n, \\ & y^i - (w^T x^i + c) \geq -\delta - \xi_i, i = 1, 2, \ldots, n, \\ & \xi_i \geq 0, i = 1, 2, \ldots, n. \end{aligned}$$

- SVR with kernel

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

$$\begin{aligned} s.t.\quad & \delta + \xi_i \geq y^i - (w^T \phi(x^i) + c), i = 1, 2, \ldots, n, \\ & y^i - (w^T \phi(x^i) + c) \geq -\delta - \xi_i, i = 1, 2, \ldots, n, \\ & \xi_i \geq 0, i = 1, 2, \ldots, n. \end{aligned}$$

Robust QSSVR for electric load forecasting

- Quadratic surface SVR model (Luo et al., 2021)

$$\begin{aligned}
\min_{W,b,c,\xi} \quad & \sum_{i=1}^{n} \|Wx^i + b\|_2^2 + C_p \sum_{i=1}^{n} \xi_i \\
s.t. \quad & \delta + \xi_i \geq y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c), i = 1, 2, \ldots, n, \\
& y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c) \geq -\delta - \xi_i, i = 1, 2, \ldots, n, \\
& \xi_i \geq 0, i = 1, 2, \ldots, n.
\end{aligned}$$

- Theoretical development: dual QSSVR, optimality analysis
- Solution method development

Robust SVR for electric load forecasting

- Weighted quadratic surface SVR (WQSSVR) (Luo et al., 2021)

$$\begin{aligned}
\min_{W,b,c,\xi}\quad & \sum_{i=1}^{n} \beta_i \|Wx^i + b\|_2^2 + C_p \sum_{i=1}^{n} \beta_i \xi_i \\
s.t.\quad & \delta + \xi_i \geq y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c), i = 1, 2, \ldots, n, \\
& y^i - (\frac{1}{2}(x^i)^T W x^i + b^T x^i + c) \geq -\delta - \xi_i, i = 1, 2, \ldots, n, \\
& \xi_i \geq 0, i = 1, 2, \ldots, n.
\end{aligned}$$

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

where $u_i = |\gamma_i - \overline{\gamma}| / MED$, $\gamma_i \triangleq |y^i - \hat{y}^i|$ ($\hat{y}^i = w^T x^i + c$, where w and c are generated by using the training points

Benchmarking w/o data integrity attack

- WQSSVR is picking up!

MAPE (%) of hourly load forecast without data attacks.

Zone	IRLS_bis	L_1	MLR	SVR_Gau	WQSSVR
21	5.30	5.33	**5.22**	6.31	5.38
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

Benchmarking with attacks targeting economic losses

- $N(\mu, \sigma^2)$

Averages of MAPE (%) and SE of MAPE averages (%) for under normally distributed data attacks targeting economic losses.

	k	$p\%$ $N(0.25, 0.5^2)$	$N(0.5, 0.5^2)$	$N(0.75, 0.5^2)$
IRLS_bis	40	5.23/0.01	5.23/0.01	**5.24/0.01**
L_1		**5.16/0.02**	**5.19/0.02**	5.50/0.03
MLR		9.23/0.18	17.41/0.27	27.50/0.40
SVR_Gau		6.39/0.05	6.91/0.06	8.45/0.13
WQSSVR		5.28/0.05	5.27/0.05	5.31/0.05
IRLS_bis	50	5.46/0.01	10.44/0.29	28.22/0.46
L_1		**5.24/0.01**	5.97/0.09	9.63/0.18
MLR		11.03/0.25	22.66/0.40	35.01/0.47
SVR_Gau		6.84/0.06	8.87/0.14	14.27/0.22
WQSSVR		5.34/0.07	**5.60/0.09**	**5.84/0.09**
IRLS_bis	60	7.90/0.11	21.93/0.45	38.60/0.42
L_1		**5.47/0.03**	10.35/0.12	25.27/0.34
MLR		13.29/0.39	27.36/0.43	42.27/0.41
SVR_Gau		7.66/0.10	12.93/0.27	25.13/0.39
WQSSVR		5.64/0.08	**5.81/0.06**	**11.97/0.31**
IRLS_bis	70	11.84/0.21	29.19/0.35	46.26/0.39
L_1		6.80/0.14	20.56/0.39	41.61/0.91
MLR		15.22/0.42	32.52/0.38	48.59/0.36
SVR_Gau		9.12/0.07	19.77/0.30	38.45/0.29
WQSSVR		**5.86/0.06**	**9.58/0.35**	**26.00/0.61**
IRLS_bis	80	15.96/0.36	35.27/0.46	56.23/0.35
L_1		10.67/0.31	31.18/0.75	57.01/0.28
MLR		17.89/0.42	37.20/0.45	57.55/0.31
SVR_Gau		11.87/0.14	28.73/0.29	51.86/0.19
WQSSVR		**7.96/0.26**	**19.28/0.52**	**47.90/0.19**
IRLS_bis	90	19.02/0.43	40.97/0.49	63.60/0.40
L_1		16.10/0.62	39.62/0.86	64.38/0.84
MLR		19.76/0.42	41.98/0.48	64.19/0.41
SVR_Gau		15.84/0.25	37.25/0.34	**60.69/0.26**
WQSSVR		**12.39/0.95**	**32.14/2.28**	62.97/2.47

