



The Utility Effect in Cybersecurity of Demand-Response Systems

Oluwafolajinmi Olugbodi, Shaline Kishore, Parv Venkitasubramaniam

Department of Electrical and Computer Engineering at Lehigh University, Bethlehem, PA

Introduction and Background

- Cyber-enabled Demand Response: an electricity tariff imposed by central and utility regulators to motivate changes in electric use by consumers to:
 1. Better match the load requested with the supply
 2. Mitigate high market prices or to alleviate stresses on the grid under duress via real-time pricing signals
- Real-time component of the two-way communication link also exposes Demand-Response systems to cybersecurity threats
- Price-data injection: tariff dispatched by utility regulators to end-use customers is supplanted by the attacker's synthesized tariff;
 - Attack propagates miscommunication, and social and psychological disruptions—*Culture of Fear*

Aim

- The assured safety and reliability of Cyber-enabled Demand Response systems in the event of a malicious attack

Results

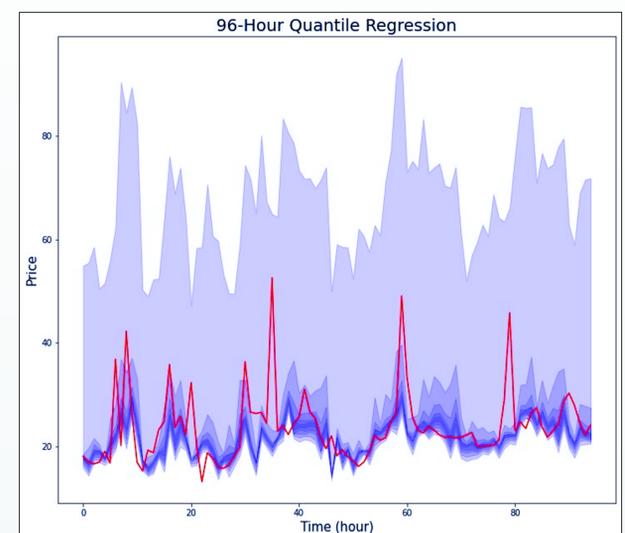
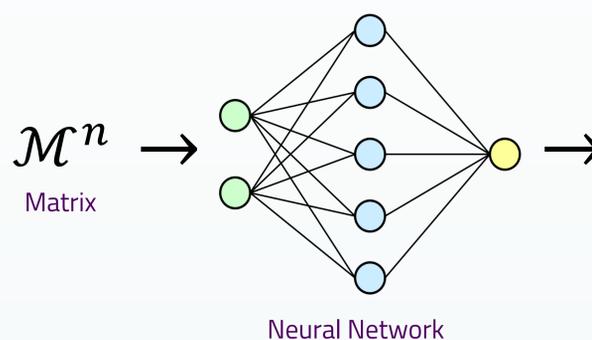
- Findings of the simulation are held in abeyance.
- Initial results prove hopeful
 - Evaluation and method of analysis of the data produced must be advanced and expanded to thoroughly encompass its abstruseness
- Infer the utility of the consumers:
 - In $-p_{i/a}$ price data injection scheme, drastically change in manner that causes the consumers to participate in a continually irrational behaviour
 - In $+p_{i/a}$ scheme, consumers retain the comportment expected of end-users in an uncorrupted environ

Conclusions

- Cybersecurity concerns in Demand-Response systems are weapons that subject the common individual to torment and persecution
- Detection of irregularity in consumer's utilities can help to mitigate and eventually neutralize the effects of preliminary-to-full-scale cyber strikes

System Under Attack (Simulated Model)

- Approach was built on the foundational constitution of the consumers' level of rational response—Prospect theory (PT) and Expected Utility theory (EUT) and the stability of a grid's operations thereafter
- Aggregated training data (LMP data of October 2020, Berks County, Pennsylvania) into a N-dimension matrix then inputted data into a quantile regression neural network that forecasts predicted quantile levels, $\tau = [0, 0.10, 0.20, 0.30, 0.40, 0.50, 0.60, 0.70, 0.80, 0.90, 0.99]$, of prices for a four-day period



Forecasting Model

- Generated Piecewise CDFs and PDFs for each hour, from the forecast model
- Processed the PDFs through a conditional expectation price function, shown in Equation 1
 - \mathcal{M} set of consumers associated with the Berks County node have knowledge of both current and future electricity prices

$$E(x|a \leq x < b) = \frac{\int_a^b xp(x)dx}{\int_a^b p(x)dx} \quad \text{Equation 1}$$

- An optimized utility function with equation variables: flexible and inflexible load demanded, D_1 and D_2 , price per kilowatt-load, P , a proportion of P , price compensation, P_c , and nonlinear constituent kappa, κ , are derived to assess the utility of a consumer m
- δ : the minimum load deferred

$$U(\delta) = \left[D_1 + D_2 - \frac{P + P_c}{2\kappa} \right] P - P_c \left[\frac{P + P_c}{2\kappa} \right] + \kappa \left[\frac{P + P_c}{2\kappa} \right]$$

$$\delta = \min \left(\frac{P + P_c}{2\kappa}, D_2 \right) \quad \text{Equation 2}$$

- Obtained $E(U(\delta))$ and $\{P(U(\delta))_n\}$ sequences for a given hour
- Attacks presented as a series of price manipulations of the original pricing data; the LMP prices are exploited via deterministic and gaussian percentage increase and decrease of the total set of prices, $p_{i/a} = [\pm 0.10, \pm 0.20]$

References

- [1] V. Benson and J. Mcalaney, "Chapter 4 - The social and psychological impact of cyberattacks," in *Emerging cyber threats and cognitive vulnerabilities*, Academic Press, 2020, pp. 73–92
- [2] K. Takemura and H. Murakami, "Probability weighting functions derived from hyperbolic time discounting: Psychophysical models and their individual level testing," *Frontiers in Psychology*, vol. 7, 2016
- [3] PJM, "Historical Load Forecasts," *Data miner 2*, 2020
- [4] K. Hatalis, P. Venkitasubramaniam, and S. Kishore, "Modeling and detection of future cyber-enabled DSM data attacks using supervised learning," *NASA/ADS*, 27-Sep-2019

Acknowledgements

O.O. acknowledges the David and Lorraine Freed Undergraduate Research Symposium

O.O. acknowledges Kostas Hatalis on his support of the makings of the quantile regression neural network