RAIRO-Oper. Res. 57 (2023) 1329–1341
https://doi.org/10.1051/ro/2023038

RAIRO Operations Research
www.rairo-ro.org

SECURITY OPTIMIZATION METHOD OF HIGH-POWER CHARGING PILE INTER-GROUP COMMUNICATION NETWORK UNDER TRUSTED TABOO PARTICLE SWARM OPTIMIZATION

Yigang Wang and Jianfeng Zhao*

Abstract. In order to ensure the normal operation of the communication network in the event of a small number of charging pile failures, it is necessary to establish a stable communication network between the charging pile groups. In this case, it is necessary to improve the stability and viability of the communication network between the pile groups. Based on this, this paper proposes a security optimization method for high-power inter pile communication networks under trusted tabu particle swarm optimization. Using 6LoWPAN technology to optimize the wireless communication network architecture of charging piles to reduce the probability of communication network paralysis; design a neighborhood end-to-end communication strategy, and conduct research on lightweight key management of charging piles by building a three-tier architecture for the communication environment of charging piles. The trusted taboo particle swarm optimization algorithm optimizes the security of the communication network between high-power charging piles to ensure the security of the communication network. The experimental results show that after the optimization of the proposed method, the stability and invulnerability of the communication network between the charging pile groups have been effectively improved, and the method has a high convergence speed.

Mathematics Subject Classification. 68U35.

Received September 14, 2022. Accepted March 25, 2023.

1. Introduction

In recent years, the development of charging and swapping facilities has promoted the rapid development of the entire electric vehicle industry [1, 2]. However, the rapid development of the industry has also brought certain threats to information security. Among them, solving the information security problem of the communication network between electric vehicles and charging piles is the most critical. However, at present, there are no information security requirements and relevant standards for the communication network between electric vehicles and charging piles in China, which leads to the uncertain situation of both electric vehicle enterprises and charging pile enterprises on the issue of information security of the communication network in the charging process [3, 4]. In this context, the communication network security of charging piles, especially the communication network security between high-power charging piles, has become an urgent problem to be solved.

Keywords. Trusted taboo particle swarm optimization, High-power charging pile, Communication network, Time stamp asynchronous replacement, Lightweight key management.

Southeast University, Nanjing, Jiangsu 210000, P.R. China.
*Corresponding author: zhaochenpie7@163.com

In response to the above problems, relevant scholars have proposed some solutions and measures. Among them, the literature [5] proposed a WSN routing algorithm suitable for the electric vehicle charging pile cluster management system. This method integrates the analytic hierarchy process and the dispersion maximization method. The two-layer networking communication architecture of the management system based on optical fiber communication technology and wireless sensor network (WSN) is determined. Wireless sensor network (WSN) originated from self-organized wireless networks, emphasizing closed-loop, fully functional networks (sensing, data transmission, system control, data applications, etc.), with features such as node miniaturization, dry battery power supply, unattended, self-organized multi-hop, and so on. According to the application environment of charging pile clusters, an efficient WSN routing mechanism based on geographic location information-GLAR is proposed, which alleviates the "hot zone" problem to a certain extent and realizes the minimum hop routing. According to the user's charging law, the Monte Carlo simulation method is used to simulate the user's charging demand, and the performances of GLAR (Geographic Location Aware Routing) and LEACH (Low Energy Adaptive Clustering Hierarchy) are simulated and compared under the same network environment. The research results show that this method can meet the requirements of the charging pile group for the performance and security of communication services. Literature [6] proposes a blockchain-based V2G anonymous identity authentication method, which considers that the communication entities in the vehicle-to-grid (V2G) energy trading system lead to electric vehicles (EVs) due to the lack of identity verification and anonymity protection. There are security and privacy risks with V2G communication entities such as charging stations and data centers. Establish a blockchain-based energy trading system model, use the blockchain's distributed ledger to perform energy transactions, and use elliptic curve digital signature algorithms and one-way hash functions for identity verification. Design an anonymous identity authentication scheme to achieve privacy protection and mutual authentication between EVs, charging stations and data centers, while minimizing EV communication overhead and computing overhead. The research results show that the method can effectively reduce the communication cost and computing time. In order to ensure the communication security of the three-layer architecture of the management control center, the electrical control cabinet and the electric vehicle charging pile, and to take into account the communication efficiency of the electric vehicle charging pile, literature [7] proposes a lightweight key management scheme for the charging pile, and gives a detailed key management implementation process. The key security, forward and backward security, anti-attack ability, computing load and key storage quantity of the scheme are analyzed. The research results show that the scheme has the ability to resist forgery attacks, man-in-the-middle attacks and replay attacks, taking into account both security and efficiency, and can meet the communication security requirements of charging piles.