An example of attacks targeting economic losses

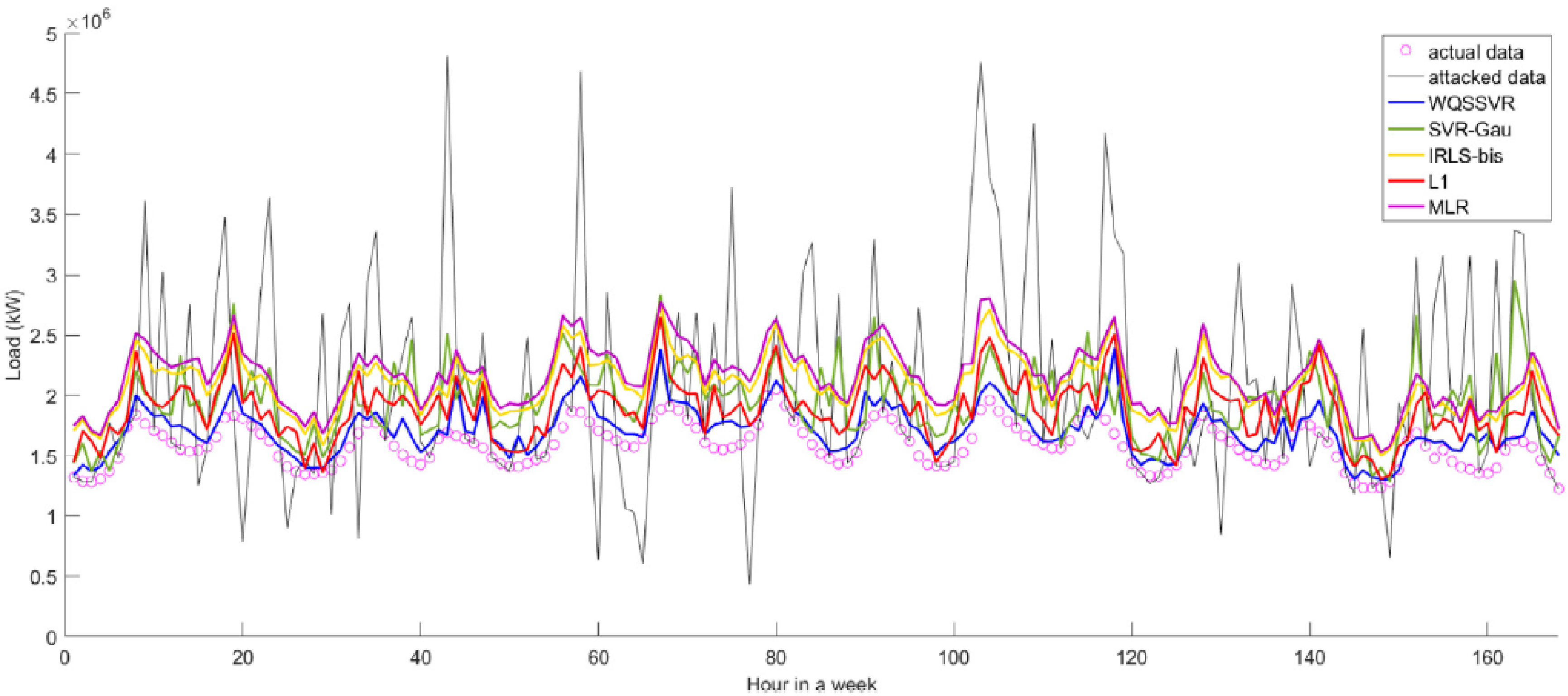


Fig. 1. Fitted (2005/1/7–2005/1/13) hourly load profile under normally distributed data attacks targeting economic losses.

Benchmarking with attacks targeting system blackouts

- $k\% = 70\%$
- $U(-0.8,0.2)$

MAPE (%) of zones from GEFCom 2012 under data attacks targeting system blackouts.

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**

Lessons learned

- In our experiments, robust load forecasting models (L_1, IRLS, and SVR with Gaussian kernel) may fail to provide reliable load forecasts under large-scale data integrity attacks (for $k\% \geq 40\%$).
- WQSSVR model is capable of producing more accurate and robust load forecasts.
- When more data points (e.g., $k\% \geq 70\%$) of whole data set) are attacked with a large mean of perturbation magnitude, the WQSSVR model demonstrates much stronger robustness than other.
- Better robust electric load forecasting is needed for facing various types of data integrity attacks.