Protected Bidding Against Compromised Information Injection in IoT-Based Smart Grid

Md Zakirul Alam Bhuiyan[1,2], Mdaliuz Zaman[1], Guojun Wang[2(✉)], Tian Wang[3], Md. Arafat Rahman[4], and Hai Tao[5]

[1] Department of Computer and Information Science, Fordham University, New York City, NY, USA
[2] School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China
csgjwang@gmail.com
[3] Department of Computer Science and Technology, Huaqiao University, Xiamen, China
[4] Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Pekan, Malaysia
[5] Department of Computer Science, Baoji University of Arts and Sciences, Baoji, Shaanxi, China

Abstract. The smart grid is regarded as one of the important application field of the Internet of Things (IoT) composed of embedded sensors, which sense and control the behavior of the energy world. IoT is attractive for features of grid catastrophe prevention and decrease of grid transmission line and reliable load fluctuation control. Automated Demand Response (ADR) in smart grids maintain demand-supply stability and in regulating customer side electric energy charges. An important goal of IoT-based demand-response using IoT is to enable a type of DR approach called automatic demand bidding (ADR-DB). However, compromised information board can be injected into during the DR process that influences the data privacy and security in the ADR-DB bidding process, while protecting privacy oriented consumer data is in the bidding process is must. In this work, we present a bidding approach that is secure and private for incentive-based ADR system. We use cryptography method instead of using any trusted third-party for the security and privacy. We show that proposed ADR bidding are computationally practical through simulations performed in three simulation environments.

Keywords: Internet of Things (IoT) · Smart grid · Demand response Security attack · Privacy · Compromised information injection

1 Introduction

Considering Internet of Things (IoT) technologies in smart grid applications is an important method to expedite the informatization of power grid infrastructure. IoT is composed of embedded sensors and actuators, which senses and

A.-S. K. Pathan et al. (Eds.): SGIoT 2018, LNICST 256, pp. 78–84, 2019.
https://doi.org/10.1007/978-3-030-05928-6_8

controls the behaviors of the energy world. IoT is attractive for features of grid catastrophe prevention and decrease of grid transmission line and reliable load fluctuation control. Automated demand response (ADR) with IoT-based smart grids maintain facility for consumers to run a major role in optimizing energy consumption patterns, that is, decreasing or shifting their energy use during peak periods in response to time-based charges or other methods of economic inducements. It maintains demand-supply stability and in regulating customer side electric energy charges. Future IoT-based smart grid integrates demand response [4,9].

Demand bidding (DB) program is an important type of demand responses [8,11]. Southern California Edison (SCE) has recently approved DB program in practice. The consumer can pick a bidding charge as part of the consumer of energy usage discount. If the real quantity of energy reduction corresponds to given demand, the consumer gets rewarded. Alternatively, if the consumer cannot to save the energy usage according to the demand, no commercial punishment is incurred. An important goal of IoT-based smart grids is to enable a type of DR approach called automatic demand bidding (ADR-DB). Demand bidding is often considered to purchase sharing and allocation problem in energy usage market [4,11,14] (Fig. 1).

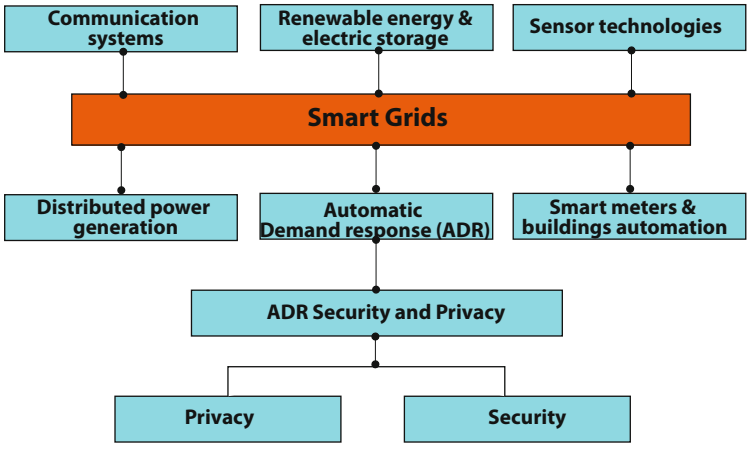

Fig. 1. Security and privacy concerns with ADR in smart grids.

