Tools and Techniques for Intelligent and Secure Energy Trading | 26 May 2022

Limiting the impact of cyber-attacks in a Multi-Agent based simulation of Local Energy Markets

Rui Andrade

ISEP - GECAD

Outline

CONTEXT AND MOTIVATION

LOCAL ENERGY MARKET

LEMMAS SIMULATION TOOL

CYBER-SECURITY MODULE

CASE STUDY

CONCLUSIONS

Context and motivation

- The energy grid is:
- Powers the modern world:
- Revolutionized:
  - Agriculture
  - Health system
  - Manufacturing
  - Transportation
  - Computer Era

Context and motivation

The need of dealing with the Renewable Energy System

- The EU expects this to be a major change at European level, since it aims at the option for renewable and green energies
- The European Commission forecasts that around 50% of electrical systems in 2030 will be supplied by renewable and sustainable energies

Context and motivation

The need to create systems that support a large amount of energy

- Systems that support large amounts of renewable energy fluctuation, highly distributed by small groups of consumers
- Providing a safe environment for the negotiation
  - Evaluate participants' trust level
  - Ensure that participants provide correct information

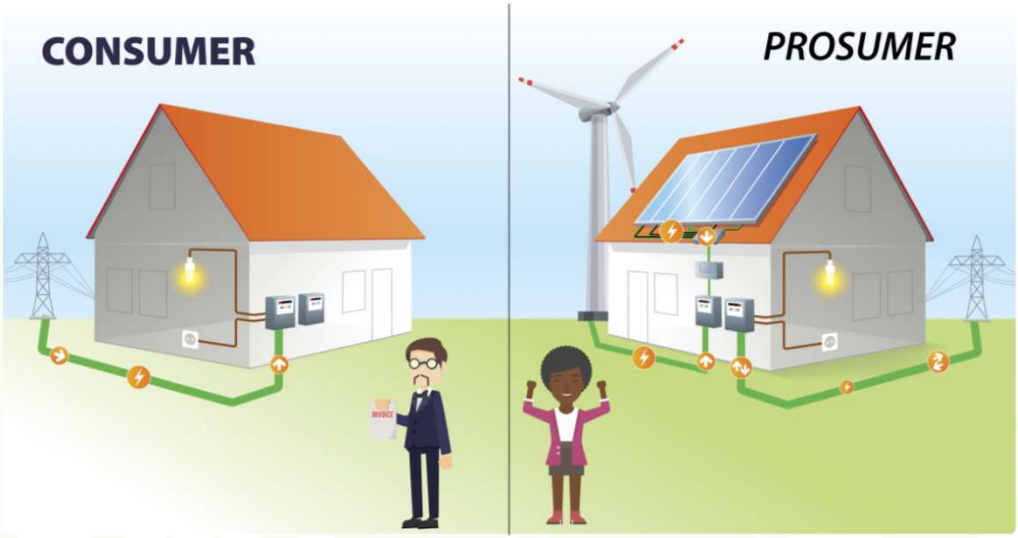
Context and motivation

The need to create systems that support and process this distributed and renewable generation

- Most of these renewable energy systems will be implemented in the homes of consumers
- New market paradigm **Local Energy Market**

Local Energy Market

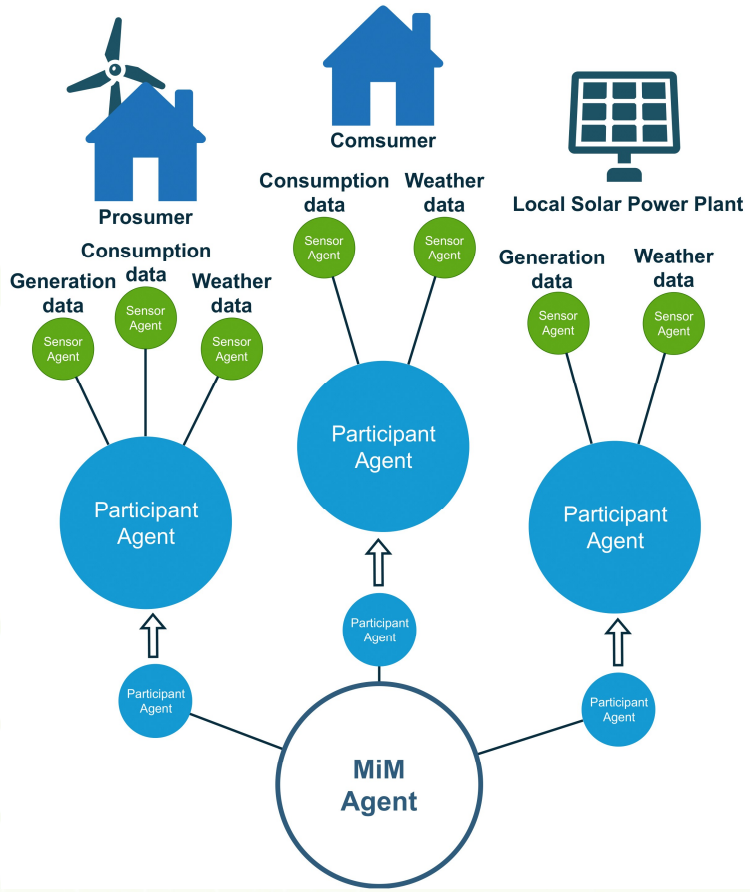
- Reduced physical area, for example a neighborhood
- Participants
  - Consumers
  - Producers
  - Prosumers (consumer with generation)
- Cyber-Physical System



