Detection of the False Data Injection Attack in the Smart Grid using ANN

Zakaria El Mrabet[1], Daisy Flora Selvaraj[1], and Prakash Ranganathan[1]

[1]School of Electrical Engineering and Computer Science, University of North Dakota

DECS

UND UNIVERSITY OF NORTH DAKOTA

Outline

- Introduction
- Problem Statement
- Objective
- Methodology
- Simulation Results
- Conclusion
- References

Introduction

- Globally, utilities loss 96$ billion per year due to non-technical loss: typically electricity theft, fraud, billing errors, and other loss revenue.
- **False Data Injection** is regarded as a fraud that manipulates maliciously and illegally the actual energy consumption.
- **How FDI is conducted** ? The attacker injects malicious packets in the wireless network by either hijacking the communication channel or compromising the smart meters.

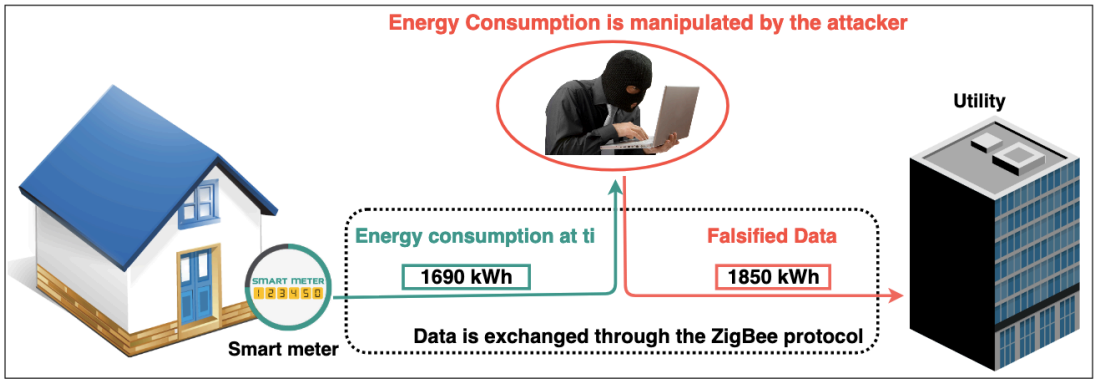


Fig. 2. An FDI attack scenario

[1] Northeast Group LLC, “Electricity Theft and Non-Technical Losses: Global Markets, Solutions, and Vendors,” 2017.

