A Big Smart Energy Game and A Small Cyber Game

KU Cyber Smart Team

May 23, 2018

Table of Ccontents

Abstract

- We devise security games in a smart energy game-theoretic setting. This yields a nested game which helps predicting attacks.

Notations

- $G = (\mathcal{N}, A, u(t))$
  - $\mathcal{N}$ – players
  - A – schedules
  - u – utility
  - $t = (f, b)$ where f is aggregated forecast, and b is battery states (of all players?)

The Daily Energy Game

- Initialisation
  - Hardware Distribution (smartmeters)
  - Software Distribution (Schedules A)
- Game Preparation
  - 1. Forecasting (expected user demand f is sent to utility company)
  - 2. Price Fixing (utility company decides price and sends info to user – this is u)
- Game Play
  - No communication is required so this is secure provided we can trust users
- Consumption, yields actual demand

Security Assessment

- Critical assets:
  - smart meter hardware and software
  - game-related data (schedules, utility function)
  - communications channels (wireless, cable)
- Our focus:
  - Data, communications channels
  - An attacker modifies the flow of data in Step 1 & 2

Types of Attacks

- Interception
  - all players know each other's energy behaviours
  - an external attacker can learn the energy behaviour of the users by hacking into the smartmeters, or by eavesdropping on the communication channel
- Modification
  - an internal attacker can modify smartmeters to falsify the real behaviour
  - an external attacker can modify the energy behaviour and damage both users and utility company
- Fabrication
  - make up new data
- Interruption
  - any user can corrupt the game by not providing accurate information

Attackers and Attacks

- An attacker might target either the utility company or some users.
- Internal Attacker
  - If the attacker is another user, his goal might be to reduce his cost.
  - Types of attacks:
    - udetectable (structured, unstructured)
    - Detectable
- External Attacker
  - An external attacker is most likely to attack the utility company by perturbing the gameplay and hence destroying its use to the company.
  - Types of attacks?

Nash-Equilibrium Attack (Internal)

- Attacker is one of the players
- He has access to the gameplay equipment
- He can run a perturbed version $G(\epsilon)$ of the game G
- Goal: find ϵ such that the solved perturbed games satisfies:
  - His own consumption reduces
  - The consumption of some others increases
  - This model includes his own increased energy cost to launch this attack (to run the gameplay)
- Case Study (Game by Pilz et al): is vulnerable to this attack (or not?)

Motivation

- There a different possible types of attacks on big games in a smart energy system.
- We would like to use game theory to help deciding what is going on.

Notations

- Utility Company
  - $c^{\mathcal{U}}_{monitor}$ – the cost for monitoring forecast data
  - $c^{\mathcal{U}}_{defend}$ – the cost for monitoring an attack (defense)
  - $l^{\mathcal{U}}_{udetect}$ – the resulting damage for an udetectable attack (could be [detect/udetect] repudation, loss of business)
  - $l^{\mathcal{U}}_{detect}$ – the resulting damage for a detectable attack (could be [detect/udetect] repudation, loss of business)
- Attacker
  - $c^{\mathcal{A}}_{detect}$ – the cost for a detectable attack
  - $c^{\mathcal{A}}_{udetect}$ – the cost for an udetectable attack
  - $l^{\mathcal{U}}_{udetect}$ – the benefit for an udetectable attack
  - $l^{\mathcal{U}}_{detect}$ – the benefit for a detectable attack

Strategies

- Actions for Utility Company
  - Monitor
  - Not monitor
  - $S_{\mathcal{U}} = \{monitor, not\ \ monitor\} = \{s^{\mathcal{U}}_{monitor}, s^{\mathcal{U}}_{not\ \ monitor}\}$
- Actions for the Attacker
  - Detectable attack
  - udetectable attack
  - Not attack
  - $S_{\mathcal{A}} = \{detectable\ \ attack, udetectable\ \ attack, not\ \ attack\} = \{s^{\mathcal{A}}_{detect}, s^{\mathcal{A}}_{udetect}, s^{\mathcal{A}}_{not\ \ attack}\}$

The Game

- Utiliy matrix:

$\mathcal{U} \downarrow \mathcal{A} \rightarrow$	$s^{\mathcal{A}}_{det}$	$s^{\mathcal{A}}_{udet}$	$s^{\mathcal{A}}_{-attack}$
$s^{\mathcal{U}}_{mon}$	$-c^{\mathcal{U}}_{mon} - c^{\mathcal{U}}_{def}, -c^{\mathcal{A}}_{det}$	$-c^{\mathcal{U}}_{mon} - l^{\mathcal{U}}_{udet}, l^{\mathcal{U}}_{udet} - c^{\mathcal{A}}_{udet}$	$-c^{\mathcal{U}}_{mon}, 0$
$s^{\mathcal{U}}_{-mon}$	$-l^{\mathcal{U}}_{det}, l^{\mathcal{U}}_{det} - c^{\mathcal{A}}_{det}$	$-l^{\mathcal{U}}_{udet}, l^{\mathcal{U}}_{udet} - c^{\mathcal{A}}_{udet}$	$0, 0$

- Assumptions:
  - $c^{\mathcal{A}}_{detect} < c^{\mathcal{A}}_{udetect}$
  - $c^{\mathcal{U}}_{monitor} + c^{\mathcal{U}}_{defend} < max(l^{\mathcal{U}}_{detect}, l^{\mathcal{U}}_{udetect})$

Equilibrium Analysis

- This will be done when everyone is happy with the game!

Discussion

- Is the loss for a detectable and an udetectable attack the same ?

References

1 Recent Advances in Local Energy Trading in the Smart Grid Based on Game-Theoretic Approaches, M. Pilz L. Al-Fagih, IEEE Transactions on Smart Grid, DOI: 10.1109/TSG.2017.2764275, 2017

2 Energy Storage Scheduling with an Advanced Battery Model: A GameTheoretic Approach, M. Pilz, L. Al-Fagih E. Pfluegel, Best Paper award at the Int. Research Conf. on Sustainable Energy, Engineering Materials and their Environment, Newcastle, UK, July 2017