LEMMAS Simulation Tool

Agents

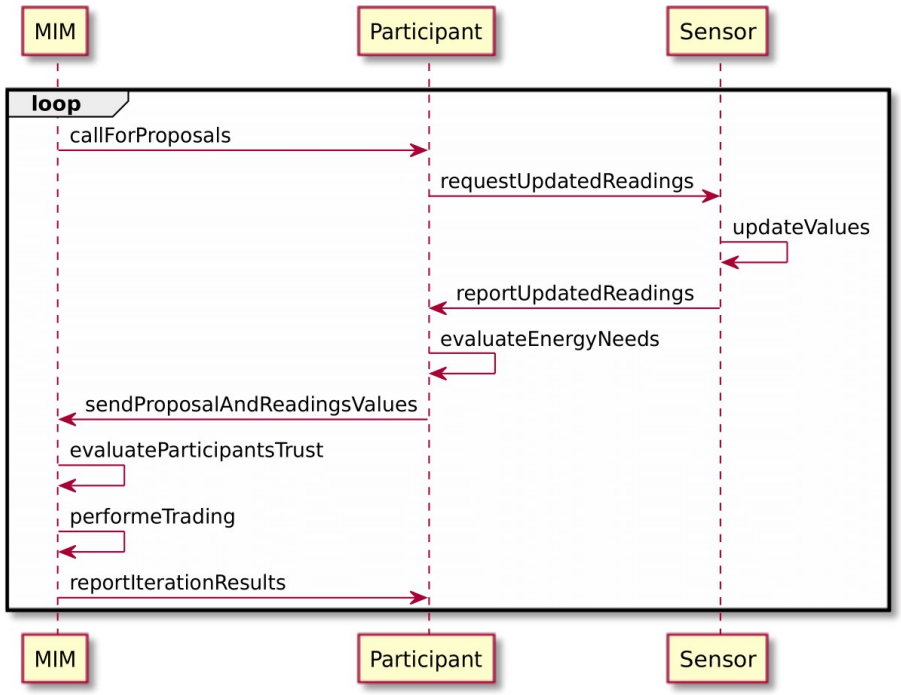
- Sensor agent
- Participant agent
- Market Interactions Manager (MIM)



