processes

MDPI

Article

The Impact of Attacks in LEM and Prevention Measures Based on Forecasting and Trust Models

Rui Andrade *, Isabel Praça *, Sinan Wannous and Sergio Ramos

GECAD—Knowledge Engineering and Decision Support Research Centre, School of Engineering, Polytechnic of Porto (ISEP/IPP), 4200-072 Porto, Portugal; sinai@isep.ipp.pt (S.W.); scr@isep.ipp.pt (S.R.)
* Correspondence: rfaar@isep.ipp.pt (R.A.); icp@isep.ipp.pt (I.P.)

Abstract: In recent years Local Energy Markets (LEM) have emerged as an innovative and versatile energy trade solution. They bring benefits when renewable energy sources are used and are more flexible for consumers. There are, however, security concerns that put the feasibility of the local energy market at risk. One of these security challenges is the integrity of data in the smart-grid that supports the local market. In this article the LEM and the types of attacks that can have a negative impact on it are presented, and a security mechanism based on a trust model is proposed. A case study is elaborated using a multi-agent system called Local Energy Market Multi-Agent System (LEMMAS), capable of simulating the LEM and testing the proposed security mechanism.

Keywords: local energy market; security; forecasting; trust models; multi-agent simulation

check for updates

Citation: Andrade, R.; Praça, I.; Wannous, S.; Ramos, S. The Impact of Attacks in LEM and Prevention Measures Based on Forecasting and Trust Models. *Processes* **2021**, *9*, 314. https://doi.org/10.3390/pr9020314

Academic Editor: Hussain, M.Z.

Received: 26 December 2020
Accepted: 5 February 2021
Published: 8 February 2021

1. Introduction

Energy and power systems play a major role in today's modern society. They are critical infrastructure and, as such, improving and creating better and more reliable systems is a desired goal. A current trend in power systems is the increasing use of renewable energy resources. This shift to greener energy sources can be very beneficial for the environment. However, it creates new challenges for the energy grid and power systems as a whole. To deal with these challenges the Local Energy Market (LEM) is an emergent solution [1] that is being proposed and studied by various authors. Participants in this kind of market tend to be traditional households, small scale energy generation power plants, small industry and households with self generation (prosumers). These participants can be divided into three groups, which are: (i) consumers, (ii) producers and (iii) prosumers.

The Local Energy Market provides more flexibility for consumers and it is better suited to deal with renewable sources of energy. However, the creation of the Local Market comes with challenges of its own. There needs to be a system in place to support energy trading, where the main challenges are cyber-security and Trust in the negotiations. In this paper, we studied the kinds of attacks that jeopardize the local energy markets; and we also studied the mechanisms to mitigate and eliminate some of these possible attacks. These security mechanisms are based on a Trust model [2] that tries to detect participants with malicious activities and forecasting models which provide predictions to be used by the trust model. A case study including 18 participants with different consumption and generation profiles is proposed, and a LEM Multi-Agent simulation framework called (LEMMAS) [2] was used to simulate market trading based on realistic data. The simulation was performed with and without malicious activities, in order to evaluate how the security mechanisms act in the different scenarios.

The remain of the paper is organized as follows. Section 2 contextualizes the LEM and the cyber-security concerns associated with it. Section 3 details the technologies and the implementation of the simulation. Section 4 presents the case study developed as well as the experimental results. Section 5 concludes this article with an overview on the proposed work and discussion of the obtained results.

2. Context

2.1. Local Energy Market

The Local Energy Market (LEM) [3] is a different and innovate energy market model. There is no absolute definition of a LEM, however a general concept can be identified, through the many authors' work of approaching the idea of a LEM. These authors working on this topic have a tendency to divide it in 3 key features: (i) Market structure; (ii) Advantages; (iii) Challenges.

The LEM structure is usually defined as a group of local participants (such as a neighborhood) [1,4,5], which can make energy trading between themselves. In a common local market, there are 3 kinds of participants [5–7]:

- Consumers:who wish to purchase electrical energy;
- Producers: who wish to sell electricity;
- Prosumers: (consumers with some source of energy generation) who wish to purchase and sell electrical energy.

In a LEM, all the participants and the whole underlying electrical smart-grid infrastructure (which is a basis of the LEM) have consumption monitoring sensors, monitoring sensors for generation, energy storage systems and other data sources; as well as network communication technologies to share this information [5,6]. Thus, this energy power grid is defined as a Smart-Grid [1].

A LEM provides the main service of negotiation to its participants. This negotiation is offered as an iterative negotiation processes, where, in regular periods the participants have the opportunity to submit their proposals to buy or to sell energy, and agree on a market price in each period [8].