The communication network between the charging piles is an important basic system for realizing the communication between the charging pile and the monitoring center and providing related services. Usually, the charging pile is unattended, and it takes a long time for the maintenance personnel to arrive at the scene after finding the fault. Therefore, in order to ensure that the communication network can still maintain normal operation when a small number of charging piles fail, a stable communication network needs to be established between the charging pile groups. Based on the existing research, this paper proposes a security optimization method for the communication network between high-power charging piles under the trusted taboo particle swarm optimization, in order to improve the stability and invulnerability of the communication network.

2. Communication network architecture between high-power charging piles

2.1. Wireless communication network architecture of charging pile

Wireless communication technology [8] is usually adopted for remote monitoring of charging piles. This is because the construction site of these charging piles adopts wired wiring, which is difficult and costly. Moreover, considering that in the actual construction situation, most parking spaces only reserve the installation conditions of charging piles, and will not be installed in place at one time, so the wiring is simpler wireless communication with easier expansion has become a more suitable technical choice for charging pile networking. As shown in Figure 1, it is a relatively common charging facility wireless communication network networking scheme.

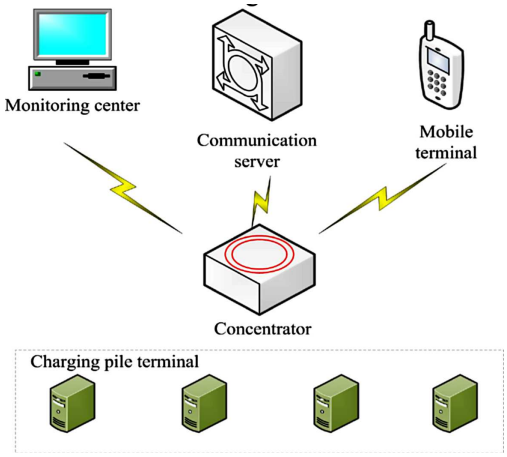

FIGURE 1. Architecture diagram of wireless communication network of charging pile.

As can be seen from the architecture diagram shown in Figure 1, the charging pile communication network generally consists of three parts: the terminal network, the concentrator device, and the cloud network. The terminal network consists of multiple charging piles, which can be networked by wired or wireless connection. The concentrator device is usually a gateway device, and the information of each charging pile will be gathered here, and then uploaded to the cloud network through the concentrator. In the current actual situation, mobile communication technologies such as 4G are usually used to realize the connection between the concentrator device and the cloud server. When there is a Wi-Fi hotspot nearby, the connection can also be completed through the Wi-Fi hotspot. Cloud network is a remote charging facility management platform. The collection and real-time display, data storage query and statistics, and remote control of charging point related information must be completed on or with the help of this platform. Meanwhile, if the personal terminal wants to obtain the charging point information, it must also be connected to this platform. However, it can be observed from this architecture diagram that there is an unavoidable defect in this centralized network architecture, that is, the performance of the concentrator device will directly determine the performance of the network, and the failure of the concentrator can easily cause the entire terminal network of paralysis.

2.2. Optimization of communication network architecture between charging pile groups

According to the analysis results of the traditional charging pile communication network in Section 2.1, this paper uses the wireless communication method based on 6LoWPAN technology [9] to optimize the communication network. Because 6LoWPAN technology is based on IP technology, using 6LoWPAN technology can realize that each charging pile terminal has its own IP address and establish an all-IP communication network. Such a network is conducive to monitoring each charging pile, and at the same time brings more convenience when connecting the charging pile communication network to the Internet, which is conducive to the remote transmission of charging data and other cloud-based related services.

The network system is mainly composed of charging pile terminal 6LoWPAN network, data transmission equipment and monitoring center, as shown in Figure 2. The charging pile forms a 6LoWPAN wireless communication network through the internal communication module, that is, the charging pile terminal 6LoWPAN network (hereinafter referred to as "terminal 6LoWPAN network"). Terminal the 6LoWPAN network is mainly composed of border routers (6LoWPAN Border Router, 6LBR) and information nodes. Data transmission equipment is a network equipment used to connect the charging pile terminal network with the Internet, and plays an important role in controlling data sending and receiving, network maintenance, and protecting network security. Since the terminal 6LoWPAN network is based on the IPv6 protocol, and the current Internet is mainly based