2 Design of Protected Bidding in IoT-Based Smart Grid

An IoT-based smart grid is envisioned to be a fully automated system that can be to obtain decreased cost and better quality of service. These show potential benefits that are rigorously built on wide area measurement and control system, which is called WAMCS. This offers high-level detectability and manageability in energy grid functions. Subsequently, we consider the WAMCS as the system model in this work.

In smart grid, data is collected by the phasor measurement units (PMU). The data collected by PMUs provide the foundation for automatic, effective, and well-organized system management. But there can be cyber enemies or attackers who can come up with the purpose of interfering or basing the basic system functions and they can make an effort to introduce false information into the measurement data through intentionally deployed suspicious PMUs. Regarding the case of IoT-based network, collected data can be compromised at the time of data collection [6,10,12]. Successful false information board attack may compromise the auspicious functionalities described above. They can also ruin the total smart grid system functions. There are numerous threat models [2,3,5,7,13] for smart grid network. We consider that PMUs in the WAMCS, which might be attacked and colluded by the false information board that the attackers can make. For example, they can change and recode the programing interface and settings, or make disconnection in the interface and alter the privacy information board for data transmission and reception [1]. In the case of IoT-based smart grid network, if we consider only one false measurement information board, it might not be able to cause much influence on smart grid system functions. This reason is that the system can be enabled to correct minor errors and faults itself in the subsequent time.

We consider the security and privacy to protection unauthorized information injection. We explain here how we set the privacy and security features in the case of ADR-DB system as follows. We also depict the way the system is controlled (i.e., in the case of the ease of the consumer information recording, cancellation, and demand provision as the incentives to the bidding winners). (1) Anonymity–a bidder or bid winner can attend the bidding and their information must not be recognized after bidding process is over by untrustworthy or unauthorized parties. However, the bidder winner's acceptability and bidding information must be certifiable. Also, at the bidding round, it should be maintained that no entity is noticeable. In this way, the anonymity of the bidder can be maintained: (2) Non-repudiation–participating bidders are able to refuse their bids after becoming the winning bidders; (3) Non-linkability in a few rounds of bidding: it should be maintained that no individual should be able to have access to the outcome; because this may facilitate a bidder to be recognized in several rounds of bidding; (4) privacy–untrustworthy entities can be restricted who may find the chance to construct links to the bidding winner and to designated consumers; (5) Forward security: bidding is done with cryptography key, even if the existing bidding key is attacked, the system maintain security so that information board having the previous keys can be disclosed.

Regarding the given system model and threat models above, our objective is to design a protected and effective, and privacy-oriented ADR-DB bidding process for the IoT-based smart grid.

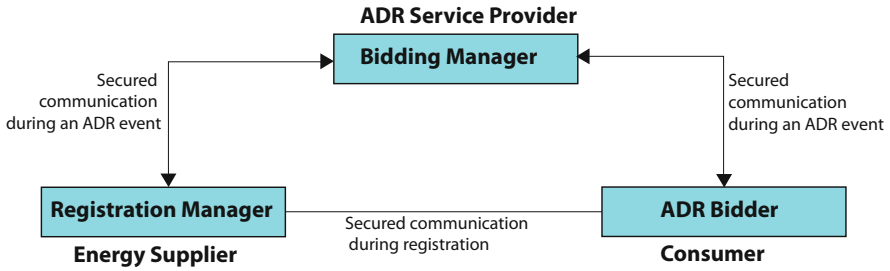

Fig. 2. System architecture for security and privacy in bidding process.

3 Architecture of Protected Bidding Process

We have three units in the architecture: (i) registration manager as the energy supplier, (ii) bidding round manager, and (iii) participating bidders. We maintain norms and definitions that are coherent to with open ADR specification. The registration manager uses privacy technique to distinguish the agreement and basic of the bidder's uniqueness in secret and bidder's cryptography-based registration key. Bidding round manager holds the bidding round process so as to make certificates for the bidding in every round. We can see in Fig. 2 that represents our system architecture.