LEMMAS Simulation Tool

Agents

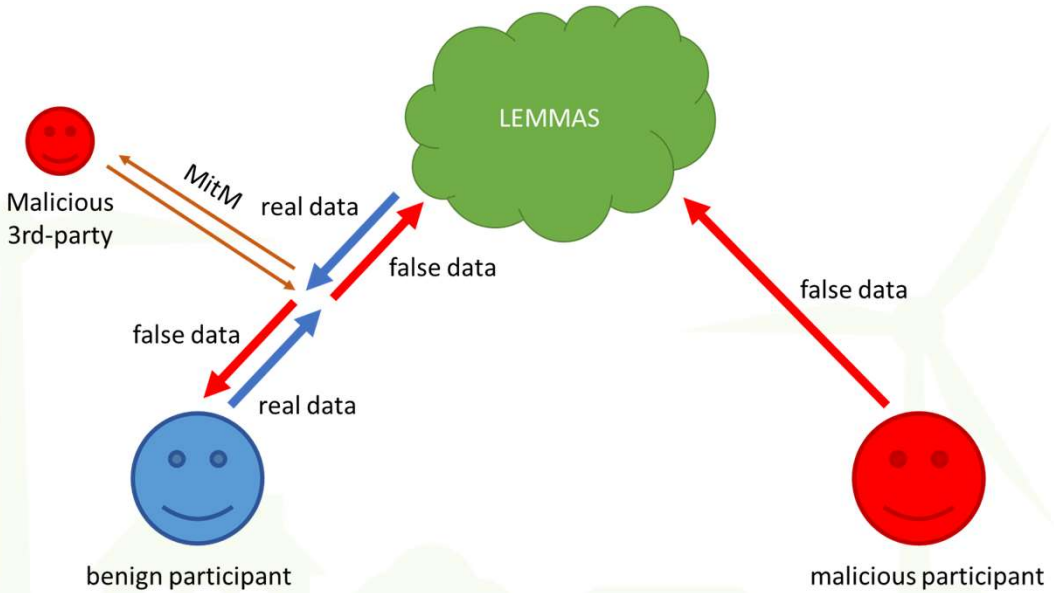
- Sensor agent
- Participant agent
- Market Interactions Manager (MIM)



Challenges in Local Energy Markets

Vulnerable against false data attacks:

- Intentional false submissions by participants
- Man in the Middle attack (MitM)



Trust Module

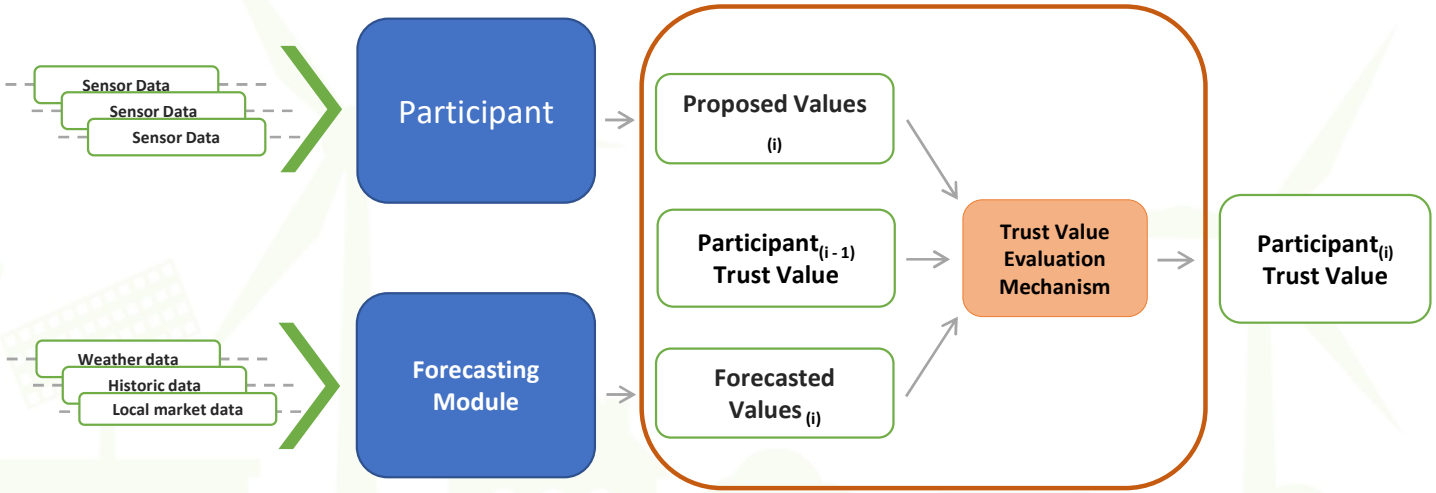
Trust

- Based on E-Comerce
- Institutional Model
  - MIM agent as an institution

Trust Module

- Trust mechanism
- Based on a forecasting
  - Historical data
  - Contextual
  - Weather

