Study of Security Techniques in AI-based Energy Harvesting

Masoumeh Mohammadi Insoo Sohn

Division of Electronics and Electrical Engineering
Dongguk University

Masoumemohammadi7293@gmail.com isohn@dongguk.edu

Abstract

Energy limitations remain a key concern in the development of new technologies like the Internet of Things (IoT). Energy harvesting (EH) is a technology to capture ambient energy and converts it into usable electric power for mitigating the dilemma between limited battery capacity and increasing energy consumption. However, increasing attacks lead to suffering the EH system from energy-information security. Considering energy security and information privacy are important issues in the EH systems because data security in both fields has a vital role. Artificial intelligence (AI) and machine learning (ML) are critical technologies in security, due to their intelligent analysis framework. This paper reviews two AI- base proposed models for joint protection of energy security and information privacy.

1. Introduction

Energy harvesting technology is an important technology that allows us to collect and store tiny amounts of energy from their ambient environment in real time and use it to power electronic devices [1]. Due to the limited battery capacity and the need to be frequently charged finding a solution to overcome this issue is essential. In addition, the developments of new technologies like the Internet of Things (IoT) and wireless network are opening more eyes to the capabilities of EH solutions. EH allows wireless devices to harvest energy from surroundings, store energy in their own batteries, and transmit it to other low-power devices. wireless power transmission (WPT) technologies lead to increasing the popularity of EH technology due to the transmission of electrical energy without wires as a physical connection [2]. Using EH mitigates the batteries limitation but security and privacy issue remain the main concern with improving new technologies.

The knowledge that AI learns from data could bring many benefits like having more secure systems and improving the Quality of Service (QoS) of users. The energy security mechanism for having better QoS needs user data to train models for malicious node detection. Security becomes an important element in protecting data from external and internal threats. Thus, it is inevitable to access and leak private information, e.g., energy status and consumption habits of users. In addition, direct access to training datasets also raises public concerns about privacy and confidentiality [3] Federated learning (FL) is a new breed of Artificial Intelligence (AI) that mainstream distributed learning technologies, which incorporates data from multiple nodes while avoiding direct data exposure to adversaries [4] [5].

2. Energy Security and Information Privacy

Energy security and information privacy both deal with data and having an appropriate security protocol is very important. But energy security and information privacy are at opposite ends because when we want to establish information privacy protocol, a lot of energy is consumed, that's why we have to create a trade-off between them to have efficient performance. Therefore, the remainder of this article is structured to introduce two proposed models for joining energy security and information privacy.

Xi Lin.[6] proposed a novel robust-efficient wirelessly powered edge intelligence (WPEG) framework. they combined IoT networks and WPT technologies with federated edge learning to improve edge learning performance, which is ignored by the previous works. The issue of energy in the learning process has always played an important role in the learning cycle. Some existing works consider it, which is not only unrealistic but also a limitation in learning performance. as regards, they used energy harvesting to guarantee the device learning in FEL technology. In their framework, at first-time security of both energy and the knowledge-sharing process was considered. they employ a more lightweight and efficient consensus protocol BFT-DPoS in edge blockchain systems. Moreover, they used a two-stage game with incentive mechanisms for energy-knowledge trading to have optimal economic incentives and power transmission strategies. At stage I economic reward is determined and at stage II power transmission strategies are done according to the given economic rewards. Finally, they compare their proposed framework power transmission with two classic schemes: 1) random FEL (RFEL), and 2) uniform FEL(UFEL) in terms of the utility of the MEC node and the utility of WPT nodes. Also, numerical results have proved optimal learning parameter design could achieve optimal global learning efficiency. with this framework, the tradeoff between the learning parameter and the global system efficiency has been studied as they mentioned they can use more mobility of users in their future works.

Qianqian Pan.[7] proposed a new framework for Joint Protection of Energy Security and Information Privacy for Energy Harvesting which was considered in many articles independently although there are overlaps between them. their proposed model consists of three main plans: 1) Energy User (EUs): This plane includes numerous wireless devices

with limited energy. 2) FL and Differential privacy (DP) Empowered Energy Transmitter (ET): energy security, information privacy, and energy transfer happen in this part 3) Servers that have the responsibility of the model management for EH, they supposed static nodes, and each EU requests and harvests energy from its nearest ET. For energy security, they used a federated model with a multilayer feedforward neural network, which uses the ReLU function for hidden layers and Softmax for the output layer. In this part, ET nodes detected malicious energy users by their historical energy behaviors and current energy status based on FL. DP provides strong theoretical guarantees for statistical analysis to protect privacy without any background knowledge of the attackers [8]. Therefore, they used the DP protection mechanism with budget privacy for information privacy. This method is utilized to perturb the model parameters before uploading to the server, by using adding noise the most common popular method t is adding Laplace noise. For creating a balance between protecting energy security and information privacy they proposed an incentive mechanism derives which is defined as Nash equilibrium with the Newton-Raphson algorithm. This mechanism Encouraged ET nodes to participate in the federated model training via rewards and also simulates the high-quality learning behaviors of ETs with optimal training strategy for all ETs. Finally, experimental results verified the optimization of the utility of each ET, encourages their participation, and balance the joint energy-information security of their proposed method. their standard for evaluation was the rate of detected malicious EUs. They compared the performance of the proposed federated energy security scheme with the Conventional rule-based method and the smart method without FL. Their proposed schemes converge the test loss to a low value faster than the baseline

3. Conclusion

This paper has presented a survey of two proposed models for joining energy security and information privacy. Due to the capabilities that AI adds to the system, we can use these approaches to design security models by considering both energy and information. FL is a kind of machine learning that reduces data security and privacy concerns by maintaining stores of local data, which was used in two proposed models. Consequently, performance of proposed security schemes compared with the Conventional methods without FL have efficient performance via time and system throughput, and energy.

Acknowledgments

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20224000000020).

References

[1] U. Saleem, S. Jangsher, H. K. Qureshi, and S. A. Hassan, “Joint subcarrier and power allocation in the energy-harvesting-aided D2D communication,” IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2608–2617, Jun. 2018.

[2] R. Zhang and C. K. Ho, “MIMO broadcasting for simultaneous wireless information and power transfer,” IEEE Trans. Wireless Commun., vol. 12, no. 5, pp. 1989–2001, May 2013.

[3] M. Pooyandeh and I. Sohn, “Edge network optimization based on ai techniques: A survey,” Electron., vol. 10, no. 22, 2021, doi: 10.3390/electronics10222830

[4] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020.

[5] M. Pooyandeh and K. Han, “applied sciences Cybersecurity in the AI-Based Metaverse : A Survey,” 2022.

[6] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and M. J. Piran, “Blockchain-Based Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design,” *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14685–14698, 2022, doi: 10.1109/JIOT.2020.3024246.

[7] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, “Joint Protection of Energy Security and Information Privacy for Energy Harvesting: An Incentive Federated Learning Approach,” *IEEE Trans. Ind. Informatics*, vol. 18, no. 5, pp. 3473–3483, 2022, doi: 10.1109/TII.2021.3105492.

[8] C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, and G. Wu, “Differential privacy preserving in big data analytics for connected health,” J. Med. Syst., vol. 40, no. 4, 2016, Art. no. 97