Problem statement

- False data injection attack impact

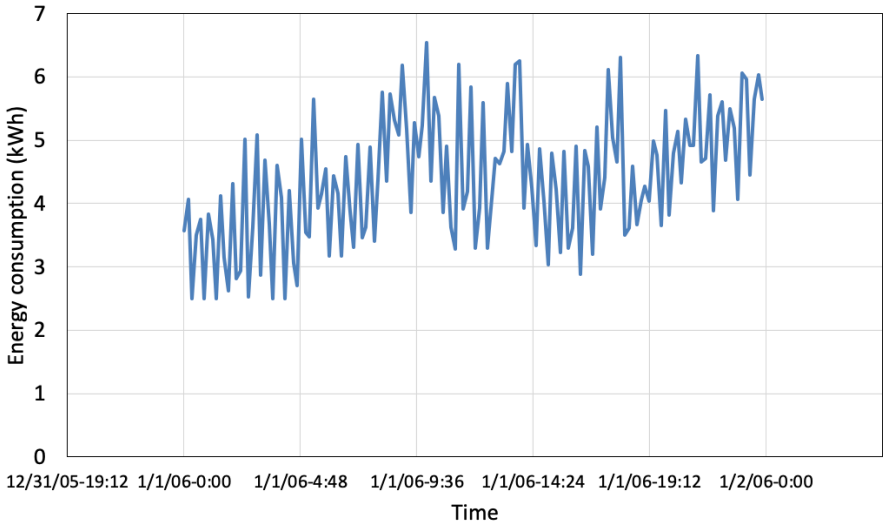


Fig. 3. A normal energy consumption for a given household

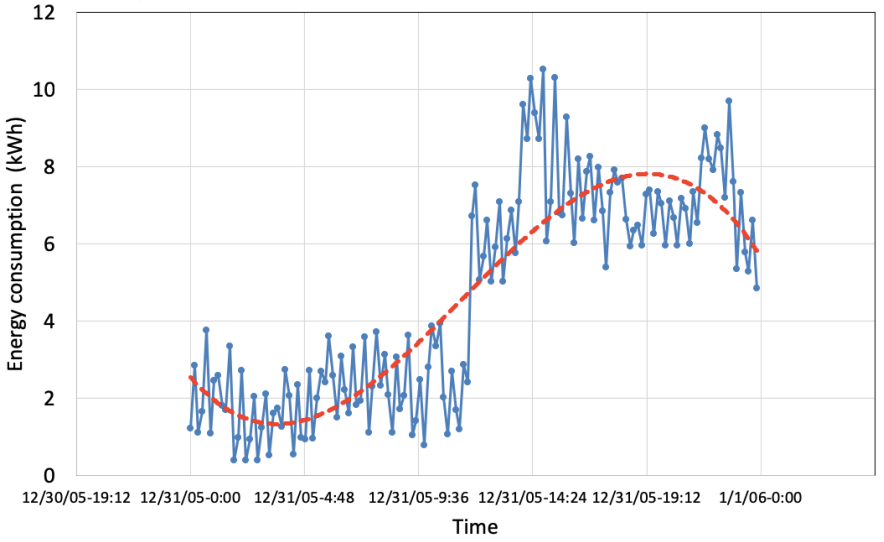


Fig. 4. Falsified energy consumption via the FDI attack

Objective

- Modeling the FDI attack using two membership functions: Sigmoid and Trapezoidal.
- Developing an Artificial Neural Network based model for detecting the FDI attack.
- Conducting a parametric study to find the optimal configuration for ANN.
- Comparing the proposed approach against SVM and Random Forest based on several performance metrics including the probability of detection, the probability of miss detection, and the accuracy.

Methodology: Dataset

- The used dataset includes the electricity demand profiles for 200 households randomly selected among the ones available in the 2009 Residential Energy Consumption Survey (RECS) dataset for the Midwest region of the United States for one year.

- The profiles have been generated using the approach proposed by Muratori et al. [1], that produces realistic patterns of residential power consumption, then validated using metered data with a resolution of 10 minutes.

- Households vary in size and number of occupants and the profiles represent total electricity use. Each household consists of four main features: date, time, energy demand, and the cost per kWh.

[1] M. Muratori et al. “A highly resolved modeling technique to simulate residential power demand,” Appl. Energy, vol. 107, pp. 465–473, Jul. 2013.

Methodology: FDI attack model

- **Attack scenario 1: Increasing the energy consumption during the peak hours**
  - It is assumed that an adversary seeks to increase the energy consumption of a compromised smart meter during the peak hours in order to increase drastically the electricity bills of the targeted user. This can be modeled using the trapezoidal function:

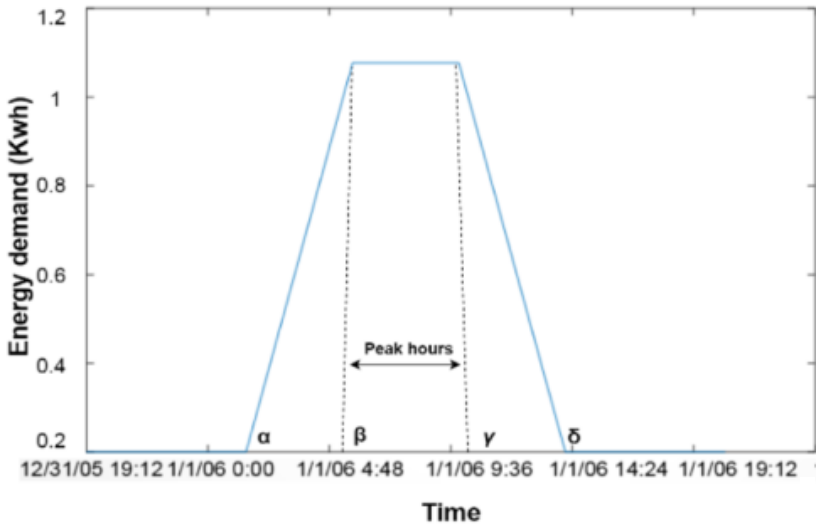


Fig. 5. Scenario 1: Increasing the energy demand consumption during the peak hours

$$u(x,\alpha,\beta,\gamma,\delta) = \begin{cases} 0, & x < \alpha \\ \frac{x-\alpha}{\beta-\alpha}, & \alpha \le x \le \beta \\ 1, & \beta < \alpha \le \gamma \\ \frac{\gamma-x}{\gamma-y}, & \gamma < x \le \delta \\ 0, & x > \delta \end{cases} \quad (1)$$

Here x is the time variable and [β, γ] is the peak electricity usage time interval.

Methodology: FDI attack model

- **Attack scenario 2: Increasing the energy demand during the off-peak hour for a long period of time**
  - It is assumed that the attacker performs an abnormal load increase in energy consumption for several hours during the off-peak hour to affect the electricity bill of a targeted user. This can be modeled using the sigmoid function is used:

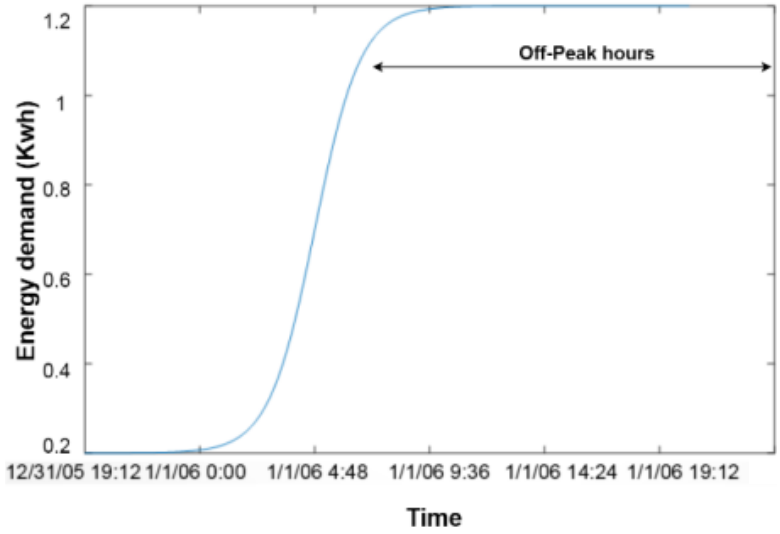


Fig. 6. Scenario 2: Increasing the energy demand consumption during the off-peak hours