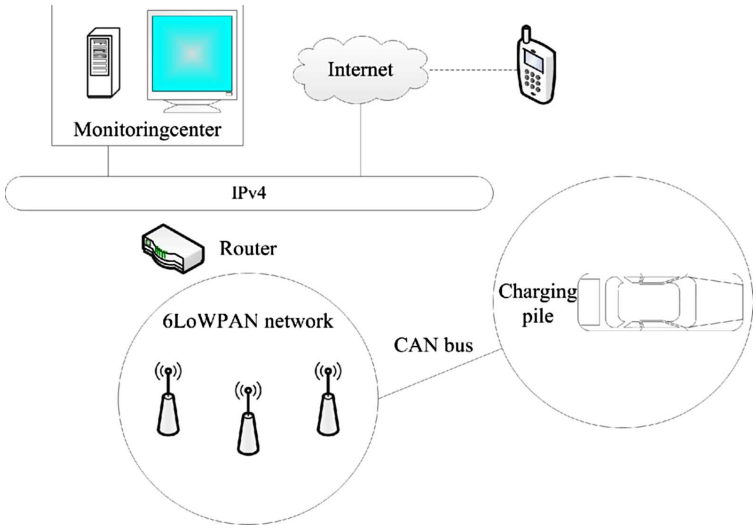

FIGURE 2. Architecture diagram of communication network between charging piles.

on the IPv4 network, the terminal 6LoWPAN network cannot directly communicate with the current IPv4 network, and network protocol conversion is required. In the communication network system between charging pile groups designed in this paper, 6LBR is responsible for completing the conversion between IPv6 and IPv4, so as to realize the normal communication between the terminal 6LoWPAN network and the IPv4 network.

As shown in Figure 2, when a vehicle uses any charging pile for charging, the information acquisition module inside the charging pile will realize two-way communication with the BMS inside the electric vehicle. This function is mainly realized by the CAN bus protocol, and the charging pile will automatically Obtain relevant information about the charging process, such as vehicle battery model, battery capacity, battery voltage and other information. The information acquisition module of the charging point processes the collected data according to the designed data format, and then directly or indirectly transmits the data to the 6LBR device in the 6LoWPAN network of the terminal through its upper level node. The 6LBR performs relevant processing on the data and then transmits the data to the server of the charging point monitoring center. If the charging state of the charging pile is abnormal, the charging pile will generate an abnormal signal and then transmit it to the monitoring center through the communication network. According to the content of the signal, the fault of the charging pile can be quickly learned and the identity code of the faulty device geographic location.

The monitoring center in this network is a place for data visualization and remote operation by staff. If it is in a charging station, the monitoring center is usually a control place for security, fire protection and other systems. In the monitoring center, the operation status of each charging point terminal can be reflected in real time through the large screen or other visual equipment. At the same time, the data can be sent to the cloud data center through the Internet. With the help of big data analysis and other means and mobile terminal applications such as mobile phones, more accurate charging services can be provided for electric vehicle users. Compared with the traditional charging pile wireless communication network, the optimized charging pile group communication network can not only realize two-way communication, but also avoid the problem of the whole terminal network paralysis caused by concentrator failure.

3. Security optimization of communication network between high-power charging piles

3.1. Neighborhood end-to-end communication strategy based on timestamp asynchronous replacement

Compared with the centralized control strategy, the distributed control strategy that only needs asynchronous communication between neighboring charging piles has lower requirements on the real-time communication and can reduce the communication overhead. The specific interaction process of end-to-end communication is divided into three parts: communication content, communication process and update strategy.

3.1.1. Content of communication

Each charging pile has established a database to store its charging pile information and prediction data. During communication, the content sent by the charging pile is exactly the same as the content in the database.

The database stores n group of prediction data and m time stamps in total. Each group of data is the power and voltage prediction result of the corresponding charging pile, and a time stamp is attached to record the generation time of the original data. The storage information of the charging pile a about the charging pile b includes: the time stamp of the charging pile, the active power increment, the reactive power increment, and the predicted voltage value.

In particular, in the initial period when the communication has not yet started, the missing time stamp, active power increment, and reactive power increment are replaced by 0, and the predicted voltage value is replaced by 1.

3.1.2. Communication process

For a single charging pile, the communication process is shown in Figure 3. First, set the adjacent charging piles of each charging pile according to the distribution of charging piles, and ensure that all charging piles can communicate directly or indirectly through intermediate charging piles. After the reactive power response is triggered, the communication starts. During the communication process, the information before and after the reception is compared. If the database is updated, the information is sent to the adjacent charging pile, otherwise it waits for the information to be received again. Finally, when the overall voltage deviation is less than the end threshold, the communication and reactive power response are ended.

At the same time, the reactive power response of the charging pile is calculated at the initial moment of each cycle. If the data in the database cannot fully cover the calculation requirements of the reactive power response of the charging pile, the missing part of the active power and reactive power increment is replaced by 0, and the part missing the voltage value It is replaced with the voltage value of the most recent time in the database. After the calculation of the reactive power response of the charging pile is completed, the prediction results of the active power, reactive power increment and voltage will be updated to the database.

