Abnormal Detection System Design of Charging Pile Based on Machine Learning

Yanjie Li1,*, Xiaoyu Ji1, Dongxiao Jiang2 and Tao Meng2*

1School of Electrical Engineering, Zhejiang University, Hangzhou, China
2Electric Power Research Institute, State Grid Jilin Company, Changchun, China

*Corresponding author e-mail:yanjiele@zju.edu.cn

Abstract. With the exhaustion of fossil energy and people's increasing attention to environmental protection, electric vehicles began to be popularized around the world. As an important infrastructure, the EV charging network is faced with the risk of a series of network attacks, which may cause economic losses to the power grid and car owners, and even endanger the stable operation of the power grid. In order to solve the security problem of charging piles, we designed an abnormal detection system for charging piles based on the power consumption side channel and machine learning. By collecting power consumption information of the charging control unit of charging piles, the abnormal detection system determines whether charging piles are facing attacks or not. We have verified three kinds of attacks, proving that our anomaly detection system can effectively detect attacks and protect the security and stable operation of charging piles.

1. Introduction

With the development of battery technology and government incentives, the driving range of electric cars increases gradually, and electric cars begin to be popular with the public. By the end of June 2020, there were 1.322 million charging piles in China, including 558,000 public charging piles. The number will reach 1.66 million by this year and 11.2 million in 2025[1]. The State Grid of China has developed a Smart Internet of Electric Vehicle Charging Network (SIEN). Charging piles have gradually become one of the most necessary infrastructures for the popularization of electric vehicles[2].

The function of the charging pile is similar to the refueling machine in the gas station. It can be fixed on the ground or wall and installed in public buildings (public buildings, shopping malls, public parking lots, etc.) and residential parking lots or charging stations. It can charge various types of electric vehicles according to different voltage levels. The input end of the charging pile is directly connected to the AC power grid, and the output end is equipped with a charging plug for charging EV. People can swipe recharge cards and operate the human-computer interaction interface on the charging pile and choose different charging ways and charging time. The charging pile screen can show charging quantity, cost and charging time data.

These public charging piles are often deployed in the wild or unattended environment and use mobile communications and other ways to connect to the central station. If they do not get adequate protection, they are vulnerable to cyber physical attacks, leading to electricity stealing, unavailability of charging piles, and even endanger the stability of power grid or resulting in failure of electric cars and other problems. To solve this problem, this paper proposes a charging pile security monitoring
technology based on power consumption side channel. By collecting power consumption information of core modules of the charging pile and using online machine learning algorithm, the power consumption is monitored in real time and abnormal behaviors are warned.

2. Literature Review

2.1 Attacks for charging pile

As for the attack measures for charging piles, some attacks have attempted to attack the communication protocols of charging piles and electric vehicles or to influence the distribution grid by attacking charging piles. According to the charging rules of charging piles, Zhang[3] et al. proposed two attack schemes from the perspective of attackers trying to influence the smooth operation of the distribution grid: attacks against huge slow charging loads at night and attacks against fast charging loads in the daytime. Li[4] et al. proposed that the Smart Internet of Electric Vehicle Charging Network (SIEN) mainly presents three attacks: distributed data tampering, distributed denial of service (DDoS), and forged command attacks. Besides, the charging protocol between EV and smart charging pile is vulnerable to eavesdropping, tampering, DDoS attack, and other security threats due to the lack of security analysis and protection mechanism.

2.2 Defense measures for charging pile

As for the defense measures for charging pile, Xu [5] proposed a secure authentication mechanism based on cryptography to protect the charging protocol. Huang[6] proposed a decentralized security model to improve the security of trading between EVs and charging piles. Wei [7] proposed a network security situation awareness model for charging pile systems. The model introduced network security detection, threat early warning analysis, risk decision response and security trend assessment. Li[8] proposed a decentralized and privacy-preserving charging scheme to solve the privacy leakage problem of cloud-based centralized management mode. Fang[9] proposed a RFID-based authentication system for the electric vehicle charging station. The analysis shows that the system has good computing and storage performance and security.

