Poster: SNIPPET – Secure and Privacy-Friendly Peer-to-Peer Electricity Trading

Aysajan Abidin*, Raf Callaerts†, Geert Deconinck‡, Shenja van der Graaf§, Akash Madhusudan*, Mehdi Montakhabi§, Mustafa A. Mustafa‖*, Svetla Nikova*, Domenico Orlando¶, Jessica Schroers¶, Simon Vanhove†, and Fairouz Zobiri‡
*imec-COSIC, KU Leuven, Belgium
†IEEL, KU Leuven, Belgium
‡ELECTA, KU Leuven, Belgium
§imec-SMIT, Vrije Universiteit Brussel, Belgium
¶Centre for IT & IP Law and imec, KU Leuven, Belgium
‖Department of Computer Science, The University of Manchester, UK

***Abstract*—Peer-to-peer electricity markets allow users to trade electricity among themselves thereby increasing their financial well-being. However, such markets also create opportunities for malicious players to misbehave in order to maximise their profits. Potential threats are impersonation, data manipulation, disputes and privacy breaches; users' bids are closely correlated to their consumption patterns, which may reveal sensitive information. In this poster, we present work in progress to design a number of technical solutions (i.e., bid/offer creation, strategic bidding, market clearance, settlements, billing, dispute resolutions) to facilitate secure and privacy-friendly peer-to-peer electricity trading. The designed solutions will have limited (or no) impact on the grid, be compliant with the relevant legislation, and serve the existing (and new) market players' interests even if they might have disruptive effect on the current energy value network chain.**

I. Introduction

Smart grid enables bi-directional data communication as well as electricity flows between different components and entities, aiming to make the power system more efficient and reliable. A key smart grid component is the smart electricity meter – devices installed at customer premises that measure and send various metering data at sub-hour intervals, e.g., every 15-30 minutes. This enables decentralised peer-to-peer (p2p) electricity trading markets – a potentially game-changing application – that allow users to trade electricity among themselves (via trading platforms), rather than buying from or selling to only their suppliers – centralised third parties.

However, such p2p markets require complex interactions and data exchanges among various existing and new market players, inevitably introducing several issues. Considering the time and computational constraints of the market operations, as well as the interconnectedness and interdependence between different market players, ensuring secure data exchanges in p2p markets is not trivial. Entities need to authenticate each other and be assured of the integrity of the messages they receive. Similarly, ensuring that personal data of users are not revealed to any ineligible party is not straightforward [1]. Examples of personal data are users' names, addresses, electricity consumption, preferences, monthly bills, etc. All these are sensitive data, as for example, from users' bids one can learn their consumption patterns, which in turn reveal their behaviour, or other sensitive information, such as by combining data to expose circumstances relating to personal health. The same applies to commercially sensitive data, such as which customers of a given supplier trade how much electricity on the p2p market. Moreover, local trading increases the range of stakeholders involved in managing energy transactions, necessitating research into the application of centralised regulatory regimes such as European data protection law and network and information security law, on dispersed stakeholders with varying responsibility. In addition, combining market objectives (maximise profits) with technical objectives (respect grid constraints, optimise grid usage) is not trivial. P2p electricity trading might also be disruptive, leading to changing roles of different stakeholders and appearance of new players. Current legal frameworks do not support p2p electricity trading, which raises the question to what extent changes in the legal framework are necessary.

We report on work in progress under the SNIPPET project[1] that brings together state-of-art in security and privacy for smart grid, empowers consumers to maximally use green energy locally, and is within current/future regulatory boundaries.

II. Preliminary Results

A. Value Network Mapping, Business and Legal Analysis

We deployed business model matrix analysis to develop four future scenarios based on customers' information ownership and citizens' level of involvement as sources of uncertainty in the future [2]: (S1) Direct peers – active citizens and direct customer ownership, involving only prosumers as a new role; (S2) Direct customers – passive citizens with direct customer ownership, involving prosumers and representatives as new roles; (S3) Indirect customers – passive citizens with intermediated customer ownership, involving prosumers, representatives, and brokers as new roles; and (S4) Indirect peers – active citizens with intermediated customer ownership, involving prosumers and brokers as new roles.