There are several potential advantages in a LEM when compared to traditional electricity markets. Some authors [1,7] allege that LEM would perform more efficiently than the traditional electrical grids. In the meantime, they affirm that the change to the Local Energy Market (LEM) system would decrease the world's greenhouse effect [1] and would create a more sustainable environment [6,7]. In comparison to traditional markets, in the LEM, participants (especially traditional consumers) are more involved and have a more active role in the market. These participants then are able to trade directly and can obtain energy price reductions or even make profits by participating [1,6,7]. Finally, the fact of the LEM being flexible and versatile makes that LEM and traditional markets can coexist [6,7], then the local market could mold to the needs of each specific community.

The adoption of the LEM at a large scale is being hindered by some challenges, such as security concerns and malicious activities [1]. In its operation the LEM encounters a lot of sensitive information, and there is a need to secure it properly from unauthorized access, and from malicious entities who can interfere with data in order to have some type of profits or financial advantages. For this reason, there is a need for Trust in the Local Energy Market's negotiations. Technical challenges such as the implementation of Smart-Grids, social challenges such as consumers adoption and the lack of adequate legislation are some of the barriers that the LEM faces today [7].

2.2. Security and Cyber-Attacks in Local Energy Markets

The Smart Grid is the physical basis for the LEM, as [4] have identified. Security is critical regarding any energy supply system, particularly for the Smart Grid; and this is an area of active research. There are some parts of the Smart Grid that need special security care, as well as can have potential security vulnerabilities.

A Trust model capable of providing security in negotiations is necessary for the success of LEM. In order to propose a Trust model which can better play its role in the general security, firstly there is a need to understand security as a whole. For any LEM, and Smart Grid, it is very important to have reliable network communication mechanisms; this is pointed as a main security focus [9–11]. The authors' worries due to security in communications are divided into 10 topics by [9]. These topics are the following:

- High Level Security—cyber-security attacks such as Man-in-the-Middle (MitM), Denial of Service (DoS), and others must be defended against;
- Privacy—sensitive information must be kept secure;
- Availability—critical systems and services must avoid down time;
- Integrity—data must not be corrupted or inappropriately modified;
- Authentication—only legitimate participants should have access to the system;
- Authorization—participants should only have access to parts of the system that concern them;
- Auditability—it must be possible to analyze the historical data of the system;
- Non-repudiability—there must be no ambiguity in the origin of data;
- Third-party Protection—the systems must be protected against third-parties;
- Trust—all parts of system must be trustworthy in order for the system as a whole to be trustworthy.

This last point of trust is precisely where the trust model explored in the article focuses. The system as a whole needs to be trusted. And the negotiation process is the central point to secure.

Participation must be real and trustworthy, this is concept of trust in the LEM. Untrustworthy participants are undesirable, because it can influence the market result in a negative way, and should be prevented for participating once identified.

Trust in the LEM negotiations is also connected to several security aspects:

- Participants must be authenticated;
- Participants must be authorized;
- Participation needs to be non-repudiable;
- Integrity of data is needed.

Integrity of data in this context must be addressed from two directions: hardware malfunctions may create incorrect data, and participants themselves may attempt to change data in order to gains a financial benefit. Integrity attacks can take several forms: Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, Man in the Middle (MITM), Time Synchronization, Masquerading and Load-Drop Attacks [12]. All these aspects need to be taken into account when designing a Trust model for this context.

2.3. Forecasting

Forecasting electricity consumption is crucial in the context of energy markets. In order to have a better balance between energy consumption and generation, it is very important to have adequate and reliable models to forecast electrical energy demands. Normally, load forecasting can be divided, according to the prediction horizon, into three main categories: 1 h to 1 week ahead for short-term, 1 month to 1 year ahead for medium-term, and up to 10 years for long-term load forecasting [13]. Furthermore, most common inputs might include multiple historical data, such as: previous consumption values, weather data, and contextual numerical data (hour, day of the week, day of the month, month of the year, year, etc.).

Various Artificial Intelligence (AI) methods can be utilized to forecast energy consumption and generation, primarily supervised machine learning and artificial neural networks (ANN) [14,15].

Murat et al. [16] used ANN techniques to forecast energy demands in the context of transportation. The authors performed a case study containing historical data from 1970 to 2001. The results showed that their model was successful at forecasting in the applied context.

Ahmad et al. [17] reviews the techniques of ANN and Support Vector Machines (SVM) applied to the context of energy forecasting in buildings. The authors conclude that both techniques are capable of delivering good results.

Ahmad et al. [18] compared the Random Forest to ANN in the context of energy consumption forecasting. The results of this work show that both Random Forest and ANN are adequate to apply in energy forecasting problems, and both produce similar results.