$$f(x) = \frac{1}{1+e^{-x}} \quad (2)$$

Here x represents the energy demand value

Methodology: Dataset

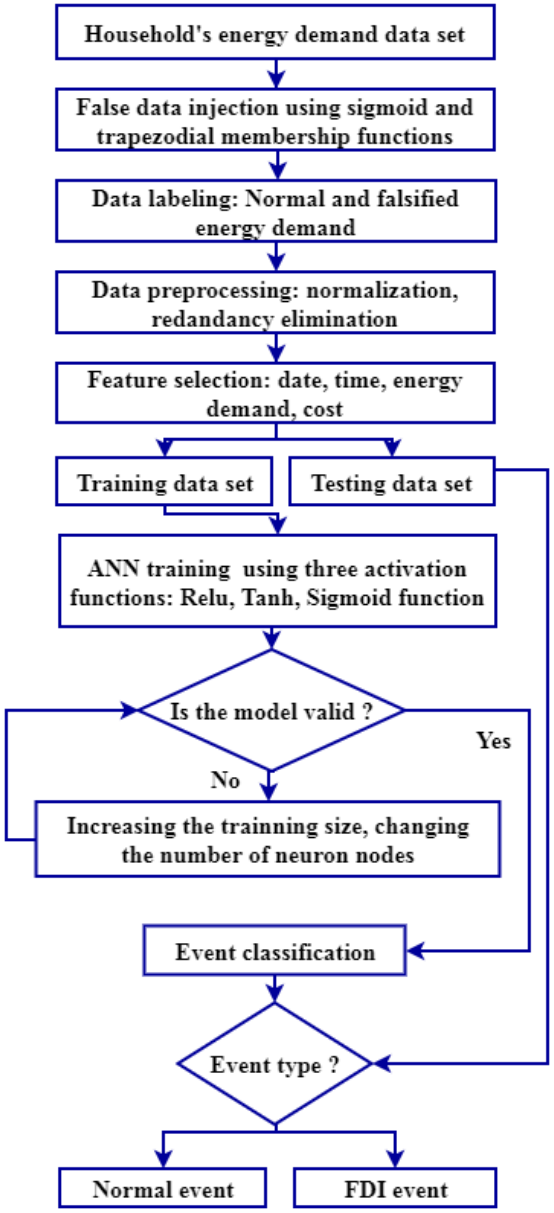
- Table below provides some statistics about the dataset which includes legitimate energy consumption and the falsified measurements during scenarios 1 and 2.

Duration of the collected data	**1 year with 10 min resolution**
Number of instances	52560
Number of falsified data	26250
Number of normal data	26250
Number of attributes	4

Methodology: ANN model

- The pospoed ANN is composed of an input layer, two hidden layers, and the output layer where each layer is composed of several neurons.

- A neuron is a computation unit which takes a set of inputs where each input is associated with weight and predicts the output using an activation function.



Methodology: ANN model

- Three activation functions are investigated with ANN:
  - Sigmoid function is given by:

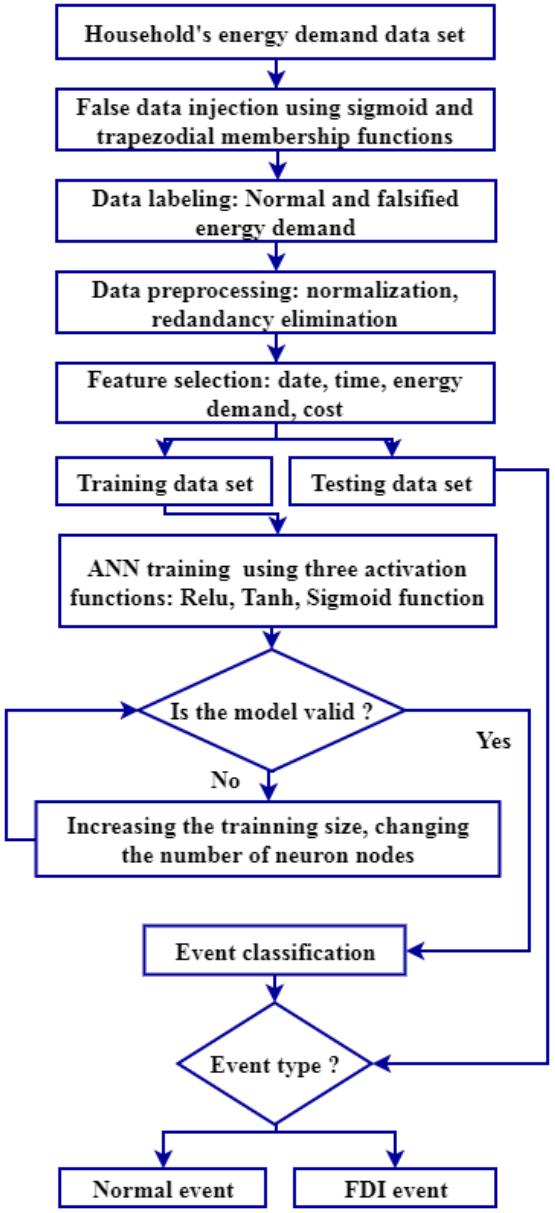
$$f(z) = \frac{1}{1+e^{-z}} \qquad (3)$$