This led to identification of two new roles in the electricity market: broker and representative. Broker (platform) is an intermediate actor which facilitates (i.e., supports prosumers to perform) trading in peer-to-peer electricity markets. It

[1] https://www.esat.kuleuven.be/cosic/project/snippet/

has access to information of all involved parties and their transactions. Representatives (home energy system providers) represent their clients (i.e., prosumers) in electricity markets (including the p2p electricity markets). To do so, they manage their clients' assets (i.e., battery, solar panels, flexibility) and information. In other words, they transform passive citizens to active players in the market. Amongst the current market players, aggregators seem to be well-positioned for this role.

In terms of legal analysis, both of the emerging roles act as intermediaries to facilitate market participation of prosumers. Firstly, the broker can be qualified as an interface between the user and the market. Such an activity can be performed by electricity customers either jointly acting or an energy community. In principle, a group of customers can be considered 'jointly acting' if they are located on the same premises. Generally, this association would not be organised as a separate legal entity. In contrast, a citizen energy community is a legal person, with stricter membership and control requirements (art. 16 Electricity Directive [3]). Secondly, the representative is an agent of the user, to which control over user's assets is delegated. The representative enjoys a mandate to trade electricity (and flexibility) on behalf of the user on the energy markets. Such a function could be taken up by an aggregator. Based on the available information of multiple users, an aggregator can trade electricity loads and remunerate prosumers correspondingly.

B. Security, Privacy and Data Protection Analysis

Electricity data may encompass a wide array of types of data: names, addresses, account number, smart meter ID/IP address, consumers' profile, billing data, electrical appliances, generation and storage devices, production, consumption (load graphs), messages' metadata, kind of data (metering or tampering alert). These data do often fall under the definition of 'personal data' under the General Data Protection Regulation (GDPR). Personal data are qualified by Article 4.1 GDPR as "any information relating to an identified or identifiable person". The identification can be direct or indirect. It is fair to say that representatives and brokers, as providers of services different from electricity production, distribution or metering, would be classified as Energy Service Companies.

The activity of representatives and brokers as envisaged could, if operated by third parties, add more than one layer between the customers and the actors in charge of distribution and transportation of electricity, themselves data controllers for different activities and purposes. Such a plurality of data controllers could be an inconvenience, generating fragmentation and confusion in the data subjects willing to advance their legitimate requests. To this would also be added a constant stream of information regarding data protection from a number of firms. Since the broker has information about all users participating in the trading market, the broker can be a single point of failure. Hackers may target the broker to steal users' information. As users share their information with their representatives, they might act as a semi-honest adversary – use the information about users and their buying or selling history to deduce even more, potentially sensitive, information about them. Representatives may also attempt to target each other to be able to attract more users to represent. Users could aggregate their supply/demand bids and provide only the aggregate bids to their representatives. As there is no direct link between the users and the broker, and if the representatives submit only aggregate bids to the broker, the broker should not be able to infer any user information. As the broker is capable of doing inference attacks on the users by analysing their bids/offers, it should use secure computation techniques such as homomorphic encryption and multiparty computation (as in [4], [5]) to perform operations (e.g., bid-to-offer matching) in a privacy-friendly way.

III. Future Research

Privacy-friendly optimal bidding strategies: design optimal bid-and-offer computation algorithms and strategies taking into account heterogeneous flexibility sources (thermostatically controlled loads, electric vehicles, batteries) and renewables, respecting users' comfort constraints and preferences. Such strategies optimally will combine flexibility in time (e.g., minimal user cost) and in space (e.g., minimal grid impact), allowing local (privacy-friendly) multi-objective optimisation.