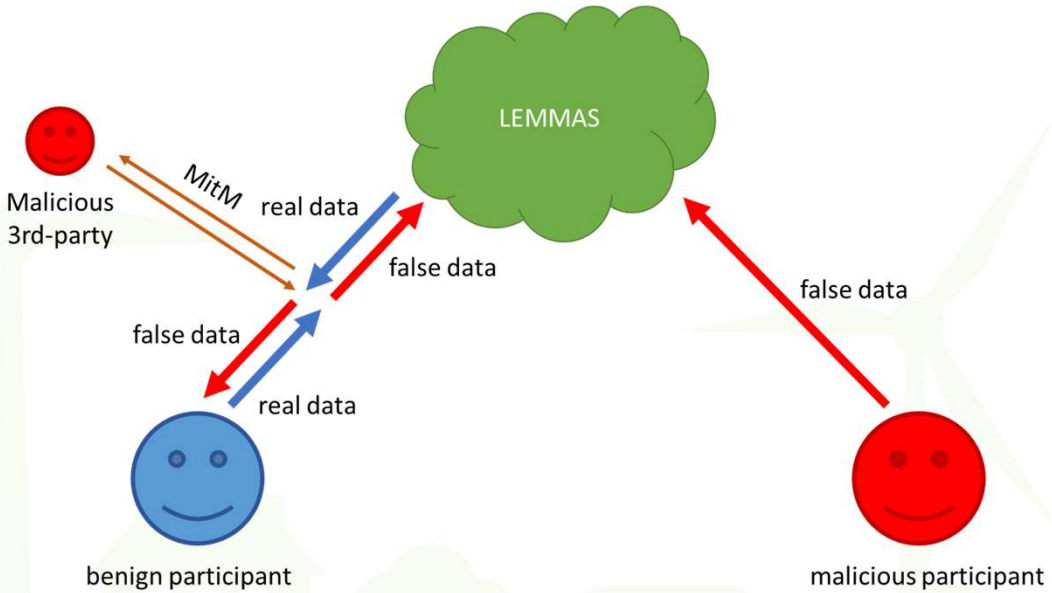
Trust_Score ∈ [0 ,1]



Challenges in Local Energy Markets

Vulnerable against false data attacks:

- Intentional false submissions by participants
- Man in the Middle attack (MitM)



Cyber-Security Module

- Detect particpants under cyber-attack
- Uses ML models trained to detect Cyber-attacks:
  - Support Vector Machine **(SVM)**
  - Extreme Gradient Boosting **(XGB)**
  - Light Gradient Boosting Machine **(LGBM)**

- Analise Network data:
  - duration
  - orig_ip_bytes
  - resp_ip_bytes
  - ...

Cyber-Security Module

- Produces a percentagem confidence value for each possible outcome
- Example:
  - Benign = ? %
  - Attack_1 = ? %
  - Attack_2= ? %
  - …
  - Attack_n = ? %

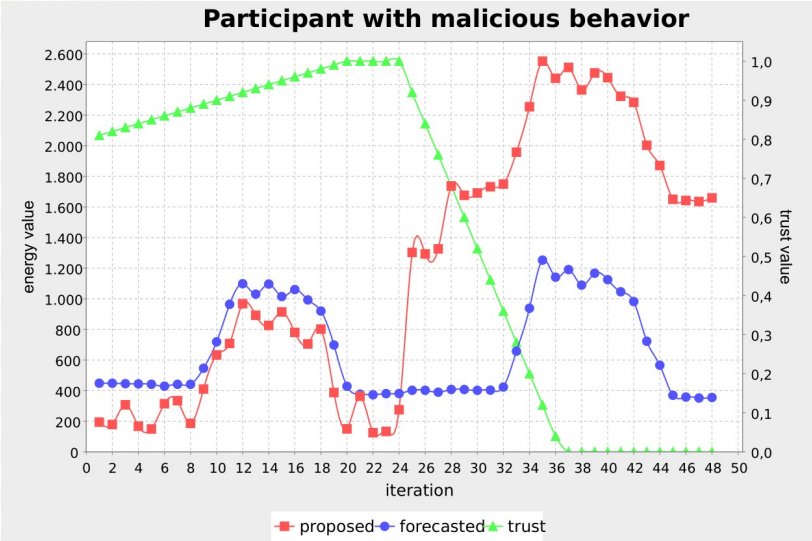
Security_Score = Benign – (Attack_1 + Attack_2 + … + Attack_n)

