Exploring Physical-Based Constraints in Short-Term Load Forecasting: A Defense Mechanism Against Cyberattack

Mojtaba Dezvarei[1], Kevin Tomsoic[1], Jinyuan Stella Sun[1] , Seddik M. Djouadi[1]
[1] The University of Tennessee, Knoxville

INTRODUTION

- Short Term Load Forecasting (STLF) is to forecast the load for a short time horizon concerned with scheduling purposes, from one hour to one week ahead.
- Among input variables, temperature plays key role for STLF as many loads are sensitive to temperatures, such as, heating and cooling.
- As temperature is obtained by third party services/AP, it is vulnerable to data disruptions and cyberattack.
  - More challenging as the attacker may benefit from AI/ML methods to skip detection scheme.

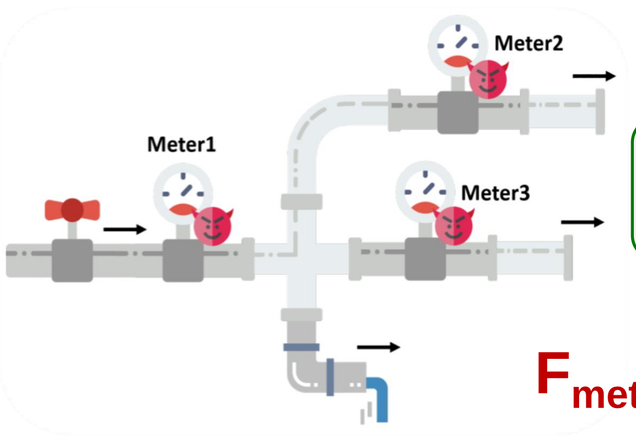
$y_t = f(\bar{X}_t)$

f: *forecasting function (MLR, ANN, SVM, etc.)*
y_t: load at time t
$\bar{X}_t$: input (independent variables) at time t

- Weather (**temperature**, humidity, …)
- Calendar day (time of day, day of week, …)
- Social events (holidays, sport event, ...)

MOTIVATION

- Physical-based constraints can provide obstacles that makes attacks more difficult.
- Attacker needs to meet the constraints imposed by the physical/topology of system and evade any built-in detection mechanisms in the system.



Water flow measurement

linear equality/ inequality constraints

$F_{meter1} > F_{meter2} + F_{meter3}$

PROBLEM STATEMENT

- Considering the temperature as a targeted variable, attacker seeks to solve following for being undetectable:

$$\min_{\tilde{X}} \quad H_\theta(\tilde{X})$$
$$s.t. \quad \left\| X - \tilde{X} \right\|_p \leq \epsilon \quad \Rightarrow \text{Detection scheme constraints}$$
$$+$$
$$g(\tilde{x}) \leq 0 \quad \Rightarrow \text{Physical-based constraint}$$

- Adding $\mathbf{g}(\boldsymbol{x})$ obtained by physical/topological information of STLF increases complexity of the problem that attacker needs to solve for a successful malicious action.
  - H is attacker simulated forecasting model parameterized by θ.
  - $\tilde{X}, X$ are the injected and actual temperature data.
  - ϵ threshold value for detection scheme.

PROPOSED APPROACH

- The physical/topology information in STLF is not apparent like Kirchhoff's laws.
- Spatial distribution of load forecasting zones is considered to investigate the relation between the different zones to derive constraint.
- An index representing variations between load zones by time series similarity measures may challenge the attacker to meet that.

- Correlation-based distance: $d_{COR}(X,Y) = \sqrt{2(1 - COR(X,Y))}$
- Periodogram-based distance: $d_p(X,Y) = \sqrt{\sum_{j=1}^{[\frac{N}{2}]} [\rho_x(\omega_j) - \rho_y(\omega_j]^2}$
- Autocorrelation-based distance: $d_{ACF}(X,Y) = \sqrt{(\hat{\rho}_{X_T} - \hat{\rho}_{Y_T})^T \, \Omega \, (\hat{\rho}_{X_T} - \hat{\rho}_{Y_T})}$
- Symbolic representation SAX: Time series transforming into a string.
- Euclidean-based distance: $d_{EUC}(X,Y) = \sqrt{\sum_{j=0}^{N-1} (x_i - y_i)^2}$

SIMULATION RESULT

- Case study
  - ERCOT historical summer load
  - 8 weather-based zones
  - Considered two West and FarWest stations
- STLF Model
  - Multiple Linear Regression (MLR)

$$f_1 = \beta_0 + \beta_1 T + \beta_2 H + \beta_3 D + \beta_4 LL_{1w} + \beta_5 LL_{2w}$$
$$f_2 = \beta_0 + \beta_1 DH + \beta_2 MT + \beta_3 MT^2 + \beta_3 MT^3 + \beta_4 HT + \beta_5 HT^2 + \beta_6 HT^3$$

D, M , and H: day of the week (excluding the weekend) month of the year, and hour of the day, T: temperature ,LL1w and LL2w: one and two-week lagged load data.

- Injected $N(0,1)$ to West zone temperature.

Method	No False Injection			False Injection	
	No Model	f_1	f_2	f_1	f_2
d_{ECU}	110644.5	110587.1	110675.4	110652.9	110602.3
d_{COR}	0.3204611	0.3183464	0.2687631	0.326226	0.2826415
d_{ACF}	1.247954	1.146977	1.015968	1.149789	1.040784
d_p	0.1336534	0.1309215	0.1109201	0.1273667	0.1091463
d_{SAX}	2.004495	1.735943	1.417392	2.454994	1.002247

- Proposed a framework to spatially investigate STLF for a defense mechanism.
- Applied similarity measures to explore physical-based constraint.
- Outperformance of SAX method, showing more sensitivity to false data injection.