3. Technologies and Implementation

In order to adequately simulate the LEM and explore the desired, security detection and attack prevention mechanism, a framework was developed capable of fulfilling this objectives. The framework is separated into 3 major components: (i) a Multi-Agent System (MAS), called Local Energy Market Multi-Agent System (LEMMAS), that simulates the LEM; (ii) a Forecasting tool that provides energy generation and consumption predictions; (iii) and lastly, a Trust tool which takes into consideration the energy predictions and the LEM data in order to evaluate which participants are trustworthy. This framework is illustrated in Figure 1.

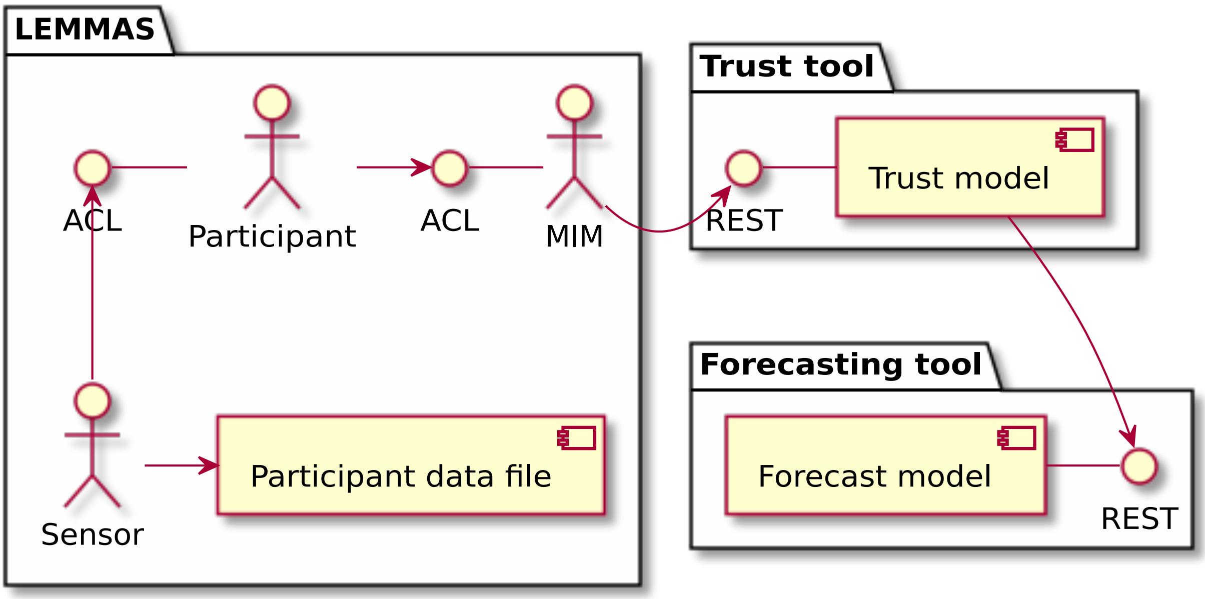


Figure 1. Developed Framework.

3.1. LEMMAS

LEMMAS is a MAS tool developed with the objective of simulating the LEM. In LEMMAS the LEM components are represented as Agents, who are able to communicate among themselves using Agent Communication Language (ACL) messages, as shown in Figure 1. There are 3 kinds of agents:

- MIM—Market Interactions Manager (MIM) is the agent responsible for performing the negotiation as well as interacting with the Trust and Forecasting tools;
- Participant—this agent represents a real market participant. This agent is capable of sending proposals to the MIM in order to negotiate energy according to his needs;
- Sensor—the sensor agent is an intermediary between the real world information collected by sensors or external sources, and the respective participant agent, which in tern uses this information to evaluate his energy needs.

The LEMMAS tool provides a service of negotiation for its participants. This service is offered as an iterative negotiation process, where in each negotiation period each participant can submit proposals to buy or to sell energy. In this tool the negotiation is performed following a double-sided auction [19]. Lastly, proposals submitted by participants deemed untrustworthy by the Trust tool, detailed in Section 3.3, are ignored in order to perform negotiation in a secure environment.

3.2. Forecasting Tool

A Forecasting tool was developed to provide dynamic forecasting services through a RESTful communication protocol. This configurable tool was built in Python using

Scikit-learn [20], and used to compare and build forecasting models using multiple models and historical data sets. It utilizes the following forecasting models:

1. Adaboost.R2;
2. Random Forest;
3. Gradient Boosting Regressor;
4. Support Vector Regressor;
5. Linear Regressor.

Services provided by this tool include:

1. Training Module: to build forecasting models to be used later for forecasting energy consumption;
2. Tuning Module: to tune forecasting models using combinations of input parameters and historical data values;
3. Predicting Module: to predict next values using the model resulting from the training module.