However, these defense measures did not take into account threats from the physical world, such as attackers maliciously altering wiring or maliciously removing critical modules, or burning malicious programs through maintenance interfaces. For this reason, we propose a charging pile security protection method based on the power consumption side channel to realize the host-based security protection.

3. The security analysis of charging pile

3.1 Basic structure of charging pile

The system of a single-phase AC charging pile is simple and covers a small area. It can be conveniently installed in various public places and the internal parking lot of the community. It can also be installed in various large, medium and small charging stations. It adopts self-service operation, which is suitable for all kinds of unmanaged parking lots. Users can complete charging, paying, and other operations independently. It is the main charging equipment for small electric vehicles. AC charging system is composed of leakage current detection and protection switch, electricity meter, AC control unit (ACCU), auxiliary power supply, charging socket, and man-machine interaction unit. EVIU801, a billing verification unit, and a full touch screen are configured in the human-machine interface of AC charging pile. EVIU801 collects trading and electric degree information and communicates with the ACCU. ACCU interacts with vehicle battery management system (BMS) for charging control. The total system diagram is shown in Fig.1.
3.2 Security analysis of charging pile

The AC charging control module of the charging pile is usually an embedded system with microcontrollers and other chips. At present, the chips commonly used with AC charging piles include DSP, microcontrollers and FPGA. There already are some known threats to these chips. The security threats mainly include software security threats and hardware security threats. For instance, Johannes [10] found that STM32F0 has vulnerabilities such as design weakness in the security configuration storage. Azhar [11] discovered that in the IoT background, DSP faces the threats of hardware Trojan. For charging pile equipment, because the equipment is often deployed in an unattended environment, an automatic anomaly monitoring method is needed to realize remote anomaly monitoring.

4. Abnormal detection system design

For the security monitoring system of charging pile, due to the existence of electromagnetic interference under strong electric environment and the power side channel has stronger anti-interference ability, we adopt the power side channel to realize the security monitoring of charging pile.

4.1 Security state division of charging pile

According to different standards of reliability evaluation of electric power IoT terminals, different states can be divided. When the electric power terminal state tends to not meet the requirements of reliable criteria of the state, the maintenance personnel should take the necessary measures to ensure terminal reliability restore to an acceptable level.

Probabilistic power system reliability analysis usually divides its operating state into two types: Normal state and at risk. Billinton further divided normal into healthy and marginal[12]. Similarly, the operation state of power Internet of Things devices can be divided into the following three typical operation states: normal state, risk state, and accident state.

State 1(normal state): In this state, there is no component fault in the terminal of the Power Internet of Things, nor any malicious behavior. In other words, the terminal and terminal run in the planned way, and the terminal device in normal state does not need to carry out additional monitoring tasks.

State 2(risk state): In this state, the terminal of the power Internet of Things has not been effectively attacked, but the attacker is trying to attack the terminal, or there is an attack, but the impact of the attack is not serious. The terminal of power Internet of things has certain abnormal performance.
State 3(accident state): In this state, the terminal of the power Internet of Things receives an attack, and there may be an equipment component fault and terminal equipment is not working normally. There is malicious firmware replaced by the attacker or malicious injected code, resulting in terminal business logic error.

4.2 Security monitor system design
As an inherent attribute of the terminal equipment, the bypass signal of the side channel can reflect the working state of the equipment. By learning the performance and output of the bypass signal in different states, we can extract the relevant features of the bypass signal. Common side-channel features include frequency domain features and time-domain features. Then, based on the characteristics, we can determine whether the device is working properly, or whether it has been attacked.

After the side channel characteristics of the terminal equipment are obtained, the common attacks and abnormal changes of each side-channel information on the terminal equipment shall be analyzed, and the side channel information of different attack types shall be clustered. Here, hierarchical clustering, K-means, and other clustering methods are used.

Collecting the side channel information of different types of attacks or anomalies and storing it as a negative sample library can further improve the performance of the classifier.