4 Protocol Development

The protocol is comprised of the following phase:

- *Preparation phase.* At the beginning of a bidding session, a bidding round manager and a registration manager provide information board, where they can exhibit required data. These bidding information boards are usually read-only for individual and all other things. In addition, both of them produce factors and parameters to be used in the bidding protocol. It owns cryptography public- private key pair. For the security reason, it also has signing-verification key pair. Both jointly create an information board for the winning bidder.
- *Bidding key creation.* The registration manager transmits an authorized request to all the registered participating bidders. After the request is received and verified, all the participating bidders transmit the required information board, which is kept encrypted for producing the bidding round key to registration manager. The registration manager produces the bidding round keys and places the keys into the information board. Each participating bidder calculates its own bidding round key and saves it secretly.
- *Bidding round setup.* Using the parameters placed in registration manager's information board, the bidding round manager produces bidding credentials for each of participating bidders and places these credentials in their information board.

- *Bidding round.* Each of the participating bidder produces its own bid, does the encryption operation of the bid information board. They then provide signature on their encrypted bid. The bidding credentials, encrypted bid with the signature are transmitted to the bidding round manager. The bidding round manager validates every signature that was sent by the participating bidders. The bidding round manager then decrypts the encrypted bids that he receives from all of the participating bidders. Afterward, the bidding round manager proclaims the maximum bid in public in order to persist in the present bidding.
- *Bid validation.* Any participating bidder is permitted to examine the legality the bids across verifiable techniques.
- *Bidding winner declaration.* When the bidding round session is over, the bidding round manager declares the bidding winner's information. This information is usually placed on the bidding winner's information board. A participating bidder is able to verify and validate the winning bid.
- *Bidding incentive claim.* Once the bidding session is over, the bidding winner is allowed to demand the bidding incentive through a zero-knowledge proof placement to the registration manager.

As shown in Fig. 3, an UML illustration of bidding manager and other involvements in the bidding process shown in the protocol phases. Pre-processing phase is not given in the figure as it is considered to be pre-calculated. It shows that how compromised information can be injected during the bidding process.

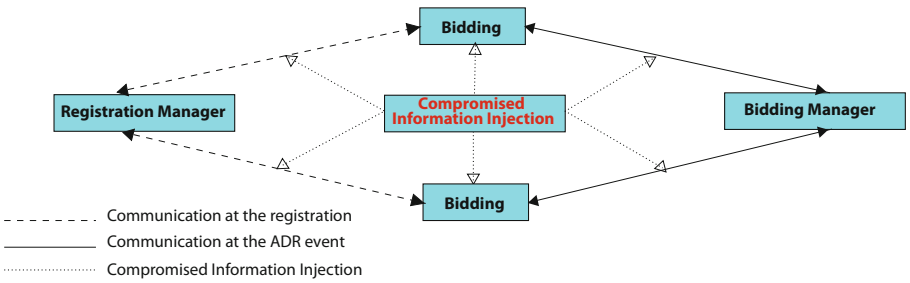

Fig. 3. Compromised information injection architecture.

5 Evaluation

We evaluate the protocol through simulations in Java in terms of primitive operations. These include modular multiplication (multiplying the two numbers and calculating the same modulus), modular exponentiation (a type of exponentiation performed over a modulus used for the public-key cryptography), modular multiplicative inverse and SHA-512 hash functions (producing an unique 512-bit signature). The bidding security key creation phase at the bidding registration

manager is programmed regarding the primitives such as 5 modular exponentiations, 3 modular multiplications and two hashes (referring to the unique hash key when their hash code is equal). We carry out the simulation of each phase 50 times and gather the data. We then calculated the amount of time take in average. Figure 4 demonstrate the process of bidding cryptographic key creation. This usually consumes the highest amount of time between all the phases of the bidding registration manager, bidding round setup and bidding round session.

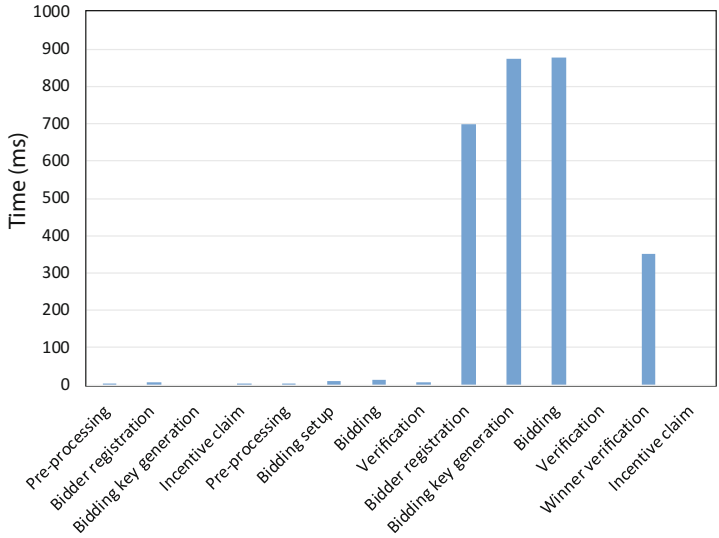

Fig. 4. Computation time needed for different phases.