3.3. Trust Tool

The trust model was developed and improved based on a previous work [2].

The objective of the trust module is to ensure that the participant's behavior is trustful and not malicious. Considering the Local Market characteristics, specifically its structure and architecture with a central agent who is responsible for the negotiations. It was opted to apply an institutional trust model, in which the market interactions manager is the responsible for apply the trust model and, in this way, ensure that it is possible to obtain trust and secure negotiations.

This trust model is based on the idea that the normal participant's behavior can be predicted considering a given historical data and contextual data.

The trust model works in the following way: to each participant is attributed a trust value (t_{pi}) in a range between 0 and 1, which is updated in each market negotiation period.

In order to obtain this value the trust module performs an acceptance evaluation between the Submitted Value (sv_{pi}) and the Forecasted value (fv_{pi}).

The trust value for the participant in the current iteration t_{pi} is given by the adding the trust value of the previous iteration ($t_{p(i-1)}$) and the result of the acceptance evaluation between sv_{pi} and fv_{pi}, as is represented in Equation (1). In the case of the first iteration the $t_{p(i-1)}$ is equal to a configurable parameter (t_{p0}).

There are two options to perform the acceptance evaluation, they are: the *asym* Equation (2) and the *sym* Equation (3).

The acceptance evaluation, Equation (2), considers the fv_{pi} and uses it to create an upper limit and a lower limit with the variable acceptance range parameter (vr). If the sv_{pi} is within the limits then sv_{pi} is accepted.

The difference the *asym* Equation (2) and the *sym* Equation (3) is that the values offv_{pi} and sv_{pi} are spawned, and in each given situation either *asym* or *sym* can be chosen depending on which one produces better results.

An improvement over the initial trust formula [2] is the addition of a fixed range parameter (fr), in case vr creates an interval smaller than the one of fr them fr is used. The addition of fr helps to evaluate submissions with low value that could get falsely rejected. With this improvement the Trust model is less likely to falsely label participants with proposals to buy or sell very low amount, or even zero, energy in an iteration.

The acceptance of sv_{pi} results in t_{pi} being equal to $t_{p(i-1)}$ + the Trust Increase Value (tiv) a configurable parameter. In the case of rejection t_{pi} is equal to $t_{p(i-1)}$ + the Trust Decrease Value (tdv) another configurable parameter.

$$t_{pi} = t_{p(i-1)} + trust\_eval(sv_{pi}, fv_{pi}) \tag{1}$$

$$asym(sv_{pi}, fv_{pi}) = \begin{cases} tiv & \text{if } sv_{pi} > fv_{pi} * (1 - vr) \text{ AND } sv_{pi} < fv_{pi} * (1 + vr) \\ tiv & \text{if } sv_{pi} > fv_{pi} - fr \text{ AND } sv_{pi} < fv_{pi} + fr \\ tdv & \text{otherwise} \end{cases} \quad (2)$$

$$sym(sv_{pi}, fv_{pi}) = \begin{cases} tiv & \text{if } fv_{pi} > sv_{pi} * (1 - vr) \text{ AND } fv_{pi} < sv_{pi} * (1 + vr) \\ tiv & \text{if } fv_{pi} > sv_{pi} - fr \text{ AND } fv_{pi} < sv_{pi} + fr \\ tdv & \text{otherwise} \end{cases} \quad (3)$$

When using the Trust formula the parameters of initial trust value t_{p0}, fixed acceptance range fr, variable acceptance range vr, trust increase value tiv and trust decrease value tdv; can be configured, in order to obtain the desired functionality for the scenario in question.

4. Experimental Findings

4.1. Case Study

In order to better understand how this model of Trust and Forecasting can work in a real market, a case study was developed for this purpose. This case study models a Local Energy Market with 18 participants, all with different consumption and generation profiles that were created using real data.

Participants in this case study can be separated into two groups, those who consume energy and those who generate it. Among consumers there are two kinds: "domestic consumers" (households), and "industrial consumers". Each participant has a different amount of historical data to be used by the forecasting algorithms and a specific range of prices that it is willing to accept in the negotiation. The list of participants, the amount of historical data they have and the price ranges they accept are presented in Table 1. This data was gathered from real consumption and generation datasets, and the price range each participant accepts was carefully selected in order to represent a realist scenario. Participants called "domestic consumer" or "industrial consumer" try to buy energy with prices in between their "min bid €/MWh" and their "max bid €/MWh", on the other hand, participants called "generation" try to sell energy with prices in between their "min bid €/MWh" and their "max bid €/MWh". The price ranges were carefully considered and in general buyers have lowers price ranges and sellers have higher price ranges. Each participant tries to maximize his own profits or savings.

