Power System Topology Identification With Security Aware Machine Learning Using Smart Meter Data

Cody Francis
Dr. Vittal Rao
Texas Tech University Department of Electrical Engineering & Computer Engineering

PRESENTED AT

Abstract

Distribution system topology identification (DSTI) has historically been accomplished by unencrypting the information that is received from the smart meters and then running a topology identification algorithm. Unencrypted smart meter data introduces privacy and security issues for utility companies and their customers. A security aware machine learning algorithm is introduced to alleviate the privacy and security issues raised with unencrypted smart meter data. The security aware machine learning algorithm uses the information received from the Advanced Metering Infrastructure (AMI) and identifies the distribution systems topology without unencrypting the AMI data by using a fully homomorphic NTRU encryption. The encrypted smart meter data is then used by the Linear Discriminant Analysis (LDA) algorithm to predict the distribution systems real time topology. This method can leverage noisy voltage magnitude readings from smart meters to accurately identify distribution system reconfiguration between radial topologies during operation under changing loads.

Introduction

All distribution system switch statuses may not accurately be captured by the Energy Management System (EMS) which oversees the operation of a given distribution system. It is often cost prohibitive to include real time telemetering in all switches on a given distribution system and alternative methods to gather switch status involve sending crews to the field which can introduce human error. These issues are why DSTI will be accomplished by using the time series voltage magnitudes received from smart meters.

The reason smart meter data was used is because there is a limited presence of nodal and line meters in distribution grids which hinders the real time identification of topology [1].

There are many approaches to DSTI but all of which assume that the smart meter data has already been unencrypted so that the needed information can be ran through the chosen algorithm. Unencrypting the smart meter data can introduce unintended issues with security and privacy for both the utility company and their customers [2].

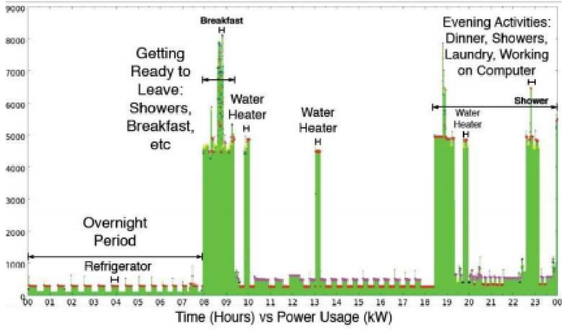

Figure 1. Load profile of residential customer over 24-hour period [6].

Smart meter data is currently encrypted using Advanced Encryption Standard (AES) which is standardized by the American National Standards Institute (ANSI) under the code for electric metering ANSI C12.22-2012. The current AES encryption is a non-homomorphic form of encryption which does not allow for mathematical operations to be performed on the encrypted information so the smart meter data must be unencrypted for it to be used in a machine learning algorithm [3].

With unencrypted smart meter data, it is possible for unintended/bad actors to determine personal behavior patterns which would allow them to target certain demographics such as latch key children or the elderly for home invasion [4]. This type of issue could open the utility company up to liability since it was the company itself that unencrypted the smart meter data to perform a host of crucial power grid operations such as distributed energy resources management, state estimation, power flow analysis, conservation voltage reduction (CVR), load management, demand response, volt/VAR optimization (VVO), to name a few [5]. As shown in figure 1 it is possible to deduce customer behavior based off usage amount and time.

Problem Formulation

The utility company's private keys are f, f_p, and g, while the public key h is generated computing the quantity shown below.

$$h = pf_q \cdot g \pmod q$$

When the smart meter wants to send encrypted information to the utility company, the information is put into the form of a polynomial m representing the smart meter data with coefficients in $\left[-\frac{p}{2}, \frac{p}{2}\right]$. After creating the polynomial, which is a representation of the information being sent, the smart meter randomly chooses a polynomial r with small coefficients (not restricted to the set {-1,0,1}), which are meant to obscure the information being sent by the smart meter. With the utility companies public key h the encrypted message e is computed by the smart meter as shown.

$$e = r \cdot h + m \pmod q$$

This encryption scheme hides the smart meter information so that it can be safely sent to the utility company but anybody knowing r could compute the message m by evaluating $e - r \cdot h$ so r must not be revealed by the smart meter to any other parties. In addition to the publicly available information, the utility company knows its own private key.

Methods and Materials

A combination of the programs OpenDSS Version 7.6.5.91, MATLAB 2020a, and a MATLAB Toolbox GridPV Version 2.2, were used to generate the synthetic data and simulate the grid operations, construct the library, and validate its successful predictions for the DSTI algorithm. The yearly sequential time simulation of the distribution system is generated using OpenDSS and the classification algorithms and encryption are implemented in MATLAB using GridPV as an interface.

This distribution system configuration was used for training and validation of the proposed algorithms for DSTI without encryption and DSTI with encryption. This system has 5 radial topologies, therefore there exist 20 possible topology transitions. Additionally, there are 5 classes that represent unchanged topology between measurement scans. In total there are 25 possible switch transitions that represent the classes for the topology problem.