Privacy-friendly market operation: design secure and privacy-friendly protocols for p2p electricity trading taking into account the many complex interactions and data exchanges among various market players which have different (usually contradicting) privacy requirements, computational capabilities and time requirements. These operations include: market clearance (bid submission, bid-to-offer matching), dispute resolutions, settlements and billing. For the market clearance operation, techniques for operating on encrypted data such as homomorphic encryption and multiparty computation (building on preliminary results [4]–[6]) seem to be suitable candidates. Whereas for settling and billing, smart contracts and distributed ledgers [7] seems to be an appropriate way to go.

Acknowledgment

This work was supported in part by the Research Council KU Leuven: C16/15/058 and by the Flemish Government through FWO SBO project SNIPPET S007619. Mustafa A. Mustafa is funded by the Dame Kathleen Ollerenshaw Fellowship awarded by The University of Manchester.

References

[1] M. A. Mustafa, S. Cleemput, and A. Abidin, "A local electricity trading market: Security analysis," in *PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2016, pp. 1–6.

[2] M. Montakhabi, A. Madhusudan, S. van der Graaf, A. Abidin, and M. A. Mustafa, "Sharing economy in future electricity markets: Security and privacy analysis," in *Proc. of Workshop on Decentralized IoT Systems and Security (DISS), in conjunction with NDSS*, 2020, pp. 1–6.

[3] "Directive (eu) 2019/944 of the european parliament and of the council of 5 june 2019 on common rules for the internal market for electricity and amending directive 2012/27/eu."

[4] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An MPC-based privacy-preserving protocol for a local electricity trading market," in *15th Int. Conf. on Cryptology and Network Security (CANS 2016)*, ser. LNCS, vol. 10052. Springer, 2016, pp. 615–625.

[5] ——, "Secure and privacy-friendly local electricity trading and billing in smart grid," *CoRR*, vol. abs/1801.08354, 2018. [Online]. Available: http://arxiv.org/abs/1801.08354

[6] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, "A secure and privacy-preserving protocol for smart metering operational data collection," *IEEE Trans. on Smart Grid*, vol. 10, no. 6, pp. 6481–6490, 2019.

[7] A. Madhusudan, I. Symeonidis, M. A. Mustafa, R. Zhang, and B. Preneel, "Sc2share: Smart contract for secure car sharing," in *Int. Conf. on Information Systems Security and Privacy (ICISSP)*, 2019.

@snippet_project

SNIPPET: Secure and Privacy-Friendly Peer-to-Peer Electricity Trading

Aysajan Abidin, Raf Callaerts, Geert Deconinck, Shenja van der Graaf, Akash Madhusudan, Mehdi Montakhabi, Mustafa A. Mustafa, Svetla Nikova, Domenico Orlando, Jessica Schroers, Simon Vanhove, and Fairouz Zobiri

Motivation

Alice has a solar panel and generates her own electricity. ☺

When she needs some extra electricity, she buys it from her supplier for **0.20 €/kWh**, but when she has some extra, she can sell it only to her supplier for only **0.05 €/kWh**. ☹

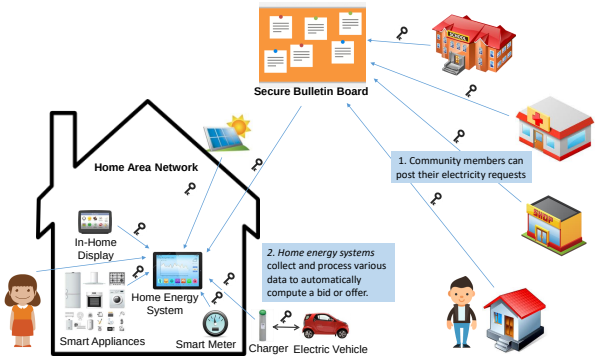
Alice prefers to **help** her **local community** – donate electricity to local hospitals for **free**, or sell it to her neighbour Bob for **0.05 €/kWh** (or more), rather than to her supplier.