Using these participants the negotiation was performed for a 48 h period for 1 h ahead trading.

The simulation was performed in three different Scenarios:

1. the first scenario represents a market performing trading without malicious activities;
2. in the second scenario, one of the markets participants starts sending adulterated proposals after the first 24h in order to influence the market outcome;
3. last scenario is the same as the previous one, however this time the Trust model is used in order to identify and prevent the malicious activities.

The participant caring out the attack increases the amount energy and the accepted price in his bids in order the try to increase the agreed price in the market.

By creating these three scenarios the objective is that the case study represents how a market can be influenced under malicious activities, by comparing the scenarios 1 and 2, as well as exploring how malicious activities may be prevented and defended against by comparing scenarios 2 and 3.

Table 1. Case Study participant's profiles.

Name	Days for Forecasting	Min Bid €/MWh	Max Bid €/MWh
domestic consumer 1	9	34	46
domestic consumer 2	4	34	46
domestic consumer 3	9	36	48
domestic consumer 4	18	36	48
domestic consumer 5	8	38	48
domestic consumer 6	440	38	48
domestic consumer 7	1	38	50
domestic consumer 8	8	38	50
domestic consumer 9	8	40	50
domestic consumer 10	23	40	50
domestic consumer 11	2477	34	46
domestic consumer 12	62	36	48
industrial consumer 1	1393	36	50
industrial consumer 2	1393	34	48
industrial consumer 3	1393	34	48
generation 1	342	40	52
generation 2	3	42	52
generation 3	3	40	52

Each participant in the simulation had a file such as the one exemplified in Table 2.

Table 2. Participant's file example.

day_m	month	hour	year	day_w	temp	prev_1	prev_2	prev_3	value	buy	sell
01	03	02	2018	4	5	458.21	473.68	453.51	450.60	41.14	0
01	03	03	2018	4	5	450.60	458.21	473.68	446.67	42.17	0
01	03	04	2018	4	5	446.67	450.60	458.21	428.78	42.64	0
01	03	05	2018	4	5	428.78	446.67	450.60	443.11	40.66	0

Each column in this file represents different information that is used in the simulation:

- "day_m"—day of the month in this period;
- "month"—month in this period;
- "hour"—hour in this period;
- "year"—year in this period;
- "day_w'—day of the week in this period;
- "temp"—temperature in participant's location this period;
- "prev_1"—participant's consumption or generation in the previous period;
- "prev_2"—participant's consumption or generation two periods ago;
- "prev_3"—participant's consumption or generation three periods ago;
- "value"—participant's amount of energy proposed to buy or sell;
- "buy"—participant's price bid to buy energy;
- "sell"—participant's price bid to sell energy.

The "value" column represents the amount of energy in the proposal and the columns of "buy"/"sell" determine if it is a proposal to buy or sell energy depending on which one has a non-zero value. A row with values of "buy" and "sell" both different from zero would create an invalid file as a participant can not be both buying and selling energy in the same iteration.

The columns of "day_m", "month", "hour", "year", "day_w", "value", and "buy" or "sell" were used to create the proposals in each negotiation iteration.

The Trust and Forecasting modules also make use of the participant's file information. The values of "day_m", "month", "hour", "year", "day_w", "temp", "prev_1", "prev_2" and "prev_3" are used by the Forecasting module to predict the participant proposal in each iteration. With trustworthy participants it is expected for the Forecasting module to make a prediction equal or very close to the "value" for the iteration. The resulting prediction is the input to the Trust model, which updates the Trust value for the participant for the current iteration.

LEMMAS system was used to simulate this market. The Trust tool in conjunction with the Forecasting tool, was used to evaluate the trustworthiness of participants. The parameters for the Trust formula were chosen as: $t_{p0} = 0.8$, $fr = 10$, $vr = 0.3$, $tiv = 0.01$, $tdv = -0.08$; and sym acceptance formula was used. The Forecasting tool was used to train a prediction model for each participant before starting the market simulation; and then, in each iteration of the simulation, predict the amount of energy each participant was proposing to buy or sell. This proved to be the best configuration for the scenarios tested.

