Research on KNN Algorithm of Charging Device Based on Attack Recognition Method

Zhiwei Huang, Xichao Yan, Qiangang Wang, Yuansheng Chen, Wenju Wu, Jiewen Zhan, Rui Chen, Kai Ding, Lianxing Zu, Aijun Xu, Zongzhou Su, Dianjun Chen, Sajia Lin, Peng Xu and Chong Wang

CYG SUNRI CO., LTD, Shenzhen 518000, China.
Corresponding author e-mail: hzw@sznari.com

Abstract. With the continuous improvement of the level of economic development and the increasingly serious environmental problems, new energy is gradually being respected by people, and more and more electric vehicles have been put on the market and gradually used widely. The development of electric vehicles has led to the development of charging devices. However, traditional charging devices operate in an open environment, and communication with other devices depends on information interaction with the network. With the development of network information today, network attacks are ubiquitous, and there are various risks in network information interaction. As long as there is a security loophole in the charging device, an attacker can use various means to attack the device and even invade the inside of the power grid, which directly affects the safe and stable operation of the power grid. Aiming at the potential threats in operation, a research on the nearest neighbor algorithm of charging device K based on attack recognition method is proposed here to improve the information security and operation reliability of charging device.

1. Introduction

As the world’s coal mine resources are increasingly depleted and environmental pollution is getting worse, countries are paying more and more attention to environmental protection, technological progress, and energy security. In the field of highway transportation, internal combustion engines that consume a lot of fossil energy are gradually being used in various other energy sources. The new energy vehicle industry with electrification as the technological background replaced by the power system ushered in good development opportunities.

In the past ten years, the technologies of pure electric vehicles, hybrid vehicles [1-4]and fuel cell vehicles and their related components have been greatly developed. The world’s automotive industry is experiencing the transition from traditional fuel vehicles to new energy batteries in the future.

The Chinese government attaches great importance to the development of clean and efficient automotive technology. China's self-developed electric vehicles and related components such as power batteries, drive motors and their controllers, charging systems, electronic monitoring systems, etc. have achieved staged results, and a number of related supporting equipment has also developed very well, and there is no shortage of charging devices in the middle. However, with the intelligence and informationization of the power grid, various network attack methods have emerged endlessly, and the charging devices are located in the public environment and are easily affected by various kinds of attacks, these attacks may sneak into the internal management system of the charging device, steal other user information, or modify their account balance for unlimited charging through virus invasion,
or even invade the power grid, causing a failure of the power grid. The existing security loopholes have become increasingly prominent, so it is urgent to improve the safety performance of the charging device in all directions.

The charging device[5-8]is an indispensable key device for the healthy development of electric vehicles. In addition to providing charging functions for electric vehicles, there are also communication modules, data storage modules, power modules, sampling modules, etc. Communication between power grids, and the charging device involves an open operating environment, and communication with other devices depends on information interaction with the network, so there are various risks, and most domestic devices use foreign chips. There may be a little-known backdoor in the chip. Once a network attack[9-12]occurs on the charging device, it will affect the normal operation of the charging device, cause the leakage of user information, and even paralyze the entire power grid.

2. Development Status

Figure 1 is an application scenario diagram of a charging device in the prior art. It can be seen from Figure 1 that the upper charging device is connected to the AC power distribution cabinet and the station-level operation monitoring system, which is an important bridge connecting the upper-layer AC power distribution cabinet to providing power to the user's electric vehicle. For the station-level operation monitoring system, it is an important source interface for providing data. The charging device uploads the status monitoring data during the charging process, analyzes the battery data of the electric vehicle, the energy billing, and the user information to the station-level operation monitoring system for data analysis and storage.

![Diagram](attachment:image.png)

**Figure 1.** Application scenario diagram of charging device

However, due to the current development of network information, there are various risks. Traditional charging devices may have certain hidden safety hazards. As long as there is a security loophole in the charging device, the attacker will use this as a breach. It will use repeated sending requests or use a large amount of useless data to cause network congestion, which will cause the device to fail to work properly, and even use the loophole to invade the system background and obtain users. Data or hijack the background. An attacker can also repeatedly send malformed attack data according to the transmission protocol defect of the charging device, so as to achieve the purpose of tampering with the electricity data to steal the electricity bill, manipulation of real-time electricity prices, tampering with the meteorological data, causing misjudgment of the environmental monitoring system, and further triggering higher-level control. The controller or dispatching center incorrectly allocates a large amount of system resources, which directly affects the safe and stable operation of the
power grid. Based on the actual work and research data, this paper analyzes the current shortcomings of electric vehicle charging devices, and proposes a research on the K nearest neighbor algorithm of charging devices based on the attack recognition method [13-16] to improve the performance of charging devices. Information security and operational reliability.

