Research on Identification Method and Device with Active Immune Attack

Qiangang Wang, Hui Liu, Wenju Wu, Yuansheng Chen, Shengyuan Xiao, Jiewen Zhan, Rui Chen, Yinghong Xie, Kai Zhang, Lianxing Zu, Xiaofan Zhu, Lei Shi, Zheng Zhang, Dongkai Fang and Heng Yin

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

Abstract. The large-scale establishment of charging devices facilitates the use of electric vehicles and promotes the development of the new energy industry. However, the core chips of most domestic charging devices use imported chips. There may be little-known backdoors in the chips, which may hide large loopholes. Once a cyber war occurs, the consequences are unimaginable. At the same time, with the intelligence and informationization of the power grid, various network attack methods are emerging, and the charging device is located in the public environment, which is vulnerable to various attacks. These attacks may sneak into the internal management system of the charging device and steal other user information, or modify your account balance for unlimited charging through virus intrusion, or even invade the power grid, causing grid failure. Aiming at the above problems, this paper adds the network attack detection module based on stack automatic encoder to the charging device to detect the data flow in the charging device in real time, mine and identify the hidden attacks in the data stream, so as to avoid the attacker further intruding the upper system through the security vulnerability of the charging device, and to improve the information security and operation reliability of the charging device, to a certain extent, it also ensures the safety of the power grid.

1. Introduction

The automobile industry is a pillar industry of the national economy and a landmark industry that reflects national competitiveness. But at the same time, the environment is facing great pressure and challenges, especially air pollution. Exhaust emissions from cars are acquiesced as one of the culprits of air pollution. China's fuel car ownership ranks first in the world, and the number is still insane. In order to reduce exhaust pollution, it is imperative to promote the development of new energy vehicles[1-3].

Since 1993, China has become a net oil importer, and oil imports have increased year by year. Due to the relative shortage of China's fossil energy production, especially oil and natural gas production, China's energy supply will rely more and more on the international market in the future. The instability of the international oil market and fluctuations in oil prices will seriously affect China's oil supply and cause a great impact on the economy and society. The development of new energy vehicles can largely get rid of the dilemma, and it will not be constrained by other countries on energy issues.

China's automobile industry started late, and in the early years, they used the market for technology. There is still a clear gap between China's traditional automobile industry and other major automobile countries. After all, traditional cars have been developed for more than 130 years, and the barriers to technology and regulations are very high and it is difficult to catch up. However, as a new field of new energy vehicles, all countries start at the same time. If China wants to upgrade its industry and realize "curve overtaking", it must work hard.
The development of new energy vehicles is inseparable from the supporting new energy vehicle charging devices. There are three types of electric vehicle charging: wired charging, unlimited charging, and overall replacement. Among them, the more mature and widely used charging method is wired charging. The wired charging is divided into AC charging device (slow charging) and DC charging device (fast charging). According to the "Development Guide for Electric Vehicle Charging Infrastructure Development (2015-2020)" issued by the Development and Reform Commission, the development goal of China's charging infrastructure is to build 12,000 centralized charging stations and 4.8 million decentralized charging devices by 2020[4-9].

The large-scale establishment of charging devices facilitates the use of electric vehicles and promotes the development of the new energy industry. However, the core chips of most domestic charging devices are imported chips. There may be little-known backdoors in the chips, which may hide large loopholes. Once a cyber war occurs, the consequences are unthinkable. At the same time, with the intelligence and informationization of the power grid, a variety of network attack methods are emerging, and the charging device is located in the public environment, which is vulnerable to various attacks. These attacks may sneak into the internal management system of the charging device and steal other user information. Or, by modifying the balance of your account for unlimited charging through virus invasion, or even invading the power grid, causing grid failures, it can be seen that the security loopholes in charging devices have become increasingly prominent, so it is urgent to improve the safety performance of charging devices in all directions.

