Avoiding Occupancy Detection from Smart Meter Energy Consumption Using Adversarial Machine Learning

Ibrahim Yilmaz, Advisor: Dr. Ambareen Siraj
Department of Computer Science, Tennessee Tech University

Introduction

- Smart meters report information every fifteen minutes as a default. New brand meters are capable of collecting data every minutes or every seconds [1]. Detail energy usage information including timing provides numerous advantages to both grid participants and utility companies such as faster bi-directional communication between utility services and end users, direct load control for demand response, energy saving and so on. The fine-grained usage data is useful for monitoring customers' loads more detailed such as forecast future load need.

Problem Definition

- The fine-grained usage data provided by smart meters bring additional vulnerabilities from users to companies.
- This time of use information can later be used for a broad range of purposes and nefarious intentions such as advertising or surveillance.
- Most of the existing privacy preserving techniques use crypto-graphical techniques that are computationally expensive for resource restrained smart meters [2].

The Proposed Scheme

- Adversarial Machine Occupancy Detection Avoidance (AMODA) model is presented in a privacy preserving manner in order to conceal time of use information without relying on third party.
- The electricity usage signal of a user is tracked by using Long Short-Term Memory **(**LSTM) model and is identified characteristic behavior of flow information from the past experience.
- Consumption patterns are modified slightly through optimized noise by the AMODA model without compromising users' billing systems functionality.
- Electricity suppliers learn nothing except total electricity usage of customers.
- The proposed scheme does not required any hardware change on the smart meter but necessitates a minor software change.

The Proposed AMODA Model Algorithm

$$\textit{objective} \quad \max\ C(M, \hat{x}, y) \qquad (1)$$

$$y \neq \hat{y} \qquad (2)$$

$$\textit{subject to} \quad \hat{x} = x + \delta x \qquad (3)$$

$$\|\delta x\| \leq \epsilon * |x| \qquad (4)$$

$$\delta x = \epsilon\ \textit{sign}(\nabla x\ C(M, x, y)) \qquad (5)$$

Notations

Name	
M	Attack Model
X	Real Sample
$\hat{X}$	Crafted Sample
Y	Label
$\hat{Y}$	Model Prediction
ϵ	Penetration Coefficient
C (M, x, y)	Cost Function

Contributions

- Our approach based on a LSTM model show the viability of an occupancy detection attack over a massive real electricity consumption dataset.
- It offers a one-size-fits-all approach for protecting privacy breach of grid customers automatically by modifying meter program.
- This automatic system provides rescheduling of users' electricity consumption in a trustworthy manner without compromising users' billing system.

Conclusion and Future Work

- The viability of an occupancy detection attack based on LSTM model is demonstrated.
- The AMODA framework is introduced as a counter attack in order to prevent abuse of energy consumption.
- Results show that the proposed privacy-aware billing technique upholds user's privacy strongly
- Future Work:
  - A more sophisticated analysis can be carried out to achieve balance between privacy and efficiency.

Acknowledgement

- This work is funded by CESR (Center for Energy Systems) at Tennessee Technological University with resource support from the Cybersecurity Education Research and Outreach Center (CEROC).

Results

Summer					
Penetration Coefficient	Home 1	Home 2	Home 3	Home 4	Home 5
0.00	0.94	0.99	N/A	0.97	0.99
0.05	0.78	0.68	N/A	0.90	0.55
0.10	0.75	0.66	N/A	0.88	0.44
0.15	0.73	0.66	N/A	0.86	0.40
0.20	0.72	0.64	N/A	0.85	0.38
0.25	0.72	0.62	N/A	0.85	0.38
0.30	0.71	0.61	N/A	0.84	0.37

Table 1: Accuracy vs Penetration Coefficient in Summer

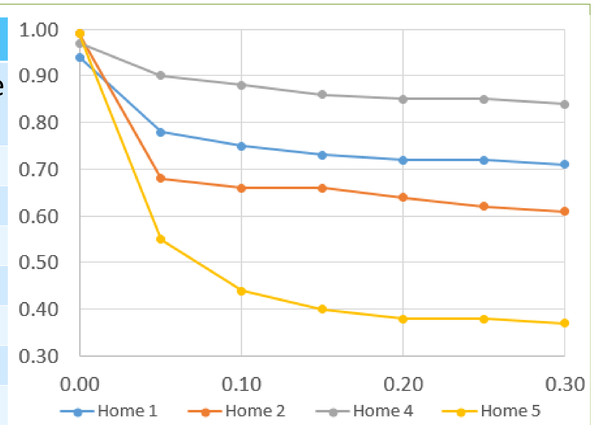

Figure 1: Accuracy vs Penetration Coefficient in Summer

Winter					
Penetration Coefficient	Home 1	Home 2	Home 3	Home 4	Home 5
0.00	0.94	0.94	0.95	0.99	0.98
0.05	0.80	0.74	0.60	0.88	0.37
0.10	0.68	0.72	0.58	0.86	0.32
0.15	0.57	0.70	0.57	0.86	0.30
0.20	0.56	0.68	0.56	0.85	0.28
0.25	0.56	0.67	0.56	0.85	0.28
0.30	0.56	0.66	0.55	0.84	0.27

Table 2: Accuracy vs Penetration Coefficient in Winter

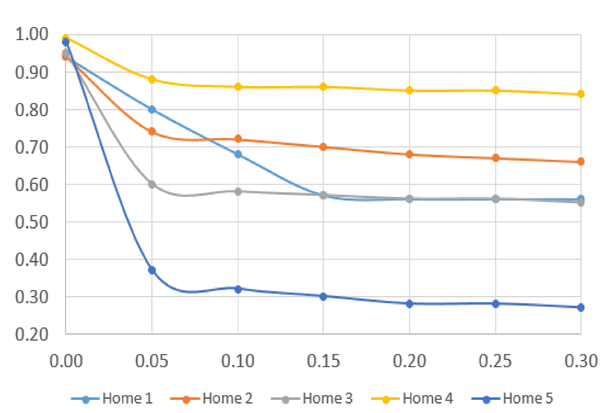

Figure 2: Accuracy vs Penetration Coefficient in Winter

References:

[1] E. L. Quinn, "Privacy and the new energy infrastructure,"Available atSSRN 1370731, 2009
[2] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj.Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 1(1):1–6, 2012.