3. Attack Recognition Model

This paper proposes a research on the nearest neighbor algorithm of charging device K based on attack recognition method. The device model shown in Figure 2 includes a human-computer interaction interface, communication module, output interface, charging power module, and classification module connected to the main controller. The classification module is connected to an electricity meter and an IC card reader. The main controller is connected to an output interface and a charging power module through a CANBUS bus, and connected to a human-computer interaction interface and a communication module through an RS232 interface. The classification module is connected to the electricity meter, The IC card reader and human-computer interaction interface are connected, and the input end of the communication module connected to the station-level operation monitoring system includes an IC card reader, electricity billing, ambient temperature, and charging time.

Among them: the IC card reader is used to obtain the IC card user data and sent to the classification module; the classification module is used to generate the corresponding message for the data obtained through the meter and the IC card reader, and the KNN algorithm is used to refer to the message as a reference to the message classify and upload the classification results to the main controller and human-computer interaction interface; the main controller is used to complete the coordinated control function of other modules, receive input instructions, switch the working status of the charging pile, control the charging power module, and output through the output interface corresponding control instructions, as well as receiving attack alarms, log records sent by the classification module, and forwarding the data classified into the normal category through the communication module; the human-computer interaction interface enables the human-machine interaction between the user and the charging pile, the charging demand information input, and the charging process data display, attack alarm display function, and transmission of charging demand information to the classification module; the charging power module is used to achieve autonomous current sharing of the power modules in parallel, so that a standard power module can be connected in parallel to form a variety of chargers controlled by the master controller to achieve its control adjustment, and then output power. The main controller receives the primary command, adjust power, and the power transmitted to the output interface to output, and transmitting power to the meter.

The working principle of this model first requires the collection of a large amount of data. First collect the normal operation electricity billing data of the charging device, IC card user data, charging price/degree, charging device output power and other data, obtain the data to generate the corresponding message, and then Take different attack methods on the device (such as dos attack, user information stealing attack, power stealing attack, etc.), obtain the data again, generate the corresponding message, and then transmit the collected message to the KNN classification module. The classification is based on the classification module based on the KNN algorithm. When the data fields of real-time messages fall into the normal category, real-time data is sent to the main controller, and the main controller forwards the real-time data, that is, through the communication module. Sent to the station-level operation management system; finally, if there is abnormal attack data (such as power stealing attack) in the data field of the message, the classification module sends an attack alarm and generates a log record to the main controller, and classifies the network attack data, the classification results are transmitted to the main controller, and when the main controller receives the points from the KNN classification module. After the result, measures will be taken in a timely manner, such as displaying the attack type on the human-machine communication interface, uploading the attack information to the intelligent management module, and finally to the operation management system, and disconnecting the output interface to stop charging to the vehicle. To achieve the purpose of attack identification.
4. Implementation Steps

4.1. Overall Implementation Steps

The overall implementation steps of the charging device K nearest neighbor algorithm based on the attack recognition method proposed in this paper are shown in Figure 3. The specific algorithm implementation steps include the following steps (shown in Figure 4):

Step 1: Collect the normal database and the abnormal database after the network attack, and then integrate and classify the data in the normal database and the abnormal database respectively, and use all the classifications as the reference sample group to obtain the reference database; The normal data collected by the charging device in daily life is collected from the data field in the message; the normal data (the data field of the message) includes electricity billing data and IC card users data, charging price, input current, input voltage, charging capacity (degrees), output power of the charging device, etc.; the abnormal database can be obtained through abnormal data generated under a network attack on the normal database. The data field part of the attack packet includes the data mentioned above; each classification corresponds to a reference sample; the classification includes a normal class, a network attack class, and the network attack class includes a network attack class including a U2R attack, R2L attack, Trojan horse attack, user information stealing attack, power stealing attack, Unauthorized access attacks, forgery and other electrical quantities of data;