3.1.3. Communication content update policy

The charging pile receives the communication content from the neighboring piles, including the timestamp of each charging pile and the corresponding active and reactive power increments, and the predicted voltage value. After receiving the information, the charging pile integrates it according to the time stamp, so that the data in the database is up-to-date. In addition, after completing the calculation of the reactive power response of the charging pile, the charging pile will update the timestamp, voltage prediction value, and active and reactive power increments in the database.

3.2. Lightweight key management of electric vehicle charging pile

According to the neighborhood end-to-end communication strategy designed above, further aiming at the communication environment of the charging pile, the research on the lightweight key management of the charging pile is carried out by constructing a three-layer architecture. The three-layer architecture specifically refers to

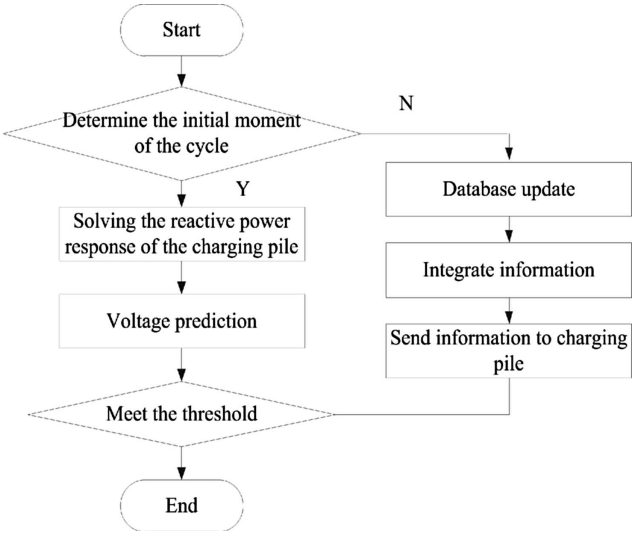

FIGURE 3. Communication flow chart.

the charging pile (CP), charging pile electrical control cabinet (control cabinet, CC) and management control center (control management center, CMC), the key management scheme has the following assumptions:

(1) Regardless of extreme cases, each key management worker is considered to be honest and reliable, and it will not deliberately expose the managed key information.
(2) When the key information of the key is stored in the physical medium, it is safe and reliable, and will not be directly obtained or modified by the intruder, and it is considered that the advanced encryption standard algorithm (AES) is relatively safe in calculation.
(3) Diffie Hellman algorithm is often used in key management to establish and exchange keys. However, the disadvantage of this algorithm is that it is vulnerable to man in the middle attack and difficult to implement when applied to charging piles.
(4) In the entire three-tier architecture, each communication member is relatively fixed, and the identification information of the participants can be confirmed with a small cost. Therefore, when the system is first built and set up, considering the certainty of the installer and the constraint of the temporary key lifetime, it is considered that the key management is safe at this time.

In the lightweight key management scheme for charging piles based on the three-layer architecture, set $T_{\text{CMC-1}}$ and $T_{\text{CMC-2}}$ as the CMC to realize the encryption and decryption time of a message, $T_{\text{CC-1}}$ and $T_{\text{CC-2}}$ as the electrical control cabinet to realize the encryption and decryption time of a message, $T_{\text{CP-1}}$ and $T_{\text{CP-2}}$ are the time for the charging pile to realize one data encryption and decryption, and M_{CC} and M_{CP} are the number of the same multicast group where the charging pile and the electrical control cabinet are located.

This paper mainly considers the following situations:

(1) When a new CC is put into use, it is necessary to distribute the master key K_P and the session key K_C of other device members of the multicast group that it will join to the newly added CC. According to the key distribution process, the time t_{CMC} required for the management and control center to distribute K_P and the time t_{CC} for CC operation can be obtained, as shown in formulas (1) and (2) respectively:

$$t_{\text{CMC}} = 2(T_{\text{CMC-1}} + T_{\text{CMC-2}}), \tag{1}$$

$$t_{\text{CC}} = 2(T_{\text{CC-1}} + T_{\text{CC-2}}). \tag{2}$$

After the management and control center distributes K_P to the newly accessed CC, it sends K_C to the newly added CC and updates the K_C of other CC. The operation time t'_{CMC} of the management control center and the operation time t'_{CC} of each CC are shown in formulas (3) and (4) shows:

$$t'_{\mathrm{CMC}} = 2M_{\mathrm{CC}}(T_{\mathrm{CMC\text{-}1}} + T_{\mathrm{CMC2}}), \tag{3}$$

$$t'_{\mathrm{CC}} = 2M_{\mathrm{CP}}(T_{\mathrm{CC\text{-}1}} + T_{\mathrm{CC\text{-}2}}). \tag{4}$$

