Privacy-friendly Multi-Agent Trading Systems for Smart Grid Application

Student: Kamil Erdayandi Supervisor: Dr. Mustafa Mustafa

Research Group: Information Management Group

- Major electricity producers and retailers have the leverage to offer better prices with non-intermittent energy supplies compared to Renewable Energy Sources.
- In order to encourage the usage of RES; local electricity producers should be able to sell their excess at a higher price than the currently offered feed-in tariffs, and at the same time, consumers should be able to buy their needed electricity from local RES owners with lower price than retail price.
- Smart grids support bi-directional electricity and communication flows. Thus, with the trading mechanisms implemented in smart grids; RES owners, using Multi-Agent optimisation techniques can collaboratively or individually maximize their profits and reduce their electricity bills by selling excess electricity to other users with a price lower than retail but higher than back grid price.
- However, these trading mechanisms may also allow malicious entities to misbehave to maximise their profits. This situations may create privacy risks in which private information of the users may be leaked.

Literature View

- Trading algorithms in smart grids have been extensively studied but without concerning any security or privacy issues [1].
- There exist privacy preserving solutions in smart grids. However these privacy preserving techniques can not be applied to multi agent energy trading [2,3].
- Although privacy preserving double auction trading algorithms have been studied well in [4,5], privacy preserving game theoretical trading algorithms have not extensively been studied yet

Research Problem

- Hence; We plan to design a privacy friendly multi-agent trading system using game theoretical approach.
- The trading market has to be secure in order to prevent malicious entities manipulating the market to reduce their costs and their profits.
- First of all, a trading platform will be designed that fits with secure computation techniques.
- Then, multi-parity cryptography algorithms will be applied over trading algorithms to make the system secure.
- Possible techniques are secret sharing schemes, garbled circuits and homomorphic encryption in which arithmetic calculation can be performed on encrypted data.

Secure Computation

Partially homomorphic cryptosystems

- **ElGamal** Allows $E(A) * E(B) = E(A * B)$ operations
- **Goldwasser Micali** Allows $E(A) * E(B) = E(A \oplus B)$ operations
- **Paillier** Allows $E(A) * E(B) = E(A + B)$ operations

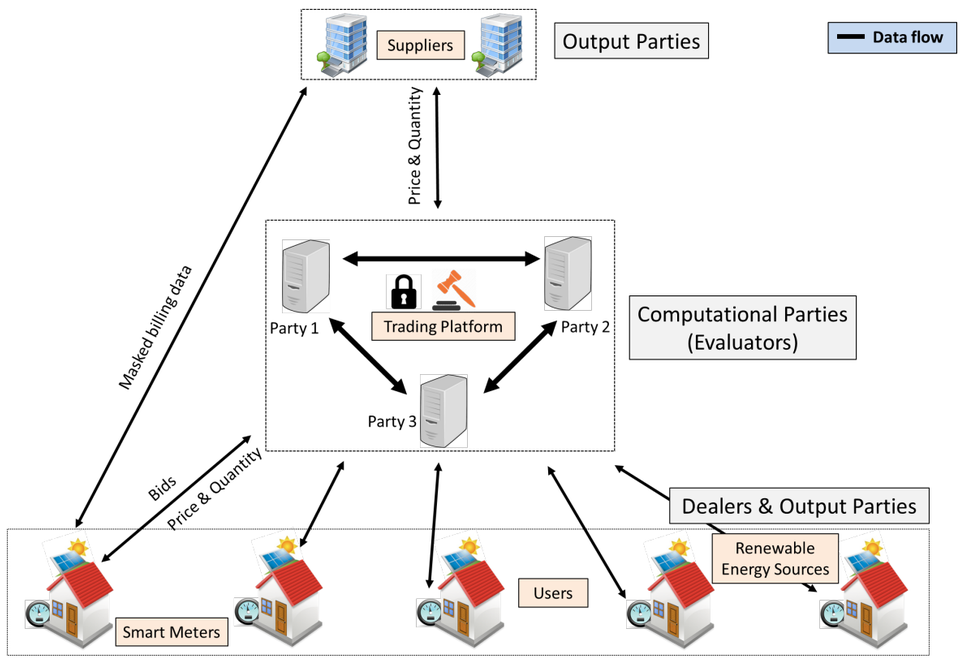
Fully Homomorphic Encryption: cryptosystem that supports arbitrary computation on ciphertexts.

Anticipated Future Research

- Privacy Friendly Non-Cooperative Trading Platform The particular non-cooperative game that has extensively been used for trading in smart grid is Stackelberg game. It is a game where a selected leader defines itâs strategy first and others optimise their strategies accordingly. We will focus in this topic for our design initially.
- Privacy Friendly Cooperative Trading Platform We plan to focus on coalition formation game for this section where agents form coalitions together to get better leverage in terms of optimisation.
- BlockChain Deployment The final distribution and transaction between the sellers and buyers can be realized by the smart contract of the blockchain to ensure the

System Model

- Suppliers are either major electricity producers having large power plants or retailers who collect electricity from wholesaler and sell it to the local users.
- RESes are local prosumers having renewable energy sources at their locations.
- Users are only electricity consumers.
- Trading Platform is a privacy preserving platform which allows aforementioned entities above to to make the following tasks in a secure way.



Threat Model

- Semi-honest model: All the agents are curious to learn private information from each other and they have the incentive to gain higher utilities by cheating on data. On the other hand they do not have the incentive to maliciously corrupt the protocol and the messages in the systems are assumed to be transmitted in a secure way
- Malicious Model: Agents have an incentive to fake the trading data, collude with other agents and deviate the interaction protocols.
- We model all the internal agents(RESes, Supliers, Users and trading platform) as semi-honest agent and the other external trying to breach system as a malicious agent.

References

[1] Zhang, Chenghua, et al.
Peer-to-Peer energy trading in a Microgrid
Applied Energy 220 (2018): 1-12.

[2] FÌelix G Ìomez M Ìamo
Do not snoop my habits: preserving privacy in the smart grid.
EEE Communications Magazine,50(5):166â172, 2012

[3] Gergely ÌAc, et.al.
I have a dream!(differentially private smart metering)
In International Workshop on Information Hiding, pages 118â132. Springer, 2011

[4] Aysajan Abidin et. al.
An mpc-based privacy-preserving protocol for a local electricity trading market
aInInternationalConference on Cryptology and Network Security, pages 615â625. Springer, 2016

[5] Bingyu Liu,
Panda: Privacy-aware double auction for divisible resources without a mediator
InProceed-ings of the 19th International Conference onAutonomous Agents and MultiAgent Systems,pages 1904â1906, 2020