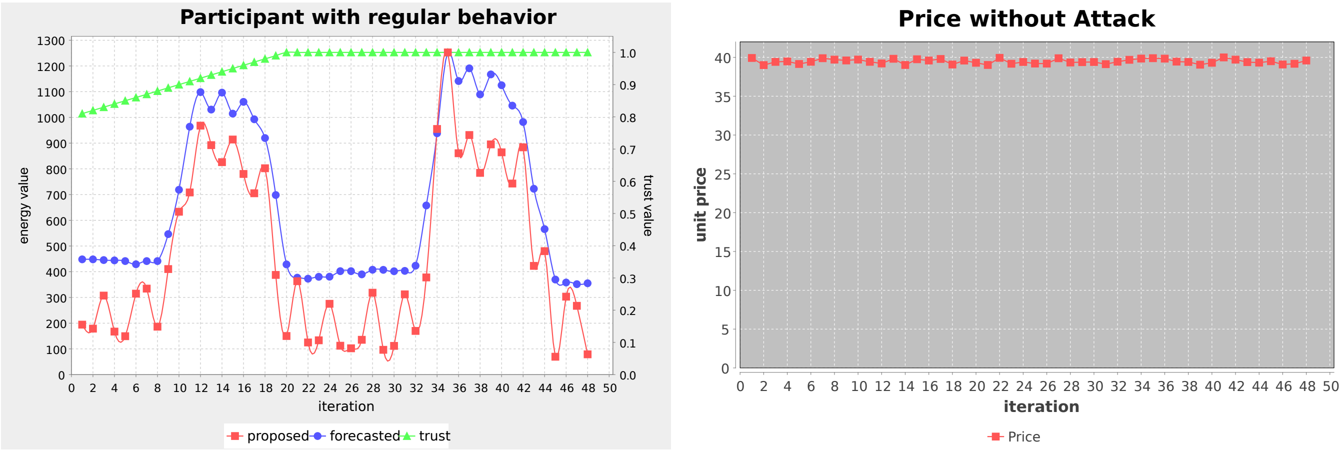
4.2. Results

The three scenarios were simulated in LEMMAS and for each negotiation iteration the: energy amount submitted in the proposal, energy amount forecasted and the trust value attributed to the participant performing the attack was recorded as well as the price agreed in each iteration. In order to visualize the results of this case study were plotted in 3 sets of charts (Figures 2–4) are included bellow, each one representing one of the Scenarios previously described.

Scenario 1 clearly shows a participant with a regular and expected behavior classified with a high trust value and a market with a stable price.

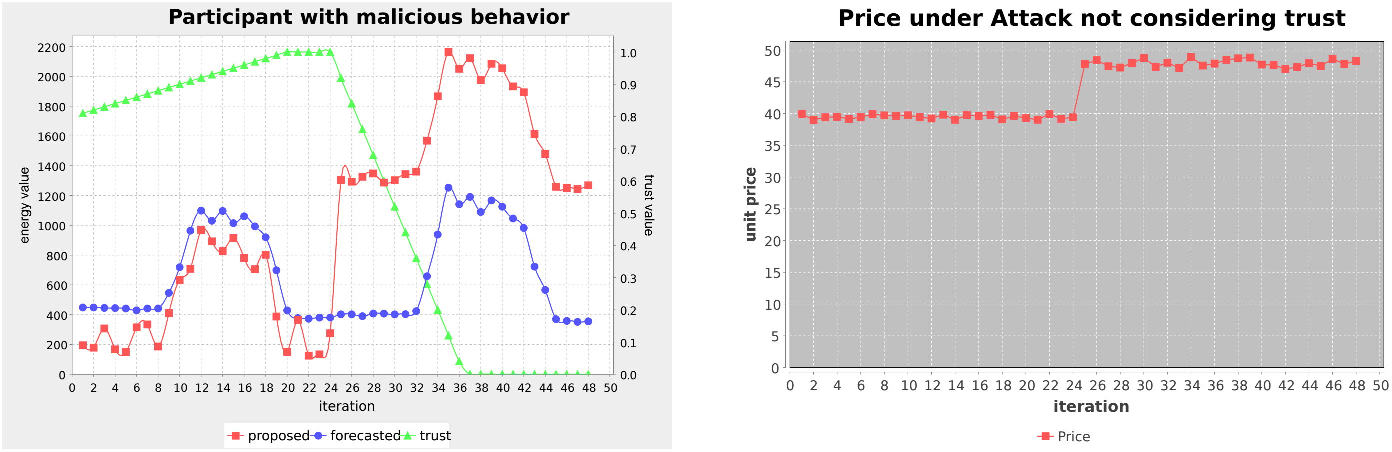
In the second scenario the participant began his attack after the first 24 h and as shown there is a visible disparity between his expected behavior predicted by the Forecasting model and the participants proposals. This resulted in receiving low trust scores repeatedly until hitting 0. However, this trust score is not being considered in the market and participants were successfully able to influence the price for the last 24 h.