To sum up, when a new electrical control cabinet CC is added, the total time required for encryption and decryption of the management control center can be obtained from formulas (1) to (3) as shown in formula (5):

$$t^{\mathrm{all}}_{\mathrm{CMC}} = t_{\mathrm{CMC}} + t'_{\mathrm{CMC}} = 2M_{\mathrm{CC}} \cdot T_{\mathrm{CMC\text{-}1}} + 2M_{\mathrm{CC}} \cdot T_{\mathrm{CMC\text{-}2}}. \tag{5}$$

From formulas (2) to (4), the encryption and decryption time required for the newly added CC can be obtained as shown in formula (6):

$$t^{\mathrm{all}}_{\mathrm{CC}} = t_{\mathrm{CC}} + t'_{\mathrm{CC}} = 4M_{\mathrm{CP}} \cdot T_{\mathrm{CC\text{-}1}} + 4M_{\mathrm{CP}} \cdot T_{\mathrm{CC\text{-}2}}. \tag{6}$$

Other CC only update the session key once, so the time required for encryption and decryption is t'_{CC}.

(2) When a new charging pile CP joins, it is necessary to distribute the master key to the newly joined CP and update the session key that the CP will join the multicast. The CP needs to obtain the master key from the management control center through the CC. During this process, the management and control center performs encryption and decryption operations as shown in formula (7):

$$t^2_{\mathrm{CMC}} = T_{\mathrm{CMC\text{-}1}} + 2T_{\mathrm{CMC\text{-}2}}. \tag{7}$$

In this process, the time consumption of CC operation is shown in formula (8):

$$t^2_{\mathrm{CC}} = T_{\mathrm{CC\text{-}1}} + 2T_{\mathrm{CC\text{-}2}}. \tag{8}$$

In this process, the time consumption of CC operation is shown in formula (8):

$$(t_{\mathrm{CC}})^2 = 2T_{\mathrm{CC\text{-}1}} + 2T_{\mathrm{CC\text{-}2}}. \tag{9}$$

Correspondingly, the time overhead of the newly put into use charging pile is shown in formula (10):

$$t_{\mathrm{CP}} = 2(t_{\mathrm{CP\text{-}1}} + t_{\mathrm{CP\text{-}2}}). \tag{10}$$

CC sends K_C to the newly added CP and updates K_C to other CP. The CC operation time is shown in formula (11):

$$\left(t'_{\mathrm{CC}}\right)^2 = 2(T_{\mathrm{CC\text{-}1}} + M_{\mathrm{CP}}T_{\mathrm{CC\text{-}2}}). \tag{11}$$

The CP operation time is shown in formula (12):

$$t'_{\mathrm{CP}} = t_{\mathrm{CP\text{-}1}} + 2t_{\mathrm{CP\text{-}2}}. \tag{12}$$

From formulas (8), (9) and (11), the total time required for the CC operation can be obtained as:

$$T^2_{\mathrm{CC}} = t^2_{\mathrm{CC}} + (t_{\mathrm{CC}})^2 + \left(t'_{\mathrm{CC}}\right)^2. \tag{13}$$

The calculation time of the newly added charging pile includes the sum of the calculation time of the master key and the session key sent by the CC to it, as shown in formula (14):

$$t_{\mathrm{CP}} = \sum_{t=1}^{m} t_{\mathrm{CP\text{-}1}} + t_{\mathrm{CP\text{-}2}}. \tag{14}$$

The computation time of other charging piles is only the time $t_{\mathrm{CP\text{-}2}}$ for updating the session key.

(3) When a device member quits, other members in the same multicast group also need to update the session key. Unlike (1) and (2), the device member who quits does not need to perform encryption and decryption operations. In addition, for the periodic update time overhead of device members K_P and K_C, reference may be made to (1) and (2), which will not be repeated in this article.

According to the above steps of lightweight key management of electric vehicle charging piles, the security of the communication network between high-power charging piles can be guaranteed to a certain extent. However, since the relationship between charging pile groups is complex and widely distributed, it is necessary to further strengthen the security of the communication network.

3.3. Implementation of security optimization of communication network between high-power charging piles

The PSO algorithm [10] has the advantages of simple operation and easy implementation, and strong global optimization ability, but the convergence speed is slow when the algorithm runs to the later stage, and the solution accuracy is not high. The convergence speed of the TS algorithm is fast, but the final convergence result of the algorithm is greatly affected by the initial solution. In view of the characteristics of the above two algorithms, on the basis of lightweight key management of electric vehicle charging piles, the two are combined to propose a trusted taboo particle swarm optimization algorithm, which can realize the complementary advantages of different algorithms, and at the same time improve convergence speed and solution accuracy. Introducing the trust function into the PSO algorithm and applying it to the selection of the optimal solution after the algorithm iteration, fully considers the network security problem in the special environment of the grid, which has great practical significance [11].