5. Experiment
We used XJ ZCJ31 series single-phase AC charging piles. Fig.2 shows the charging pile used in our experiment and monitoring system design.

![Charging pile used in experiment](image)

Figure 2. Charging pile used in our experiment and monitoring system design. (*XJ ZCJ31 series single-phase AC charging piles.*)

The monitoring system is deployed on raspberry PI. Due to the limited computing power, deep learning algorithms cannot be adopted. Therefore, we first classify the collected side-channel information through a variety of weak classifiers and then use the Adboost algorithm to improve the detection accuracy. The detection algorithms we tried included KNN, random forest, SVM, etc. The attempted attacks include stopping the TCU module by network attack(TCU attack), making the ACCU module work in abnormal state by malicious software(ACCU attack), increasing the sampling frequency of voltage and current but keep the sending frequency unchanged, thus resulting in the waste of power(Sampling attack). Our final classification results are shown in Table.1, and our final test results meet the standards for industrial applications.
Table 1. ABNORMAL DETECTION RESULTS.

| Classification Algorithm | TCU attack | ACCU attack | Sampling attack |
|--------------------------|------------|-------------|-----------------|
| SVM                      | 0.91       | 0.95        | 0.88            |
| Logistic Regression      | 0.89       | 0.91        | 0.83            |
| Random Forest            | 0.86       | 0.90        | 0.85            |
| Decision Tree            | 0.88       | 0.92        | 0.87            |
| Naive Bayes              | 0.93       | 0.94        | 0.89            |

6. Acknowledgments
This work is supported by the technology research project of SGCC "Research on Security Attack Evaluation and Monitoring Technology of Electric IoT Devices Based on Artificial Intelligence" (52230019000B).

References
[1] Prope, Bernd, et al. "Market penetration analysis of electric vehicles in the German passenger car market towards 2030." International Journal of Hydrogen Energy 38.13 (2013): 5201-5208.
[2] Number of charging piles for electric vehicles to rise, https://www.chinadaily.com.cn/a/202008/15/WS5f374ce8a3108348172607d6.html.
[3] Y. Zhang, Y. Jiang, A. Xu, C. Hong and J. Chen, "Method to Evaluate the Impact of Cyberattacks Against Charging Piles on Distribution Network," 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 2020, pp. 1-5, doi: 10.1109/APPEEC48164.2020.9220574.
[4] Li, Qianmu, et al. "Time series association state analysis method for attacks on the smart internet of electric vehicle charging network." Transportation Research Record 2673.4 (2019): 217-228.
[5] Xu, J., Yu, X., Tian, L., Wang, J., & Liu, X. Security Analysis and Protection for Charging Protocol of Smart Charging Pile. In Proceedings of the 9th International Conference on Computer Engineering and Networks (pp. 963-970). Springer, Singapore, 2020.
[6] X. Huang, C. Xu, P. Wang and H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem," in IEEE Access, vol. 6, pp. 13565-13574, 2018.
[7] Wei, Xiuling, Chuanxiang Du, and Jinlong Zhao. "A network security situation awareness model for electric vehicle shared charging pile system." AIP Conference Proceedings. Vol. 2238. No. 1. AIP Publishing LLC, 2020.
[8] Li H, Han D, Tang M. A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing. IEEE Systems Journal. 2020 Jul 28.
[9] Fang, Lei, et al. "A RFID-Based Security Authentication System Model for Electric Vehicle Charging Station." Applied Mechanics and Materials. Vol. 741. Trans Tech Publications Ltd, 2015.
[10] Obermaier, Johannes, and Stefan Tatschner. "Shedding too much light on a microcontroller's firmware protection." 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17). 2017.
[11] A. Syed and R. M. Lourde, "Hardware Security Threats to DSP Applications in an IoT Network," 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Gwalior, 2016, pp. 62-66.
[12] R. Billinton and E. Khan, "A security based approach to composite power system reliability evaluation," in IEEE Transactions on Power Systems, vol. 7, no. 1, pp. 65-72, Feb. 1992, doi: 10.1109/59.141688.