Step 2: Obtain the message of the charging device, extract the real-time data in the message, classify the real-time data and the reference database with the K nearest neighbor algorithm to classify the real-time data, and use the reference database as a reference to calculate the real-time data. The distance between each data and the samples in the reference sample group in the reference database. Select the K samples closest to the data in the sample, and count the number of categories to which the K samples belong. When the data appears in the nearest sample, the data with the highest ratio are classified into this category;
Step 3: Determine the classification of the data. When there is data in the real-time data that is classified as a cyber attack category, an attack alarm is generated and a log record is generated for storage, and the data classified as a cyber attack category is intercepted; the attack alarm is displayed on the charging device; at the same time, the real-time data classified as normal is forwarded (that is, no other processing is performed); when the real-time data is classified into the network attack category, the real-time data is forwarded (i.e., do nothing);

When an attack alarm is issued, the attack information is generated along with log records (including attack type, attack time, and data start and end addresses) and sent to the station-level operation monitoring system. When the station-level operation monitoring system receives the attack information, it sends it to the charging device. Control instructions; the control instructions include disconnecting the charging output interface and stopping charging with the vehicle.

4.2. Specific Algorithm Implementation Steps
As shown in Figure 4, the real-time data is classified by the K-nearest neighbor algorithm [17-20] in the second step by using the following methods:

![KNN algorithm implementation steps](chart)

**Figure 4.** KNN algorithm implementation steps

(1) Establish a two-dimensional coordinate system as shown in Figure 5, where the X-axis uses the number of times a message is sent as a feature quantity, and the Y-axis represents the time interval between message transmissions as a feature quantity (normally sent by different messages under attack). The time interval difference is relatively small, but when the data is attacked, the time interval is significantly different from the normal message transmission interval). The reference database is used as the known category point. When a message of an unknown category is received, it passes the European Union. The distance is calculated from the unknown point (data field in the message) to all
known category points. In general, the data is transmitted in the device in the form of a message. The message format includes the slave address and function code, start address, number of registers, number of bytes, data field and check code, etc., where the data field is the data in the present invention, including electricity billing data, IC card user data, charging demand, charging price, input current, input voltage, amount of charge (degrees), output power of the charging device, etc.

Euclidean distance calculation formula in two-dimensional plane:

\[ d_n = \sqrt{(x_1 - x_n)^2 + (y_1 - y_n)^2} \]  

Among them, \( x_1 \) represents the abscissa of unclassified points, \( y_1 \) represents the ordinate of unknown category points, \( n \) represents the nth known category point (that is, known attack category or normal data), and \( d_n \) represents the nth unknown point and known distance between point categories;

(2) Sort the calculated Euclidean distance (shown in Figure 5) according to the increasing relationship between distances; as shown in Figure 4, assume that the R2L attack class is a green square, the UR2 attack class is a red diamond, and the normal class is yellow. Triangular, unknown points are circular; the distance between the unknown points to R2L attack class, UR2 attack class and normal class is calculated by euclidean distance and sorted according to the increasing distance relationship;

![Figure 5. Example of this classification](image)

(3) Then select K points with the smallest distance from the unknown point (as shown in Figure 6); the value of K ranges from 6 to 15, the initial value is 6, and it is adjusted according to the classification;

(4) Statistics are performed according to the classification corresponding to K points, and the number of points occupied by K points in each classification is counted. The classification with the largest number includes the unknown point in the classification; as shown in Figure 6, select When the K distance is 6, the R2L attack class has 3 known class points, the UR2 attack class has 2 known class points, and the normal data has 1 known class point. According to the nearest neighbor algorithm, we can know that the unknown points are classified in the R2L attack class;
5. Conclusions
Charging device is an indispensable key device for the healthy development of electric vehicles, but it runs in an open environment and its communication with other devices depends on information interaction with the network, so there are various risks, and most domestic devices The chip used is a foreign chip. There may be a little-known back door in the chip. Once a network attack occurs on the charging device, it will affect the normal operation of the charging device, cause leakage of user information, and even paralyze the entire power grid.