The flowchart of the trusted taboo particle swarm optimization algorithm is shown in Figure 4:

The specific steps of the algorithm can be described as follows:

(1) Program initialization. Set the parameters of PSO algorithm, randomly generate the initial population, and initially set the speed and position of each particle, calculate the fitness value of each particle in the initial population, set the initial historical optimal solution of each particle, and solve the historical optimal solution of the population; Set the parameters of TS algorithm (tabu length, number of candidate solutions, etc.), randomly generate the initial solution, and leave the tabu table empty.
(2) Determine whether the PSO process satisfies the termination condition, that is, after 10 consecutive iterations, the fitness value of the global optimal solution has not improved. If this condition is met, terminate the PSO algorithm iteration process and go to step (4) to enter the tabu search stage; otherwise, go to the next step [12].
(3) Update the speed and position of each particle according to the evolution equation, recalculate the fitness of each particle, and update the optimal solution of the population history [13].
(4) From the 10 sets of iterative results with equal fitness values, select a set of solutions with the highest degree of confidence.
(5) Judging whether the termination condition of the tabu search process is satisfied, the iterative process has not improved for 20 consecutive generations or has iterated to the maximum number of iterations, then terminate the TS search and output the optimization result, otherwise go to the next step.
(6) Use the neighborhood function of the current solution to generate a certain number of neighborhood solutions, and select several candidate solutions with the highest fitness.
(7) Does each candidate solution satisfy the amnesty criterion? If it is satisfied, replace the current solution with the best candidate solution that satisfies the amnesty criterion, and replace the taboo object that entered the taboo list with the corresponding taboo object, and replace the historical optimal solution of TS with the candidate solution, and then go to step (5); otherwise, continue with the following steps.
(8) Judge the taboo attributes of each object corresponding to the candidate solution, and select the best state corresponding to the non-taboo object in the candidate solution set to replace the current solution, which

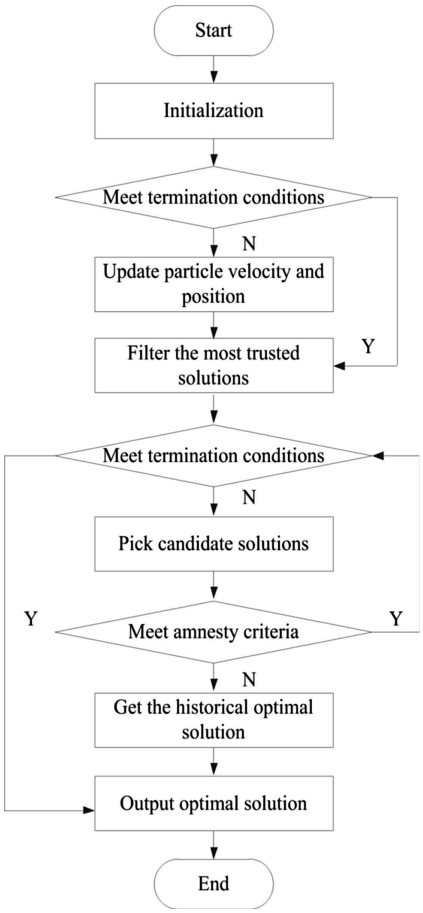

FIGURE 4. Flowchart of trusted taboo particle swarm optimization algorithm.

is the optimal solution for the security optimization of the communication network between high-power charging pile groups.

Through the above-mentioned trusted tabu particle swarm optimization steps, not only the problem of slow convergence speed existing in the traditional algorithm can be solved, but also the local optimal solution can be avoided, which helps to improve the stability and survivability of the communication network between high-power charging pile groups [14, 15].

4. FEASIBILITY SIMULATION EXPERIMENT VERIFICATION OF THE SCHEME

4.1. Experimental platform design

In order to verify the feasibility of the proposed high-power charging pile inter-group communication network security optimization scheme, a test network experimental platform including one 6LBR node, two 6LoWPAN nodes and one PC is designed. The single-chip 32-bit microcontroller TI CC2538SF53 with integrated wireless radio frequency is selected as the main control chip of the 6LBR and terminal 6LoWPAN nodes in the test network, ENC28J60 is used as the Ethernet module of the 6LBR node, and the USB serial port module is used to realize the serial communication between the PC and the development board, print serial port information.

