Detecting False Data Injection attacks in Smart Grid

Zakaria El Mrabet , Daisy Flora Selvaraj, and Prakash Ranganathan
School of Electrical Engineering and Computer Science (SEECS)

Introduction

- Globally, utilities loss 96$ billion per year due to non-technical loss – typically electricity theft, fraud, billing errors, and other loss revenue.
- ***What is an FDI attack?***
  False data injection attack (FDI) is regarded as a fraud that manipulates maliciously and illegally the actual energy consumption.
- ***How an FDI attack is conducted?***
  The attacker injects malicious packets in the wireless network by either hijacking the communication channel or compromising the smart meters.
- ***Who is the attacker?***
  Legal customer, intruder.

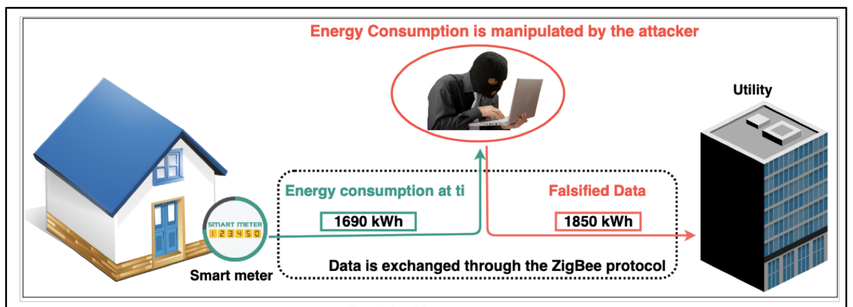

Fig. 1 An FDI attack scenario

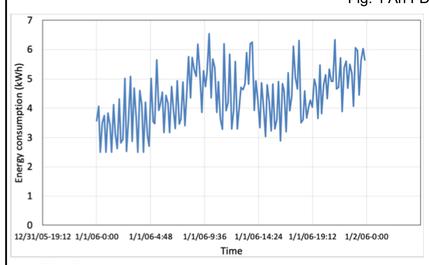

Fig. 2 A normal energy consumption for a given household

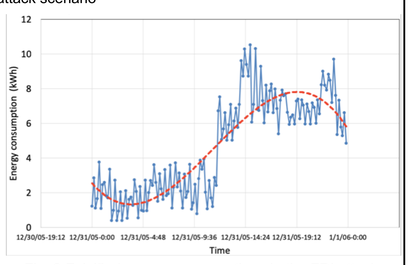

Fig. 3 Falsified energy consumption via the FDI attack

Goal

- The purpose of this research is to develop a machine learning based approach for detecting accurately the FDI attack in Smart Grid.

Methodology

- ***Data set***
  The data set used in this project includes the electricity demand profiles for 200 households for the Midwest region of the United States.
- ***Features***
  The relevant features selected from this data set are:
  - Electricity demand for each Household
  - Date of consumption
  - Time of consumption

  Additionally, another feature is included related to the cost per kWh (time-of-use).
- ***Attack model***
  To model the FDI attack, several membership functions are used to falsify the legitimate data set.
  Example of these functions are given below:

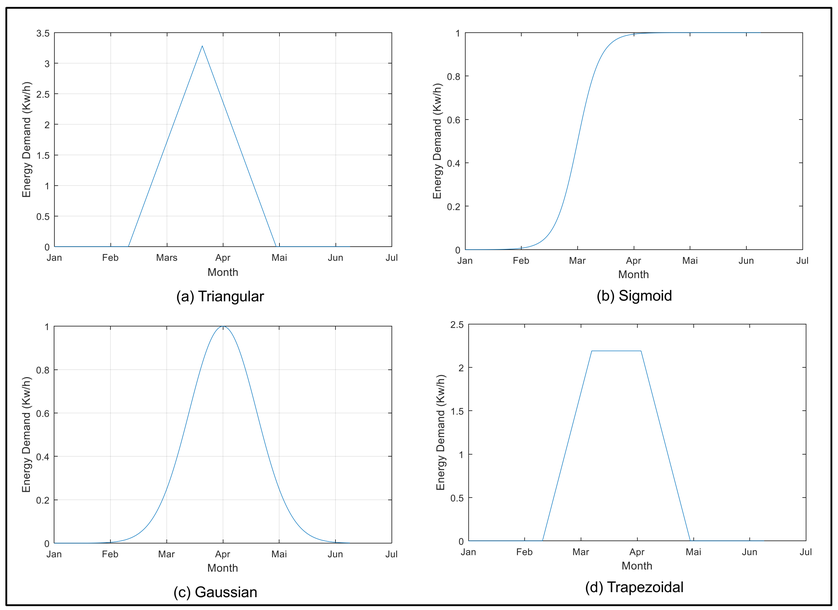

Fig. 4 Example membership function used to falsify the data

- ***Machine learning approach***
  - Train an Artificial Neural Network (ANN) classifier with various activation functions.
  - Compare the ANN model with Support Vector Machine (SVM) and Random Forest (RF).

Preliminary Results

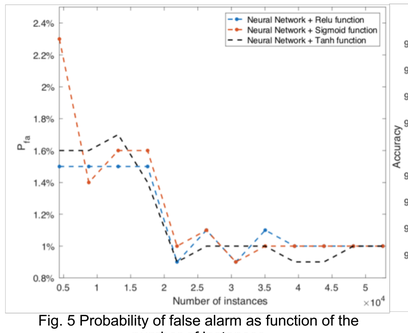

Fig. 5 Probability of false alarm as function of the number of instances

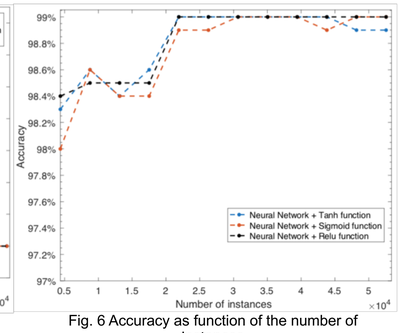

Fig. 6 Accuracy as function of the number of instances

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

- The experimental results indicate that ANN is an optimal approach for detecting the falsified injected data over other approaches.

References

- Northeast Group LLC, “Electricity Theft and Non-Technical Losses: Global Markets, Solutions, and Vendors,” 2017.
- Z. El Mrabet, et al. “Cyber-security in smart grid: Survey and challenges,” Computers & Electrical Engineering, Volume 67, 2018.
- Z. El Mrabet et al. “Detection of the False Data Injection Attack in the Home Area Network using ANN” submitted to IEEE EIT conference, 2019.