In this final scenario the participant exhibits the same behavior as in the previous scenario and receives the same low trust value by the Trust and Forecast models. This time however market is performing the negotiations considering the trust scores of the participants and as shown in Figure 4 after only 3 market iterations the participant's trust value became sufficiently low as to exclude him from negotiating, returning the market to a regular and secure environment, as it was in scenario 1.



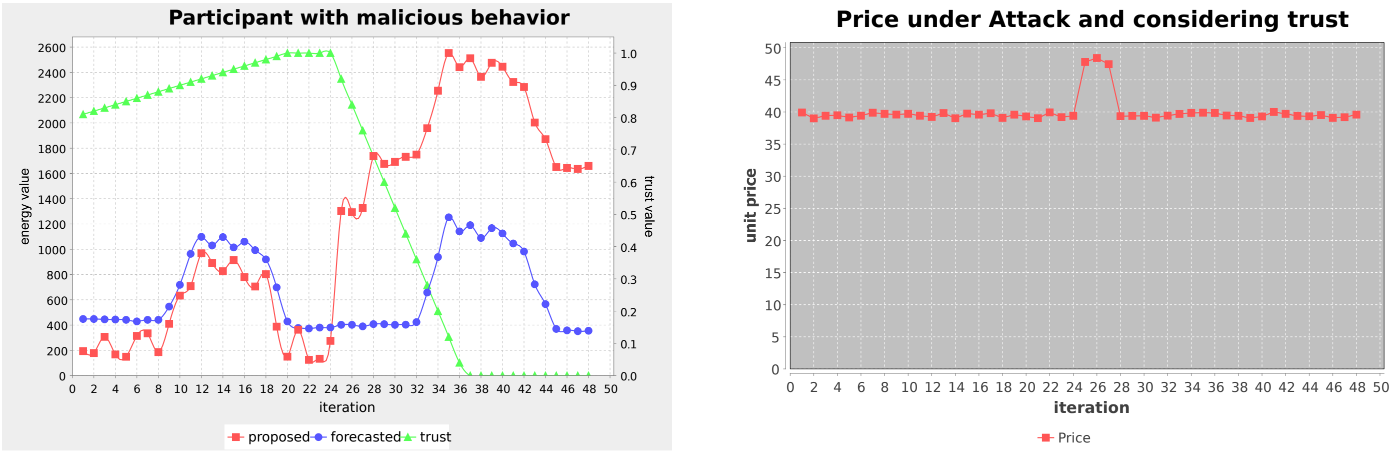
(**a**) (**b**)

Figure 2. Scenario 1. (**a**) Participant evaluation without attack; (**b**) Agreed price without attack.



(**a**) (**b**)

Figure 3. Scenario 2. (**a**) Participant evaluation with attack (not considering Trust); (**b**) Agreed price with attack (not considering Trust).



(**a**) (**b**)

Figure 4. Scenario 3. (**a**) Participant evaluation with attack (considering Trust); (**b**) Agreed price with attack (considering Trust).

5. Conclusions

This work explored the emergent Local Energy Market as well as the security threats and concerns that are associated with it. This kind of Market is better designed to take advantages of renewable energy sources and is flexible enough to the point of being able to coexist with the current power systems and energy power grids.

There are, however, several security concerns that need to be addressed before the LEM can be successfully deployed at a larger scale. These security issues can assume many forms, in this work the specific problem of data being tampered with is addressed.

A Trust model is explored based on combining a trust formulation and forecasting models. The resulting Trust model was tested in a framework, called LEMMAS, developed to simulate the LEM as Multi-Agent System.

A case study was developed using the framework. The case study simulated three scenarios in a realistic LEM with 18 participants for 48 h of negotiation. The first scenario did not included malicious activities while the second and third did so. The difference from the second and the third scenarios was that in the third scenario the trust model was used in order to prohibit untrustworthy participants to access the market. The results show that when the Trust model was used it was possible to identify the malicious activities in only 3 iterations and the market returned to a normal negotiation as it was in scenario 1. While scenario 2 was under influence of malicious activities during the negotiation.

This approach is not totally foolproof; however, it is clearly better that an unprotected market. This protection model should not be used alone either. It should be combined with other security mechanisms that may hopefully prevent tampering with data in the first place. Furthermore, if such other security measure fail a security measure based on forecasting and Trust, the one here presented shall be a welcomed second line of defence to prevent further damage once the attack is detected.