2. Charging Device Model

Figure 1 shows the application scenario of the existing charging device. The charging device is connected to a station-level monitoring system and an AC power distribution cabinet. It is an important bridge connecting the upper-layer AC power distribution cabinet to providing electric energy to the user's electric vehicle. For the station-level monitoring system, it is an important source interface for providing data. The charging device will monitor the state monitoring data during the charging process and the battery of the electric vehicle. Data analysis, energy billing, and user information are uploaded to the station-level monitoring system to analyze and store relevant data.

![Diagram of Charging Device Application Scenario](image_url)

**Figure 1.** Application scenario of charging device
The structural block diagram of the charging device is shown in Figure 2. Among them, the charging device controller is used to send down the operation instructions sent from the charging control module; The output voltage, output current, and environmental data are sent to the billing control module.

The touch controller is used for operating input to the controller of the charging device; the card reader is used to read the user information of the IC card and send it to the billing control module, the user information includes the account ID, balance, etc.; the electric meter is used to read the power consumption Information and power quality information of the grid and sent to the billing control module; display module: used for display and human-computer interaction; positioning module is used to obtain time and location information in real time and then sent to the network attack detection module through the communication module; the storage module is used to store data, including alarm information and log records; communication module is used for communication;

The metering module is used to statistically generate the power consumption information from the energy consumption sent by the meter and the power quality information of the power grid, and then bill the power consumption information to generate power billing information, which is then sent to the network attack detection module for detection; electricity billing information is obtained from the electricity meter, combined with the time-sharing electricity fee plus the profit premium to calculate the consumer's electricity bill. The data of the electricity consumption and electricity bill is transmitted to the network attack detection module through the communication module;

The network attack detection module is used to receive the data stream sent by the communication module, and perform real-time detection and classification through the stack autoencoder network model to determine whether there is abnormal data in the data stream. When there is no abnormal data, the data stream is forwarded directly to the upper layer through the communication module; when there is abnormal data, the real-time data stream is intercepted, an alarm is issued and a log record is generated, and a shutdown instruction is sent to the charging device controller; when the charging device controller receives the stop command, it will promptly take measures to disconnect the output interface and stop charging to the vehicle. Figure 3 shows the flowchart of active immune attack recognition.
Figure 3. Flow chart of active immune attack recognition

The network attack detection module also sends alarm information to the upper layer through the communication module, and the alarm information is the attack type corresponding to the abnormal data. At the same time, the network attack detection module also intercepts the data stream in real time, and issues an alert prompt. Specifically, the real-time data stream is intercepted, and the alarm prompt is displayed on the display module according to the classification of the abnormal data. The network attack detection module will also store the log records in the storage module and / or send them to the upper layer for storage.

3. Network Attack Detection Model

Real-time detection and classification includes calculating the probability of abnormal data and normal data in the data after classifying the data stream. When the probability of the abnormal data is greater than the probability of normal data, it is determined that there is abnormal data under attack in the data stream; the probability of abnormal data includes the probability that the data in the data stream will be subjected to each type of network attack; when the probability of abnormal data is greater than the probability of normal data, the probability of a network attack with the highest probability is also found among the probability of abnormal data, and the abnormal data is falls into the category of this type of cyber attack.

A stack autoencoder network model is established using the following steps:

1. Construct a first-layer autoencoder. The autoencoder has two parts: an encoder and a decoder. The function of the encoder is to map the input vector to the hidden layer to get a new feature representation. The function is expressed as follows: (1):

   \[ z = f(x) = s(W^{(1)}x + b^{(1)}) \]  

   Among them: \( x \in \mathbb{R}^{d \times 1} \) represents the input vector, \( d \) is the dimension of the input data; \( z \in \mathbb{R}^{r \times 1} \), \( r \) is the number of hidden layer units; \( W^{(1)} \in \mathbb{R}^{r \times d} \) is the input weight of the hidden layer; \( b^{(1)} \in \mathbb{R}^{r \times 1} \) is the input bias of the hidden layer; \( s \) represents the activation function, which is usually non-linear. Commonly used activation functions are: sigmoid function: \( s(x) = \frac{1}{1+e^{-x}} \), tanh function: \( s(x) = \frac{e^x-e^{-x}}{e^x+e^{-x}} \) as well as relu function: \( s(x) = \max(0,x) \); 

