Protected bidding against compromised information injection in IoT-based smart grid

Md Zakirul Alam Bhuiyan[a, b], Mdaliuz Zaman[a], Guojun Wang[b], Tian Wang[c], Md. Arafat Rahman[d], Hai Tao[e]

[a]Department of Computer and Information Science, Fordham University, New York City, NY, United States
[b]School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China
[c]Department of Computer Science and Technology, Huaqiao University, Xiamen, China
[d]Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Pekan, Malaysia
[e]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 grids; Demand response; Security attack; Privacy; Compromised information injection

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)
   Google Scholar

2. Bhuiyan, M.Z.A., Wu, J.: Collusion attack detection in networked systems. In: Proceedings of IEEE DASC, pp. 1–8 (2016)
Google Scholar

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)
Google Scholar

4. Liu, Y., Guan, X.: Purchase allocation and demand bidding in electric power markets. IEEE Trans. Power Syst. **18**(2), 106–112 (2003)
Google Scholar

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)
Google Scholar