Author Contributions: Conceptualization, R.A. and S.W.; methodology, R.A. and S.W.; data curation, R.A; formal analysis, R.A; funding acquisition, I.P. and S.R.; investigation, R.A and S.W; validation, I.P., S.R. supervision, I.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from FEDER Funds through COMPETE program and from National Funds through FCT under the project SPET–PTDC/EEI-EEE/029165/2017 and UIDB/00760/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Abidin, A.; Aly, A.; Cleemput, S.; Mustafa, M.A. *Towards a Local Electricity Trading Market Based on Secure Multiparty Computation*; 2016. Available online: https://www.esat.kuleuven.be/cosic/publications/article-2664.pdf (accessed on 7 February 2021).
2. Andrade, R.; Pinto, T.; Praça, I. Trust Model for a Multi-agent Based Simulation of Local Energy Markets. In Proceedings of the International Conference on Practical Applications of Agents and Multi-Agent Systems, Seville, Spain, 1–3 June 2020; pp. 183–194.
3. Praça, I.; Ramos, S.; Andrade, R.; da Silva, A.S.; Sica, E.T. Analysis and Simulation of Local Energy Markets. In Proceedings of the 2019 16th International Conference on the European Energy Market (EEM), Ljubljana, Slovenia, 18–20 September 2019; pp. 1–5.
4. Bremdal, B.A.; Olivella, P.; Rajasekharan, J. EMPOWER: A network market approach for local energy trade. In Proceedings of the 2017 IEEE Manchester PowerTech, Manchester, UK, 18–22 June 2017; pp. 1–6. [CrossRef]
5. Ampatzis, M.; Nguyen, P.H.; Kling, W. Local electricity market design for the coordination of distributed energy resources at district level. In Proceedings of the Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES, Istanbul, Turkey, 12–15 October 2014; pp. 1–6.
6. Teotia, F.; Bhakar, R. Local energy markets: Concept, design and operation. In Proceedings of the Power Systems Conference (NPSC), 2016 National, Odisha, India, 19–21 December 2016, pp. 1–6.
7. Mendes, G.; Nylund, J.; Annala, S.; Honkapuro, S.; Kilkki, O.; Segerstam, J. Local energy markets: Opportunities, benefits, and barriers. In Proceedings of the CIRED 2018 Ljubljana Workshop on Microgrids and Local Energy Communities, Ljubljana, Slovenia, 7–8 June 2018.
8. Etukudor, C.; Couraud, B.; Robu, V.; Früh, W.G.; Flynn, D.; Okereke, C. Automated negotiation for peer-to-peer electricity trading in local energy markets. *Energies* **2020**, *13*, 920. [CrossRef]
9. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Cyber Security for Smart Grid Communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
10. Ericsson, G.N. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. *IEEE Trans. Power Deliv.* **2010**, *25*, 1501–1507. [CrossRef]
11. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
12. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
13. Raza, M.Q.; Khosravi, A. A review on artificial intelligence based load demand forecasting techniques for smart grid and buildings. *Renew. Sustain. Energy Rev.* **2015**, *50*, 1352–1372. [CrossRef]
14. Antonopoulos, I.; Robu, V.; Couraud, B.; Kirli, D.; Norbu, S.; Kiprakis, A.; Flynn, D.; Elizondo-Gonzalez, S.; Wattam, S. Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review. *Renew. Sustain. Energy Rev.* **2020**, *130*, 109899. [CrossRef]
15. Jain, A.K.; Mao, J.; Mohiuddin, K.M. Artificial neural networks: A tutorial. *Computer* **1996**, *29*, 31–44. [CrossRef]
16. Murat, Y.S.; Ceylan, H. Use of artificial neural networks for transport energy demand modeling. *Energy Policy* **2006**, *34*, 3165–3172. [CrossRef]
17. Ahmad, A.S.; Hassan, M.Y.; Abdullah, M.P.; Rahman, H.A.; Hussin, F.; Abdullah, H.; Saidur, R. A review on applications of ANN and SVM for building electrical energy consumption forecasting. *Renew. Sustain. Energy Rev.* **2014**, *33*, 102–109. [CrossRef]

18. Ahmad, M.W.; Mourshed, M.; Rezgui, Y. Trees vs Neurons: Comparison between random forest and ANN for high-resolution prediction of building energy consumption. *Energy Build.* **2017**, *147*, 77–89. [CrossRef]

19. El-Baz, W.; Tzscheutschler, P.; Wagner, U. Integration of energy markets in microgrids: A double-sided auction with device-oriented bidding strategies. *Appl. Energy* **2019**, *241*, 625–639. [CrossRef]
20. Pedregosa, F.; Varoquaux, G.; Gramfort, A.; Michel, V.; Thirion, B.; Grisel, O.; Blondel, M.; Prettenhofer, P.; Weiss, R.; Dubourg, V.; et al. Scikit-learn: Machine learning in Python. *J. Mach. Learn. Res.* **2011**, *12*, 2825–2830.