   The role of the decoder is to map the representation \( z \) of the hidden layer back to the original input.
x, and the function is expressed as follows (2):

\[ x = g(z) = s(W^{(2)}z + b^{(2)}) \]

Among them: \( W^{(2)} \in \mathbb{R}^{d \times r} \); \( b^{(2)} \in \mathbb{R}^{d \times 1} \), the autoencoder network model output is associated with X; the first-order features of the data stream are associated with \( z \) in the first-layer encoder; the output weights of the first-order features to the output are associated with \( W^{(2)} \); First-order feature-to-output output bias associated with \( b^{(2)} \); The superscript (2) is associated with the number of network layers [10-16];

The reconstruction error of each data is the following formula (3):

\[ L = \| x - g(f(x)) \|_2^2 \]

The cost function is defined as:

\[ J(W, b) = \frac{1}{N} \sum_{i=1}^{N} \left( \frac{1}{2} \| x^{(i)} - g(f(x^{(i)})) \|_2^2 \right) + \frac{\lambda}{2} \sum_{k=1}^{S_k} \sum_{i=1}^{S_{k+1}} (W_{ji}^k)^2 \]

Among them: \( x^{(i)} \) represents the i-th sample; \( W_{ji}^k \) represents the connection weight between the \( k \)-th unit \( i \) and the \( k+1 \)-th unit \( j \); \( N \) represents the number of samples; \( S_k \) represents the number of units in the \( k \)-th layer; \( \lambda \) is the regularization coefficient, \( \lambda \) is 1.

Through error back conduction and batch gradient descent algorithm, the parameters \( W \) and \( b \) when \( J(W, b) \) is the minimum value are taken as the optimal solution; the flowchart of the first layer autoencoder is shown in Figure 4.

**Figure 4.** Flow chart of the first layer autoencoder

2. Construct the second-layer autoencoder, take \( W^{(1)} \) as the input data of the second-layer autoencoder, and perform the operation according to step 1 to construct the second-layer autoencoder to obtain the optimal solutions \( W \) and \( b \);

3. Construct the third-layer autoencoder, take \( W^{(2)} \) as the input data of the third-layer autoencoder, and perform operations according to step 1 to construct the third-layer autoencoder to obtain the
optimal solutions W and b;

4. Construct the BP neural network classifier layer and use the output of the third layer of the self-encoder as the input of the BP neural network; first perform forward calculation of the input feature vector to get the predicted category at the output layer; compare the actual corresponding categories to get the classification error, use the error back-propagation algorithm to train the parameters of the BP neural network, and fine-tune the parameters of the autoencoders at each layer[17-20].

In the process of error backpropagation, the residual δ of each layer of the network is first calculated. For each output unit i of the output layer, δ is calculated as:

\[ \delta_i = a_i (1 - a_i) (a_i - y_i) \]  \hspace{0.5cm} (5)

Among them: \( a_i \) is the sample value; \( y_i \) is the estimated value; for other hidden layers, the calculation formula of δ is the following formula (4):

\[ \delta_i^k = a_i^k (1 - a_i^k) \sum_{j=1}^{S_{k+1}} W_{ji}^k \delta_i^{k+1} \]  \hspace{0.5cm} (6)

Among them: \( k \) refers to the k-th layer network; \( S_{k+1} \) refers to the total number of network neurons in the \( k + 1 \)th layer; \( a_i^k \) is the output value of the i-th unit of the k layer.

