2019 IEEE 15th International Conference on Automation Science and Engineering (CASE)

Reliable Cooperative Charging Protocol against Fault Data for Supercapacitors Charging Systems

Yang Miao, Jianping He and Shanying Zhu

***Abstract*— A cooperative charging protocol for the supercapacitors on catenary-free trams is a promising method to solve the high-power-charging load. The protocol can efficiently improve the dynamic performance of the charging system by reducing the imbalances and overshoots of currents when the transfer data is highly accurate. However, it is noting that some internal circuit failures and external attacks will cause fault data, which is inevitable in the charging system. The fault data may reduce or even break the reliability of the system under the cooperative charging protocol. In this paper, we investigate the causes of fault data and what effects it may bring to the system with cooperative charging protocol. To solve the problem, we propose a reliable cooperative charging protocol with a data screening mechanism added in the existing protocol to guarantee the charging system from fault data. In addition, we show that the reliable cooperative charging protocol enhances the reliability of the charging system with fault data. Both simulations and experiments are conducted to demonstrate the effectiveness of the proposed protocol.**

***Index Terms*— cooperative charging, reliable protocol, supercapacitor, fault data, stability.**

I. Introduction

Onboard supercapacitors are widely used as energy supply devices on catenary-free trams [1]. The superiorities of supercapacitors are low visual intrusion, low cost of overhead infrastructures, great performance facing terrible weather conditions and high energy efficiency [2]. Supercapacitors are generally charged with a high constant current so that a single-module charging system can hardly satisfy due to the safety concern [3]. For example, the supercapacitors, used on the tram which has been put into use in Guangzhou, China, require a 900 A charging current from charging system [4]. Recently, a cooperative charging protocol (CCP) for supercapacitors was proposed to solve the high-power-charging load [5]. CCP can not only supply such a high charging current, but also effectively improve the dynamic performance of the charging system by reducing current imbalances and avoiding overshoots [6].

The cooperative charging protocol is a strategy based on cooperative control technique. Cooperative control technique is a promising and powerful technique in distributed power system, and it is widely used in energy management [7]. For example, [8] proposed a distributed cooperative secondary control of microgrids combining with feedback linearization, which is a secondary voltage control and is fully distributed without reference. There appears a better distributed cooperative control of DC microgrids in [9] which replaces the voltage control by a voltage regulator and a current regulator. It also adds a voltage set point to estimate the performance. Besides, a distributed networked method for load sharing in parallel DC-DC converters is proposed in [10], which uses consensus-voting protocols and voltage set point to guarantee the performance. Combining with the cooperative control techniques and the using of set point, [6] propose a cooperative charging protocol with a reference current to reduce the current imbalances and overshoots while charging for supercapacitors.

CCP is built on the assumption that the transfer data is accurate. However, the data is not always accurate, due to system internal measurement errors or external attacks, which may degrade the reliability of the system [15], [16]. For instance, hardware is vulnerable, which means that produce malfunctions are inevitable, thus the accuracy of data cannot be always guaranteed [18]. Meanwhile, considering the external attack, attackers can destroy the charging system by damaging or tampering with data, which bring serious power-loading problem for the charging system [19]–[21].

To resist the effects of fault data injected, there exists several mechanisms of detection and identification [11]–[13], [24], [25], which aim to guarantee the reliability of the systems by recognizing the fault data. But measuring errors, software errors and system failures may cause fault data which is close to actual value and changes randomly [18]. This kind of fault data is hard to be detected or identified. In the system with CCP, the fault data can unconsciously raise the charging currents of some modules, as a result, charging currents of the charging system will be oscillating without being detected. Consequently, the closed-loop system becomes unstable and the outputs oscillate, which have serious effects to the charging system. Therefore, the exist CCP is unreliable faced with fault data.

In this paper, we focus on how to improve the reliability of the charging system against fault data. Different from most related works which pay much attention to detecting and recognizing fault data [11], [12], [17], we only use a simple data screening mechanism similar to [14] to build a reliable cooperative charging protocol (RCCP). Our major contributions are summarized as follows:

- We introduce the causes of fault data in the cooperative charging system. The effects of fault data is analyzed by closed-loop system stability and simulation. It is found that fault data may disrupt the reliability of the

The authors are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Signal Processing, Ministry of Education of China, Shanghai 200240, China. E-mail:yangmiao@sjtu.edu.cn, jphe@sjtu.edu.cn, shyzhu@sjtu.edu.cn. This work is partially sponsored by the National Key R&D Program of China 2017YFE0114600, NSF of China(61622307, 61603251) and NSF of Shanghai Municipality of China(18ZR1419900).