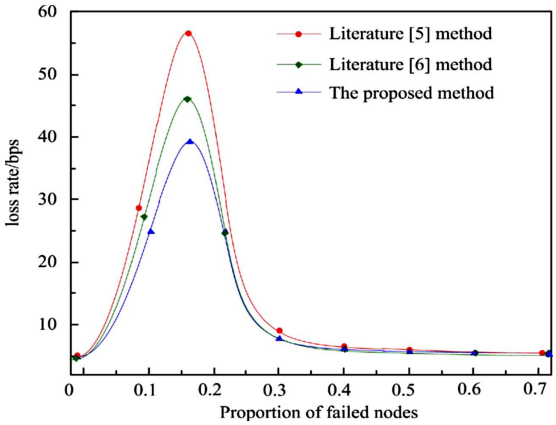

FIGURE 5. Network fault control curve.

Use Instant Contiki3.0 based on Ubuntu system as development environment, run 6LBR application program and UDP server program on embedded operating system Contiki, realize IPv6 and IEEE 802.15.4 protocol adaptation layer between protocols to support the transport of IPv6 datagrams over the IEEE 802.15.4 MAC layer. The most widely used RPL routing protocol in the 6LoWPAN network is adopted at the network layer.

In the above-mentioned experimental platform environment, the experimental research is carried out. In order to verify the effectiveness of the proposed method, the method of literature [5] and the method of literature [6] are used as comparison methods to conduct comparative analysis.

4.2. Analysis of experimental results

(1) Communication network stability

Taking the stability of the communication network as the experimental index, the method in the literature [5], the method in the literature [6] and the proposed method are used to verify the optimization effect of the communication network security. The results are shown in Figure 5.

As shown in Figure 5, under different fault proportions, the loss rate of the communication network between high-power charging pile groups presents three stages of change, the first stage is a rapid rise stage; the second stage is a rapid decline stage; the third stage is a rapid decline stage; This stage is the stationary stage. In the above three stages, the network loss rate of the proposed method is always lower than that of the literature [5] method and the literature [6] method, indicating that the proposed method can effectively suppress the impact of network failure on the stability of the communication network between high-power charging piles. influences. This is because the proposed method optimizes the communication network architecture between charging pile groups. Compared with the traditional wireless communication network of charging piles, the optimized communication network between charging pile groups can not only realize two-way communication, but also avoid the failure of the concentrator. It causes the problem of paralysis of the entire terminal network, thereby improving the stability of the communication network.

(2) Communication network invulnerability

A local observation area of the communication network between high-power charging piles with 300 nodes is established. Under this condition, the survivability of the communication network is tested, and the curve between the ratio of the average loss rate and the average disconnection is obtained as shown in the Figure 6 shown.

As shown in Figure 6, with the increase of the average disconnection ratio of the communication network between high-power charging pile groups, especially in the case of around 0.15, the average loss rate increases sharply. However, the average loss rate of the proposed method is kept at a relatively small level, indicating

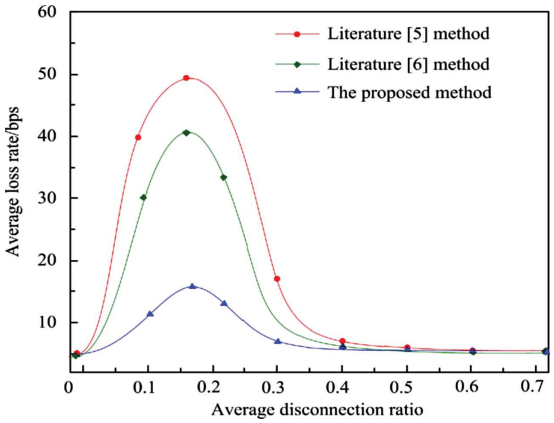

FIGURE 6. Communication network survivability verification.

TABLE 1. Convergence speed comparison.

Number of experiments/time	Convergence speed/s		
	The proposed method	Literature [5] method	Literature [6] method
1	2.35	3.25	3.55
2	2.61	3.69	3.67
3	2.97	3.97	3.94
4	3.05	4.25	4.04
5	3.12	4.63	4.28
6	3.49	4.81	4.63
7	3.66	5.09	4.99
8	3.82	5.28	5.21

that the method achieves the purpose of controlling the large-area failure loss of the communication network between high-power charging piles. The average loss rate of the literature [5] method and the literature [6] method is higher than that of the proposed method, which shows that the probability of the communication network paralysis event still exists after the traditional method is optimized.

(3) Convergence speed

In order to further verify the application value of the proposed method, with the convergence speed as the experimental index, the method in the literature [5], the method in the literature [6] and the proposed method are compared, and the results are shown in Table 1.