After calculating the residuals of each layer, adjust the parameters of each layer of the stacked autoencoder network according to the following formulas (5) and (6), \( \alpha \) is the adjustment coefficient, and \( \alpha \) is selected as 0.01; The flowchart of the stack autoencoder is shown in Figure 5.

\[ W_{ji}^k = W_{ji}^k - \alpha a_i^l \delta_i^{k+1} \]  \hspace{0.5cm} (7)

\[ b_i^k = b_i^k - \alpha \delta_i^{k+1} \]  \hspace{0.5cm} (8)

![Figure 5. Structure of a stack autoencoder network model](image_url)

4. Conclusions
Compared with the prior art, this paper analyzes and classifies the data obtained by the charging device through a stack autoencoder network model, and outputs the probability of being attacked by the network. Ensure the information security and operation reliability of the charging device, and ensure the security of the power grid.

5. Acknowledgments
This work was supported by the National Key R&D Program of China (2018YFB0904900, 2018YFB0904903).
6. References

[1] Jajodia S, Noel S, O’Berry B. Keynote 3: Topological Analysis of Network Attack Vulnerability// 2009

[2] Hug, Gabriela, Giampapa, Joseph Andrew. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. IEEE Transactions on Smart Grid, 3(3):1362

[3] Dawkins J, Hale J. A systematic approach to multi-stage network attack analysis// 2004

[4] Dong Wei, Yan Lu, Jafari, M, et al. Protecting Smart Grid Automation Systems Against Cyberattacks. IEEE Transactions on Smart Grid, 2(4):782

[5] Andre Teixeira, Henrik Sandberg, K.H. Johansson. Networked Control Systems under Cyber Attacks with Applications to Power Networks// American Control Conference (ACC), 2010. 2010

[6] Gao Z. Tracing Cyber Attacks from the Practical Perspective. 2005, 43(5):123

[7] Petit, Jonathan, Shladover, Steven E. Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2):1

[8] Mariana Belgiiu, Lucian Drăguţ. Random forest in remote sensing: A review of applications and future directions. Isprs Journal of Photogrammetry & Remote Sensing, 2016, 114:24

[9] Dong Wei, Yan Lu, Mohsen Jafari, et al. An integrated security system of protecting Smart Grid against cyber attacks// Innovative Smart Grid Technologies (ISGT), 2010. IEEE, 2010

[10] Dumitras, A, Haskell, B.G. A texture replacement method at the encoder for bit-rate reduction of compressed video. IEEE Transactions on Circuits & Systems for Video Technology, 13(2):163

[11] Hanna Kamysanska, Roland Memisevic. The Potential Energy of an Autoencoder

[12] Song J, Zhang H, Li X, et al. Self-Supervised Video Hashing With Hierarchical Binary Auto-Encoder. IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, 2018, 27(7):3210

[13] M. Zaman, M. Rahman. Experimental testing of the artificial neural network based protection of power transformers. Power Delivery IEEE Transactions on, 13(2):517

[14] Song Han, Xingyu Liu, Huizi Mao, et al. Deep compression and EIE: Efficient inference engine on compressed deep neural network// 2016 IEEE Hot Chips 28 Symposium (HCS). IEEE, 2016

[15] Brandon Reagen, Paul Whatmough, Robert Adolf, et al. Minerva: Enabling Low-Power, Highly-Accurate Deep Neural Network Accelerators. ACM SIGARCH Computer Architecture News, 2016, 44(3):267

[16] Li Deng, Geoffrey Hinton, Brian Kingsbury. New types of deep neural network learning for speech recognition and related applications: an overview// 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2013

[17] Yun Lei, Nicolas Scheffer, Luciana Ferrer, et al. A novel scheme for speaker recognition using a phonetically-aware deep neural network// ICASSP 2014 - 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2014

[18] Jui-Ting Huang, Jinyu Li, Dong Yu, et al. Cross-language knowledge transfer using multilingual deep neural network with shared hidden layers// Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on. IEEE, 2013

[19] Jorge Albericio, Patrick Judd, Tayler Hetherington, et al. Cnvulun: Ineffectual-Neuron-Free Deep Neural Network Computing. ACM SIGARCH Computer Architecture News, 2016, 44(3):1

[20] GUO Zi-jian, TANG Ming. Research of EV charging pile monitoring information modeling based on IEC61850. Power System Protection & Control, 2013, 41(3):134