Aim

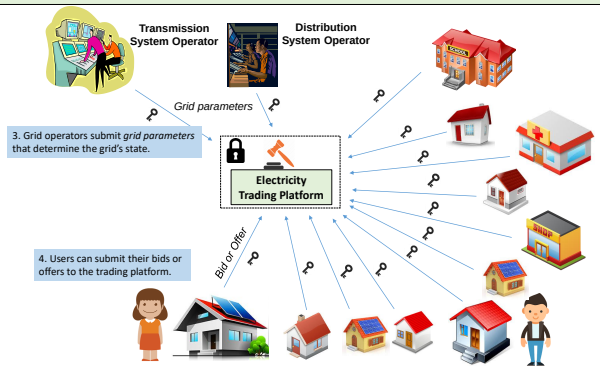
We aim to design a peer-to-peer electricity trading market that is:

- **Flexible** – users can choose with whom and when to trade;
- **Adaptable** – user bids/offers change according to user preferences and market conditions; market output changes according to user bids/offers as well as grid constraints and market conditions;
- **Secure** – transparent, verifiable and auditable market clearance, settlements and billing as well as dispute resolution mechanisms;
- **Privacy-friendly** – no one has access to users' bids and offers (except for the involved users);
- **Usable** – everything is automated.

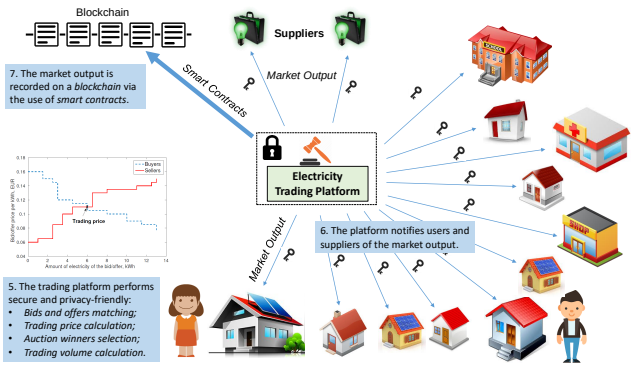
Step 1. Bid and Offer Creation



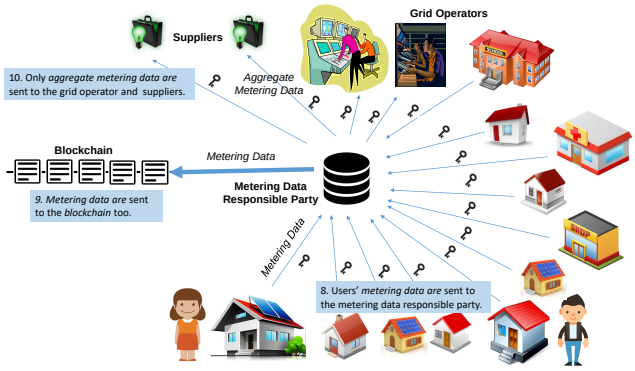
Step 2. Strategic Bidding



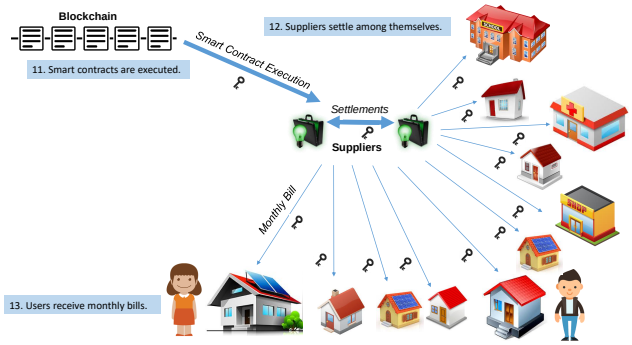
Step 3. Market Clearance



Step 4. Metering Data Distribution



Step 5. Settlements and Billing



Project Partners and Acknowledgements

This work was supported in part by the Flemish Government through FWO SBO project SNIPPET S007619.

Mustafa A. Mustafa is funded by the Dame Kathleen Ollerenshaw Fellowship awarded by The University of Manchester.