It can be seen from the data in Table 1 that the convergence time of the proposed method is shorter in many experiments, and the minimum value is only 2.35 s, which is 0.90 s and 1.20 s lower than the methods in literature [5] and [6], respectively. By comparison, it can be seen that the convergence speed of the proposed method is faster, and the security optimization of the communication network between high-power charging pile groups can be realized in a shorter time. This is because the proposed method uses the trusted taboo particle swarm optimization algorithm to optimize the security of the communication network between high-power charging piles.

The simulation results show that the proposed method can effectively avoid cascading failures in the communication network between high-power charging pile groups, and effectively guarantee the normal operation of the communication network.

5. Conclusion

In this paper, a method of communication network security optimization between high-power charging pile groups based on trusted tabu particle swarm optimization is proposed. The method uses 6LoWPAN technology to establish a wireless network among charging pile groups, and realizes monitoring, collection, control and billing of the operation status and data of charging piles, as well as security monitoring of charging piles. At the same time, the trusted tabu particle swarm optimization algorithm is used to improve the traditional PSO algorithm, which further improves the communication network security among high-power charging pile groups.

Conflicts of interest. The authors declare that they have no competing interests.
Data availability statement. The data used to support the findings of this study are available from the corresponding author upon request.
Funding. This study did not receive any funding in any form.

References

[1] J.A. Dominguez-Navarro, R. Dufo-Lopez, J.M. Yusta-Loyo, J.S. Artal-Sevil and J.L. Bernal-Agustin, Design of an electric vehicle fast-charging station with integration of renewable energy and storage systems. *Int. J. Electr. Power Energy Syst.* **105** (2019) 46–58.

[2] M.K. Boujelben and C. Gicquel, Efficient solution approaches for locating electric vehicle fast charging stations under driving range uncertainty. *Comput. Oper. Res.* **109** (2019) 288–299.

[3] S. Deb, A.K. Goswami, P. Harsh, J.P. Sahoo and A.S. Shekhawat, Charging coordination of plug-in electric vehicle for congestion management in distribution system integrated with renewable energy sources. *IEEE Trans. Ind. Appl.* **56** (2020) 5452–5462.

[4] S. Aznavi, P. Fajri, M.B. Shadmand and A. Khoshkbar-Sadigh, Peer-to-peer operation strategy of PV equipped office buildings and charging stations considering electric vehicle energy pricing. *IEEE Trans. Ind. Appl.* **56** (2020) 5848–5857.

[5] K. Zhou, X.D. Yang, Y.B. Zhang, Y. Chen, L.Y. Xie and J.J. Lu, An effective WSN routing protocol for electric vehicle charging piles management system. *Power Syst. Prot. Control* **45** (2017) 17–28.

[6] Q.L. Liu and C. Chen, Anonymous identity authentication scheme in V2G based on blockchain. *Comput. Eng.* **47** (2021) 22–28.

[7] K. Tan, Z.W. Li, Y.D. Guan, L. Ye, W.M. Tong and B.J. Zhang, Lightweight key management scheme based on communication system of electric vehicle charging piles. *Electr. Power Constr.* 40 (2019) 73–81.

[8] S.S. Amiripalli and V. Bobba, An optimal TGO topology method for a scalable and survivable network in IOT communication technology. *Wirel. Pers. Commun.* **107** (2019) 1019–1040.

[9] C.M. Li, C.Y. Li and L. Wang, Reliable data transmission method based on 6LoWPAN for building energy systems. *Build. Serv. Eng. Res. Technol.* **41** (2020) 623–633.

[10] J.J. Shin and H. Bang, UAV path planning under dynamic threats using an improved PSO algorithm. *Int. J. Aerosp. Eng.* **2020** (2020) 1–17.

[11] M. Sahin and T. Kellegoz, A new mixed-integer linear programming formulation and particle swarm optimization based hybrid heuristic for the problem of resource investment and balancing of the assembly line with multi-manned workstations. *Comput. Ind. Eng.* **133** (2019) 107–120.

[12] Z.S. Chafi and H. Afrakhte, Short-term load forecasting using neural network and particle swarm optimization (PSO) algorithm. *Math. Prob. Eng.* **2021** (2021) 1–10.

[13] D. Peng, G. Tan, K. Fang, L. Chen and Y. Zhang, Multiobjective optimization of an off-road vehicle suspension parameter through a genetic algorithm based on the particle swarm optimization. *Math. Prob. Eng.* 2021 (2021) 1–14.

[14] M. Taiebat and M. Xu, Synergies of four emerging technologies for accelerated adoption of electric vehicles: shared mobility, wireless charging, vehicle-to-grid, and vehicle automation. *J. Clean. Prod.* **230** (2019) 794–797.

[15] H.Q. Wang and C. Peng, Simulation of charging speed control of electric vehicle charging pile. *Comput. Simul.* **35** (2018) 171–175.