Detecting False Data Injection attack in Smart Grids

Zakaria El Mrabet (Ph.D. student) and Dr. Prakash Ranganathan
School of Electrical Engineering and Computer Science (SEECS)

Introduction

- Smart grid exploits information technology to intelligently deliver energy by using a two-way communication and wisely meet the environmental requirements by facilitating the integration of green technologies
- However, The inherent weakness of communication technology has exposed the system to numerous security threats.
- False Data Injection (FDI) attack is considered as a harmful attack since it can disturb the grid system state estimation and the energy distribution.
- In FDI, the attacker inject malicious packets in the wireless network by either compromising the sensor nodes or hijacking the communication channel.

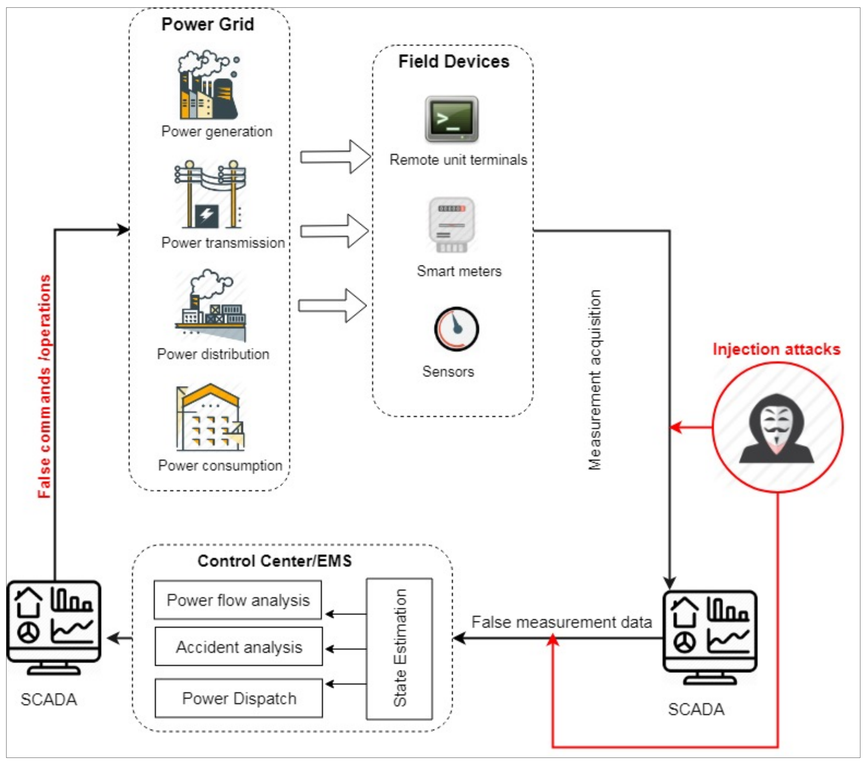

Fig. 1 FDI attack scenario in a Smart Grid

Goal

- The purpose of this research is to detect the false data injection attack in Smart Grids by developing a machine learning based approach.

Methodology

- ***Data set***
  - The data set used in this project includes the electricity demand profiles for seven households for the Midwest region of the United States.

- ***Features***
  - The relevant features selected from this data set are:
    - Date
    - Time
    - Electricity demand for Household
  - 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:

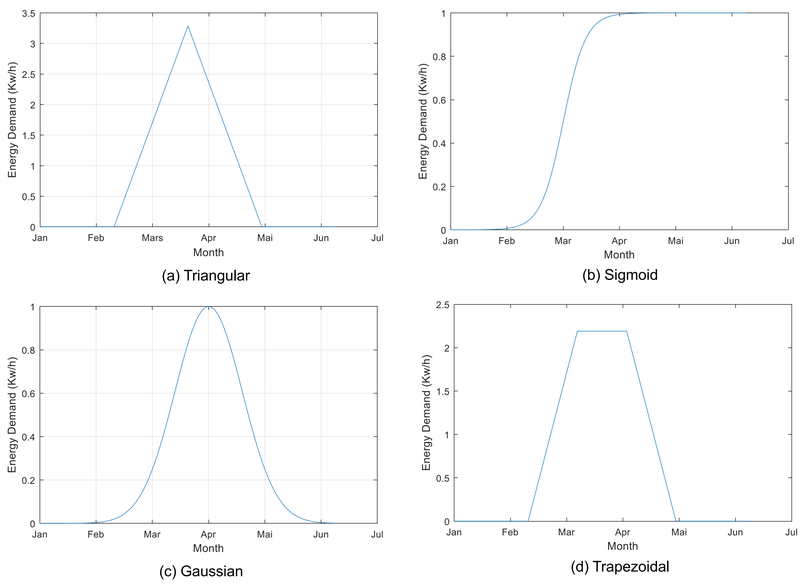

Fig. 2 Example membership function used to falsify the data

- ***Machine learning approaches***
  - Artificial Neural Network (ANN), Support Vector Machine (SVM), and Random Forest (RF).
  - Different variations are adapted: multiple kernels, different number of neurons, and varying number of trees.
  - Several performance metrics such as the probability of detection (Pd), the probability of miss detection (Pmd), and the accuracy are computed.

Preliminary Results

Algorithm	Probability of detection	Probability of false alarm	Probability of miss detection	Accuracy
SVM (RBF Kernel)	72.7%	1.8%	27.3%	86%
SVM (Sigmoid)	80.5%	12.3%	19.5%	84.3%
SVM (Polynomial)	66.9%	2.7%	33.1%	82.9%
Neural Network (Relu function, 100)	**98.8%**	**1.4%**	**1.2%**	**98.7%**
Neural Network (Logistic function, 100)	99.4%	3.4%	0.6%	97.9%
Neural Network (Tanh function, 100)	98.6%	3.6%	1.4%	97.4%
Random Forest (10 trees)	85.9%	1.1%	14.1%	92.8%
Random Forest (100 trees)	88.2%	0.2%	11.8%	94.3%

Conclusion

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

References

- Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, “Cyber-security in smart grid: Survey and challenges,” Computers & Electrical Engineering, Volume 67, 2018.
- G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A Review of False Data Injection Attacks Against Modern Power Systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.