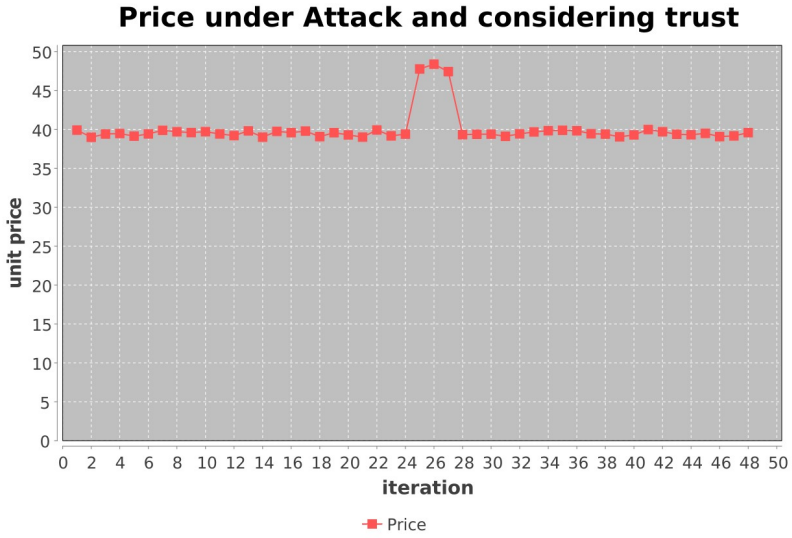
Security_Score ∈ [-1 ,1]

Case Study

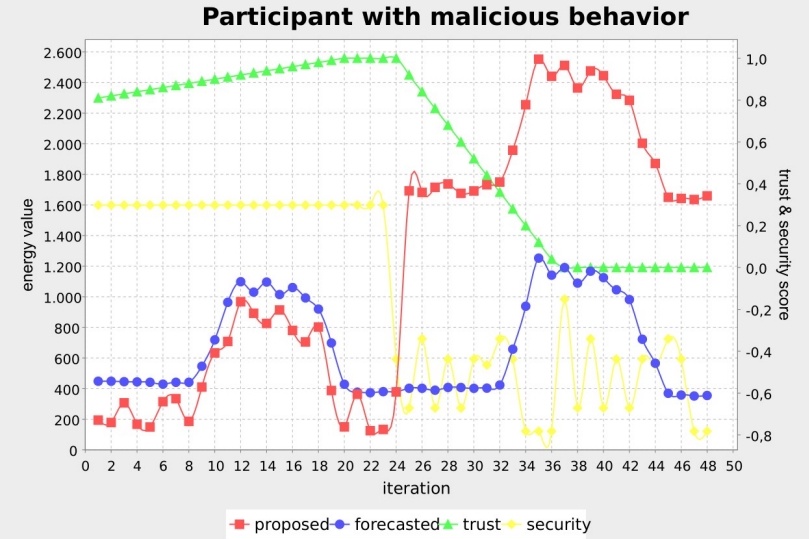
- 16 participants:
  - 13 consumers
  - 3 producers
- Simulated for 48 hours:
  - periods of 1 hour
- 1 participant suffers cyber-attack after the first 24 hours
- Two scenarios to compare:
  - Trust module only
  - Trust module and Cyber-Security module

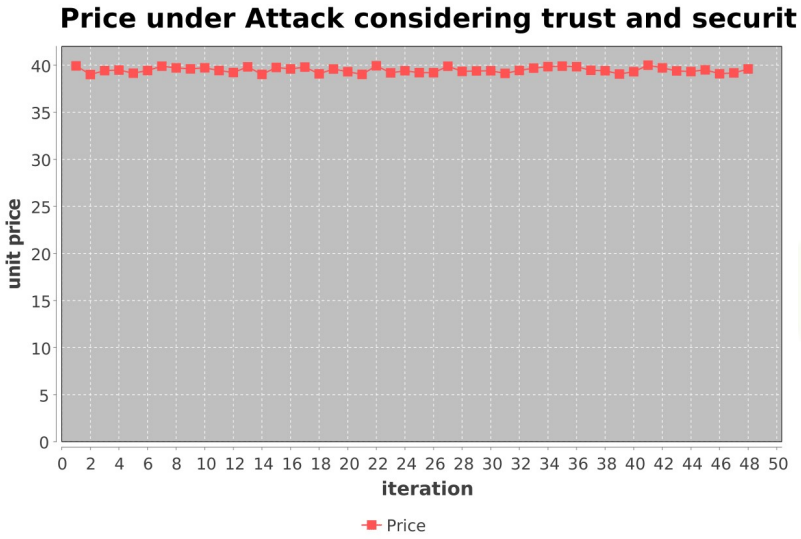
Case Study - Results





Case Study - Results





Conclusions

- Limiting the impact of cyber-attacks is a necessity for the success of the LEM
- Using an Intrusion Detection approach is an effective way to improve the security in the LEM
- The cyber-attack detection model needs to be constantly updated in order to be effective

Thank You ...