Aiming at the unknown attack of the charging device in an open environment, this paper proposes a research on the K nearest neighbor algorithm of the charging device based on the attack identification method. Through the early normal conditions and network attack message collection, a database is formed to obtain the charging device. Real-time message. After extracting the real-time data in the message, classify the real-time data and the reference database with the K nearest neighbor algorithm to classify the real-time data, and use the database as a reference to calculate each of the real-time data and the reference database. With reference to the distances of the samples in the sample group, select the K samples closest to the data in the sample, and count the number of categories to which the K samples belong. When the data appears in the nearest sample, the data belongs to the largest category, and the data is The data field (data) in the message of the charging device is classified by the K nearest neighbor algorithm into the classification, and the hidden attack lines in the real-time data of the charging device are classified to avoid the existence of an attacker through the charging device. Security vulnerabilities further invaded the upper-layer system, improving the information security and operation of the charging device Reliability, so as to achieve the purpose of attack recognition.

6. Acknowledgment
This work was by Supported by the National Key R&D Program of China (2018YFB0904900, 2018YFB0904903).

7. Reference
[1] Chan, C.C . An overview of electric vehicle technology. Proceedings of the IEEE, 81 1202.
[2] Li, S ., & Mi, C. C. . (2015). Wireless power transfer for electric vehicle applications. Emerging and Selected Topics in Power Electronics, IEEE Journal of, 3 4.
[3] Shimizu, H ., & Harada, J . (1997). Advanced concepts in electric vehicle design. IEEE Transactions on Industrial Electronics, 44 14.
[4] Riezenman, M. J . (1998). Engineering the ev future. IEEE Spectrum, 35 18.
[5] Liu, Z. , Wen, F. , & Ledwich, G. . (2013). Optimal planning of electric-vehicle charging stations in distribution systems. IEEE Transactions on Power Delivery, 28 102.

[6] Wang, G. , Xu, Z. , Wen, F. , & Wong, K. P. . (2013). Traffic-constrained multiobjective planning of electric-vehicle charging stations. IEEE Transactions on Power Delivery, 28 2363 .

[7] Lee, W. , Xiang, L. , Schober, R. , & Wong, V. W. S. . (2015). Electric vehicle charging stations with renewable power generators: a game theoretical analysis. IEEE Transactions on Smart Grid, 6 608.

[8] Mehd Etezadi-Amoli, Kent Choma, & Jason Stefani. (2010). Rapid-charge electric-vehicle stations. IEEE Transactions on Power Delivery, 25 1883 .

[9] Sridhar, S. , Hahn, A. , & Govindarasu, M. . (2012). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100 210.

[10] Hahn, A. , Member, S. , IEEE, Member, S. , & IEEE. (2011). Cyber attack exposure evaluation framework for the smart grid. IEEE Transactions on Smart Grid, 2 835.

[11] Soltan, S. , Yannakakis, M. , & Zussman, G. . (2017). React to cyber attacks on power grids. ieee transactions on network science & engineering, 99 1.

[12] Bruno, C. , Guidi, L. , Lorite-Espejo, A. , & Pestonesi, D. . (2015). Assessing a potential cyberattack on the italian electric system. Security & Privacy, IEEE, 13 42.

[13] Pasqualetti, F. , Dorfler, F. , & Bullo, F. . (2013). Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58 2715.

[14] Ameli, A. , Hooshyar, A. , El-Saadany, E. F. , & Youssef, A. M. . (2018). Attack detection and identification for automatic generation control systems. IEEE Transactions on Power Systems, 99 1.

[15] Ashok, A. , Govindarasu, M. , & Wang, J. . (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. Proceedings of the IEEE, 1 19.

[16] Sahoo, S. , Mishra, S. , Peng, C. H. , & Dragicevic, T. . (2018). A stealth cyber attack detection strategy for dc microgrids. IEEE Transactions on Power Electronics, 1 1.

[17] You Jung Kim, & Jignesh M. Patel. (2010). Performance comparison of the \( \text{rm r}^{\text{ast-tree}} \) and the quadtree for knn and distance join queries. IEEE Transactions on Knowledge & Data Engineering, 22 1014.

[18] Hou, J. , Gao, H. , Xia, Q. , & Qi, N. . (2015). Feature combination and the knn framework in object classification. IEEE Transactions on Neural Networks and Learning Systems, 1 1.

[19] Zhang, Shichao, Li, Xuelong, Zong, & Ming, et al. (2018). Efficient knn classification with different numbers of nearest neighbors. IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, 5 29.

[20] Chapelle, O. , Haffner, P. , & Vapnik, V. N. . (1999). Support vector machines for histogram-based image classification. IEEE Transactions on Neural Networks, 10 1055.