  - Hyperbolic tangent (Tanh) function is expressed as:

$$f(z) = \max(0, z) \qquad (4)$$

  - Rectified linear unit (Relu) function is given by:

$$f(z) = \tanh(0, z) \qquad (5)$$



Methodology: Performance metrics

- Accuracy:

$$Acc = \frac{TP + TN}{TP+TN+FN+FP} \qquad (6)$$

- Probability of detection:

$$P_d = \frac{TP}{TP+ FN} \qquad (7)$$

- Probability of false alarm:

$$P_{fa} = \frac{FP}{TN+FP} \qquad (8)$$

- Probability of miss detection:

$$P_{md} = 1 - \frac{TP}{TP+FN} \qquad (9)$$

Where TP: true positive, TN: true negative, FP: false positive, and FN: false negative.

Simulation Results

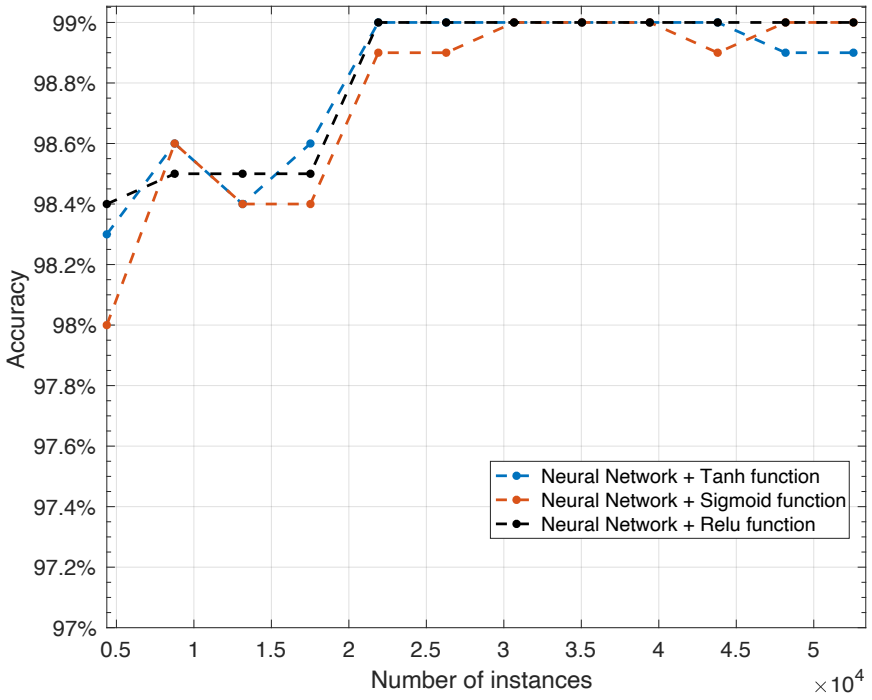


Fig. 7. The accuracy of NN with three activation functions: Relu, Sigmoid, and Tanh function, as a function of the number of instances.