Varying amounts of noise was added to the voltage magnitude measurements received from the smart meters to determine the robustness of the algorithms to noise. The noise is added to the voltage magnitude before any encryption of the smart meter data is completed with four different variations of Gaussian noise added .

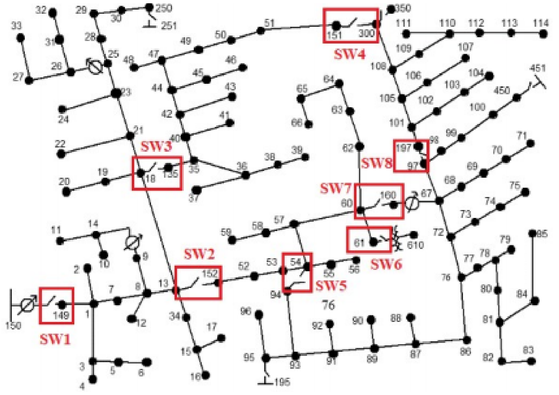

Figure 2. IEEE 123-bus feeder showing its 8 switches [8].

Preliminary Results

In this simulation a false positive is considered a prediction in the validation portion that there has been a topology change when there in fact was no topology change. The results of the simulation are shown in Table 1.

In the simulation the amount of Gaussian noise added to the voltage magnitude measurements is incremented from 0, 1, 2, and 3 percent. As can be seen from TABLE 1. both the LDA without encryption and the LDA with encryption did both exhibit a decrease in accuracy prediction as well as an increase in false positive as the noise in the voltage measurements was increased from zero to 3 percent.

These simulation results show a very low accuracy for the correct transition classification when the NTRU encryption scheme is employed, and this low accuracy seems to be further degraded by the addition of gaussian noise to the smart meter measurements.

Table 1. Simulation Results – LDA with and without encryption with varying amounts of noise.

Noise Level	LDA Without Encryption			
	Correct	*Wrong*	*% Correct*	*False Positive*
None	150	0	100	0
0.01	150	0	100	0
0.02	148	2	98.7	3
0.03	145	5	96.7	5
	LDA With Encryption			
None	57	93	38.0	5
0.01	42	108	28.0	11
0.02	33	117	22.0	38
0.03	24	126	16.0	88

Conclusion

A DSTI method by using a one-versus-all LDA classifier using only 15-minute voltage magnitude time series data as input was compared to the same classifier with a fully homomorphic encryption added to the data before being used by the classifier. The classifier without encryption appeared to function with few errors predicted of the transitions between radial topologies in the IEEE 123-Bus test system over a 9-month testing period with a prior 3-month training period even with the addition of varying noise added to the voltage magnitude measurements. The method has shown robustness to load variations and noise in measurements.

The LDA classifier with encryption does not seem to possess an accuracy that would be promising for use of this algorithm in real world scenarios, with this accuracy being even further degraded by increasing measurement noise.

The two different types of simulations with noise added to the smart meter measurements and no noise added allow us to gauge the deterioration in the predictive ability of the topology identification algorithm with and without encryption. Even though the performance of the algorithm without encryption is degraded by noise, this method would still have viable real-world application for the identification of the distribution grid topology since the performance remains high and more accurate meters could be used.

In future research the use of different homomorphic encryptions to gauge their effect on the algorithms predictive accuracy may give rise to an encryption scheme with an accuracy high enough for real world deployment.

Acknowledgements

This material is based upon work supported by the fellowship Graduate Assistance in Areas of National Need (GAANN). The author would also like to gratefully acknowledges the support of Dr. Pal for subject matter expertise in security awareness concepts.

References

1) W. H. Kersting, "Radial distribution test feeders," in IEEE Transactions on Power Systems, vol. 6, no. 3, pp. 975-985, Aug. 1991, doi:10.1109/59.119237.
2) S. Finster and I. Baumgart, "Privacy-Aware Smart Metering: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1088-1101, Second quarter 2015, doi:10.1109/COMST.2015.2425958.
3) Graepel T, Lauter K, Naehrig M. ML confidential: Machine learning on encrypted data. In: International Conference on Information Security and Cryptology. Springer; 2012. P. 1-21.
4) G. Giaconi, D. Gunduz and H. V. Poor, "Privacy-Aware Smart Metering: Progress and Challenges," in *IEEE Signal Processing Magazine*, vol. 35, no. 6, pp. 59-78, Nov. 2018, doi:10.1109/MSP.2018.2841410.
5) L. Blakely, M. J. Reno, and J. Peppanen, "Identifying Common Errors in Distribution System Models," IEEE Photovoltaic Specialists Conference (PVSC). 2019.
6) Molina-Markham "Private Memoirs of a Smart Meter," 2nd ACM Workshop on Embedded Sensing Systems For Energy Efficiency In Buildings, Zurich, Switzerland, November 2, 2010.
7) Francis, Cody & Rao, Vittal & Trevizan, Rodrigo & Reno, Matthew. (2021). Topology Identification of Power Distribution Systems Using Time Series of Voltage Measurements.
8) M. Jafarian, A. Soroudi and A. Keane, "Distribution System Topology Identification for DER Management Systems Using Deep Neural Networks," 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2020, pp. 1-5, doi: 10.1109/PESGM41954.2020.9282121.