6 Conclusion

Dealing with accurate information in the IoT-based smart grid infrastructure is significant regarding attacks situations and their severe consequences in the grid, hence, ensuring security and privacy is of great importance. Therefore, one key aim is to provide privacy and security in the ADR in order to prevent compromised information injection. Towards this, customers and demand response control should identify any unauthorized entities in the bidding process and reliability of the demand responses. In this paper, we have proposed a private and secure bidding protocol for incentive-based demand response system of IoT-based smart grids. The limitation of this paper is the performance evaluation of the security aspects of IoT based smart grid. Future work includes the detailed implementation of ADR bidding process in terms of security and privacy aspects.

References

1. Bhuiyan, M.Z.A., Wang, T., Hayajneh, T., Weiss, G.M.: Maintaining the balance between privacy and data integrity in Internet of Things. In: Proceedings of ACM ICMSS 2017, pp. 177–182 (2017)
2. Bhuiyan, M.Z.A., Wu, J.: Collusion attack detection in networked systems. In: Proceedings of IEEE DASC, pp. 1–8 (2016)
3. Liu, H., Xu, M., Wu, Y., Zheng, N., Chen, Y., Bhuiyan, M.Z.A.: Resilient bipartite consensus for multi-agent networks with antagonistic interaction. In: Proceedings of IEEE TrustCom 2018, pp. 1–8 (2018)
4. Liu, Y., Guan, X.: Purchase allocation and demand bidding in electric power markets. IEEE Trans. Power Syst. **18**(2), 106–112 (2003)
5. Lu, L., Zhu, X., Zhang, X., Liu, J., Bhuiyan, M.Z.A., Cui, G.: Intrusion detection method based on uniformed conditional dynamic mutual information. In: Proceedings of IEEE TrustCom 2018, pp. 1–7 (2018)
6. Luo, E., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J., Atiquzzaman, M.: Privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. IEEE Commun. Mag. (COMMAG) **56**(2), 163–168 (2018)
7. Rahman, F., Bhuiyan, M.Z.A., Ahamed, S.I.: A privacy preserving framework for RFID based healthcare systems. Futur. Gener. Comput. Syst. (FGCS) **72**, 339–352 (2017)
8. Rahman, M.S., Basua, A., Kiyomotoa, S., Bhuiyan, M.Z.A.: Privacy-friendly secure bidding for smart grid demand-response. Inf. Sci. **379**(10), 229–240 (2017)
9. Saleem, Y., Crespi, N., Rehmani, M.H., Copeland, R.: Internet of Things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. Technical report (2017). https://arxiv.org/ftp/arxiv/papers/1704/1704.08977.pdf
10. Tao, H., Bhuiyan, M.Z.A., Abdalla, A., Hassan, M., Jain, J., Hayajneh, T.: Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet Things J. (IEEE IoT-J), 1–10 (2018). https://doi.org/10.1109/JIOT.2018.2854714
11. Tarasak, P., Chai, C.C., Kwok, Y.S., Wah, S.: Demand bidding program and its application in hotel energy management. IEEE Trans. Smart Grid **5**(2), 821–829 (2014)
12. Wang, T., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J., Cao, J.: Big data reduction for smart city's critical infrastructural health monitoring. IEEE Commun. Mag. (COMMAG) **56**(3), 128–133 (2018)
13. Wang, T., et al.: Fog-based storage technology to fight with cyber threat. Futur. Gener. Comput. Syst. (FGCS) **83**, 208–218 (2018)
14. Weng, Y., Negi, R., Faloutsos, C., Ilić, M.D.: Robust data-driven state estimation for smart grid. IEEE Trans. Power Syst. **8**(4), 1956–1967 (2017)