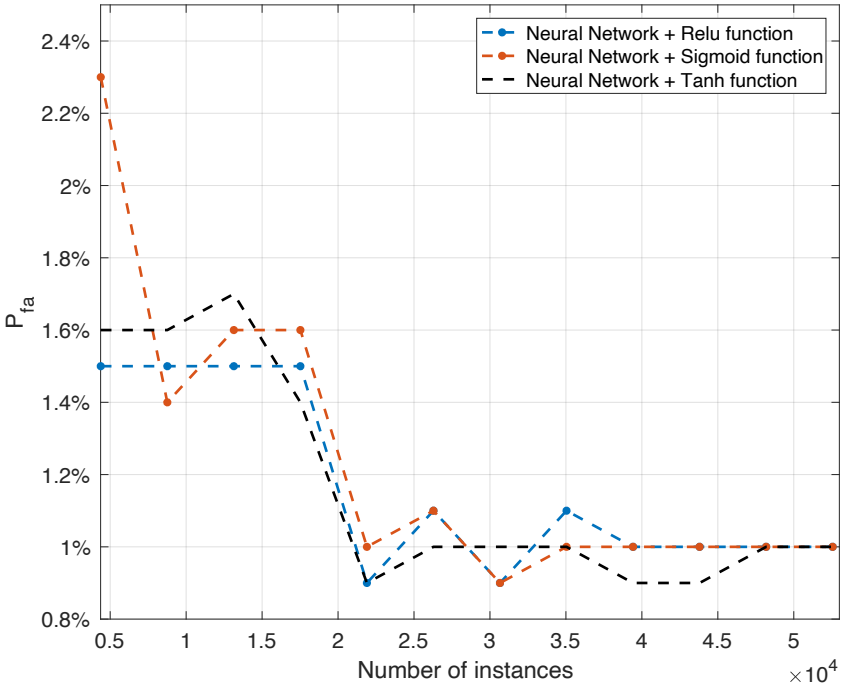


Fig. 8. The P_{fa} of NN with three activation functions: Relu, Sigmoid, and Tanh function, as a function of the number of instances.

Simulation Results

Algorithm	Accuracy	P_d	P_{md}	P_{fa}
SVM- RBF	86%	72.7%	27.3%	1.8%
SVM- Sigmoid	84.3%	80.5%	19.5%	12.3%
SVM- Polynomial	82.9%	66.9%	33.1%	2.7%
ANN- Relu (100 neuron nodes)	99%	99.4%	0.6%	0,9%
RF (10 trees)	92.8%	85.9%	14.1%	1.1%
RF (100 trees)	94.3%	88.2%	11.8%	0.2%

Conclusion

- An ANN based appraoch is developped to detect FDI attack.
- Two attack scenarios are considered to simulate the FDI attack using two membership functions namely, Sigmoid and Trapezoidal.
- The obtained results show that ANN with the Relu activation function and 100 neuron nodes detects the falsified injected data with an accuracy of 99%.
- ANN outperforms RF and SVM in terms of P_d and accuracy.
- RF with 100 trees exhibits an optimal probability of false alarm, which is 0.2%, followed by ANN with 0.9%

References

- "Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT." [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. [Accessed: 10-Dec-2018].
- D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," Electr. Inf. Shar. Anal. Cent. E-ISAC, 2016.
- G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
- Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 87–98, Mar. 2013.
- W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Comput. Netw., vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
- J. Zhao, J. Wang, and L. Yin, "Detection and Control against Replay Attacks in Smart Grid," in 12th International Conference on Computational Intelligence and Security, China, 2016, pp. 624–627.
- P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "A denial of service attack in advanced metering infrastructure network," in IEEE International Conference on Communications (ICC), 2014, pp. 1029–1034.
- Y. Yang et al., "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems," in SUPERGEN, 2012, pp. 1–8.
- El Mrabet, Z., Kaabouch, N., El Ghazi, H. and El Ghazi, H. 2018. Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering. 67, 2018, pp. 469–482.
- Z. Lu, W. Wang, and C. Wang, Modeling and Evaluating Denial of Service Attacks for Wireless and Mobile Applications. Springer, 2015.
- R. Al-Dalky, O. Abduljaleel, K. Salah, H. Otrok, and M. Al-Qutayri, "A Modbus traffic generator for e the security of SCADA systems," in CSNDSP, 2014, pp. 809–814.

Thank you!

Questions?

Zakaria.elmrabet@und.edu