**Barreto, Carlos**; **Koutsoukos, Xenofon**

**Design of load forecast systems resilient against cyber-attacks.** (English) Zbl 1446.93053

Alpcan, Tansu (ed.) et al., Decision and game theory for security. 10th international conference, GameSec 2019, Stockholm, Sweden, October 30 – November 1, 2019. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 11836, 1-20 (2019).

Summary: Load forecast systems play a fundamental role the operation in power systems, because they reduce uncertainties about the system's future operation. An increasing demand for precise forecasts motivates the design of complex models that use information from different sources, such as smart appliances. However, untrusted sources can introduce vulnerabilities in the system. For example, an adversary may compromise the sensor measurements to induce errors in the forecast. In this work, we assess the vulnerabilities of load forecast systems based on neural networks and propose a defense mechanism to construct resilient forecasters.

We model the strategic interaction between a defender and an attacker as a Stackelberg game, where the defender decides first the prediction scheme and the attacker chooses afterwards its attack strategy. Here, the defender selects randomly the sensor measurements to use in the forecast, while the adversary calculates a bias to inject in some sensors. We find an approximate equilibrium of the game and implement the defense mechanism using an ensemble of predictors, which introduces uncertainties that mitigate the attack's impact. We evaluate our defense approach training forecasters using data from an electric distribution system simulated in GridLAB-D.

For the entire collection see [Zbl 1428.68003].

### MSC:

93C83 Control/observation systems involving computers (process control, etc.)
93B70 Networked control
91A65 Hierarchical games (including Stackelberg games)
91A80 Applications of game theory
68M25 Computer security

### Keywords:

security; machine learning; power systems; load forecast; game theory

### Software:

Keras; SciPy

### Full Text: DOI

### References:

[1] Alfeld, S., Zhu, X., Barford, P.: Data poisoning attacks against autoregressive models. In: Thirtieth AAAI Conference on Artificial Intelligence (2016)

[2] Amini, S., Pasqualetti, F., Mohsenian-Rad, H.: Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans. Smart Grid 9(4), 2862-2872 (2016)

[3] Barreto, C., Cardenas, A.: Impact of the market infrastructure on the security of smart grids. IEEE Trans. Ind. Inform. 1 (2018)

[4] Chen, Y., Tan, Y., Zhang, B.: Exploiting vulnerabilities of load forecasting through adversarial attacks. In: Proceedings of the Tenth ACM International Conference on Future Energy Systems, e-Energy 2019, pp. 1-11 (2019)

[5] Choi, D.H., Xie, L.: Economic impact assessment of topology data attacks with virtual bids. IEEE Trans. Smart Grid 9(2), 512-520 (2016)

[6] Chollet, F., et al.: Keras (2015). https://keras.io

[7] Dhillon, G.S., et al.: Stochastic activation pruning for robust adversarial defense. arXiv preprint arXiv:1803.01442 (2018)

[8] Esmalifalak, M., Nguyen, H., Zheng, R., Xie, L., Song, L., Han, Z.: A stealthy attack against electricity market using inde-

pendent component analysis. IEEE Syst. J. 12(1), 297-307 (2015)

[9] Fudenberg, D., Tirole, J.: Game Theory. The MIT Press, Cambridge (1991) · Zbl 1339.91001

[10] Hernandez, L., et al.: A survey on electric power demand forecasting: future trends in smart grids, microgrids and smart buildings. IEEE Commun. Surv. Tutor. 16(3), 1460-1495 (2014)

[11] Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. 9(8), 1735-1780 (1997)

[12] Hyndman, R.J., Koehler, A.B.: Another look at measures of forecast accuracy. Int. J. Forecast. 22(4), 679-688 (2006)

[13] Ilyas, A., Santurkar, S., Tsipras, D., Engstrom, L., Tran, B., Madry, A.: Adversarial examples are not bugs, they are features. arXiv preprint arXiv:1905.02175 (2019)

[14] Jia, L., Thomas, R.J., Tong, L.: Malicious data attack on real-time electricity market. In: 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 5952-5955 (2011)

[15] Jones, E., Oliphant, T., Peterson, P., et al.: SciPy: open source scientific tools for Python (2001). http://www.scipy.org/

[16] Kirschen, D.S., Strbac, G.: Fundamentals of Power System Economics. Wiley, Hoboeken (2004)

[17] Klebanov, L.B., Rachev, S.T., Fabozzi, F.J.: Robust and Non-robust Models in Statistics. Nova Science Publishers, Hauppauge (2009)

[18] Lecuyer, M., Atlidakis, V., Geambasu, R., Hsu, D., Jana, S.: Certified robustness to adversarial examples with differential privacy. arXiv preprint arXiv:1802.03471 (2018)

[19] Liu, C., Zhou, M., Wu, J., Long, C., Kundur, D.: Financially motivated FDI on SCED in real-time electricity markets: attacks and mitigation. IEEE Trans. Smart Grid 10(2), 1949-1959 (2019)

[20] Liu, X., Cheng, M., Zhang, H., Hsieh, C.-J.: Towards robust neural networks via random self-ensemble. In: Ferrari, V., Hebert, M., Sminchisescu, C., Weiss, Y. (eds.) ECCV 2018. LNCS, vol. 11211, pp. 381-397. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01234-2_23

[21] Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, pp. 21-32 (2009)

[22] Nudell, T.R., Annaswamy, A.M., Lian, J., Kalsi, K., D'Achiardi, D.: Electricity markets in the United States: a brief history, current operations, and trends. In: Stoustrup, J., Annaswamy, A., Chakrabortty, A., Qu, Z. (eds.) Smart Grid Control. PEPS, pp. 3-27. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-98310-3_1

[23] Papernot, N., McDaniel, P., Goodfellow, I.: Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. arXiv preprint arXiv:1605.07277 (2016)

[24] Schneider, K.P., Chen, Y., Chassin, D.P., Pratt, R.G., Engel, D.W., Thompson, S.E.: Modern grid initiative distribution taxonomy final report. Technical report, Pacific Northwest National Laboratory (2008)

[25] Sevlian, R., Rajagopal, R.: A scaling law for short term load forecasting on varying levels of aggregation. Int. J. Electr. Power Energy Syst. 98, 350-361 (2018)

[26] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., Salakhutdinov, R.: Dropout: a simple way to prevent neural networks from overfitting. J. Mach. Learn. Res. 15(1), 1929-1958 (2014) · Zbl 1318.68153

[27] Szegedy, C., et al.: Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199 (2013)

[28] Tan, S., Song, W.Z., Stewart, M., Yang, J., Tong, L.: Online data integrity attacks against real-time electrical market in smart grid. IEEE Trans. Smart Grid 9(1), 313-322 (2016)

[29] Xie, L.