978-1-7281-0356-3/19/$31.00 ©2019 IEEE

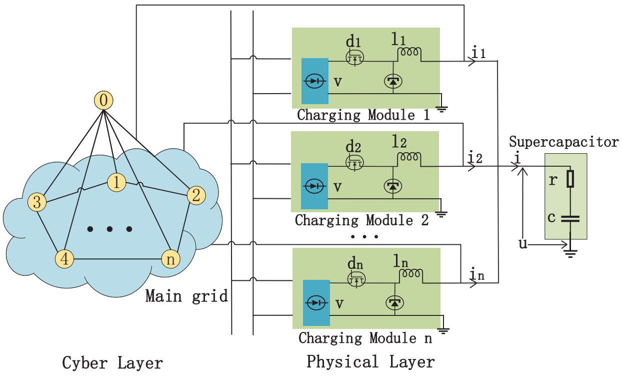


Fig. 1. Cyber and Physical Model of Cooperative Charging System

charging system by bringing power-loading problem.

- We propose a RCCP for the charging system with a data screening mechanism added in the cooperative charging protocol. We show that RCCP effectively guarantees the reliability of three-module cooperative charging system from fault data.
- Simulations are conducted to demonstrate the effectiveness of RCCP. We also provide experiments of the charging system to verify the reliability of the system with RCCP again fault data.

The remainder of this paper is organized as follows. Section II introduces the cyber-physical model of cooperative charging system and the causes and effects of fault data. In Section III, we design a reliable cooperative charging protocol and analyze the stability of the protocol. Section IV provides simulations and experiments. The conclusions are given in Section V.

II. Effects of Fault Data to the Charging System

In order to investigate the effects of fault data, in this part, we introduce the cooperative charging system model of supercapacitors simply. Then, we discuss the causes and effects of fault data to the system.

A. Cooperative Charging System Model

The cyber-physical model of the cooperative charging system is shown in Fig. 1 [5]. There are n charging modules whose inputs are supplied by main grid and outputs are going to charge for supercapacitors. The AC inputs are rectified to DC sources v by rectifiers, and the DC sources are controlled by control signals $d_1, d_2, ..., d_n$. Finally, the outputs of all the charging modules charge supercapacitors together. The supercapacitors are represented by a single R-C model which is the most popular supercapacitor model in electrical applications [22], [23].

The mathematical model got from the physical model is

$$\left\{\begin{array}{rcl} l_k\dfrac{\mathrm{d}i_k}{\mathrm{d}t} & = & vd_k - u, k = 1, 2, ..., n \\ c\dfrac{\mathrm{d}u}{\mathrm{d}t} & = & rc\dfrac{\mathrm{d}i}{\mathrm{d}t} + i, \end{array}\right. \tag{1}$$

where v is the DC source voltage for each charging module, l_k and d_k are the inductor and the control signal (duty cycle) of module k, i_k is the output charging current of module k, r, c are the equivalent resistance and equivalent capacitance of supercapacitors, u is the voltage of supercapacitors as shown in Fig. 1. $i = i_1 + i_2 + ... + i_n$ is the charging current for supercapacitors gotten from the cooperative charging system.

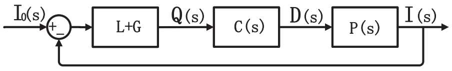


Fig. 2. Block diagram of the closed-loop control system

Based on the cooperative idea, the deviation of module k, q_k, is calculated as

$$q_k = g_{0k}(i_0 - i_k) + \sum_{m\in N} a_{km}(i_m - i_k), \tag{2}$$

where g_{0k} is the pinning gain whose value here is 1, N is the set of all charging modules, a_{km} is the adjacent element whose value is 1 when module m is the neighboring module of module k, otherwise, $a_{km} = 0$. i_0 is reference current, i_ms are the charging currents in neighbor modules of module k.

To analyze the charging system conveniently, based on the cooperative charging system model, a block diagram of closed-loop control system is built which is shown in Fig. 2 [6]. L is the Laplacian matrix and G is the pinning matrix [5]. PI controller $C(s)$ is given as

$$C(s) = K(T + \frac{1}{s}). \tag{3}$$

I_0, Q, D, I represent the matrix of reference currents, deviations, control signals and charging currents as

$$\left\{\begin{array}{ccl} I_0 & = & [i_0 \quad i_0 \quad ... \quad i_0]^T, \\ Q & = & [q_1 \quad q_2 \quad ... \quad q_n]^T, \\ D & = & [d_1 \quad d_2 \quad ... \quad d_n]^T, \\ I & = & [i_1 \quad i_2 \quad ... \quad i_n]^T, \end{array}\right. \tag{4}$$

where $q_1, q_2, ..., q_n$ and $d_1, d_2, ..., d_n$ are the deviations and the control signals(duty cycle) of module $1, 2, ..., n$.

Transfer the time-domain model of the cooperative charging system to a frequency-domain model as

$$I(s) = P(s)D(s). \tag{5}$$

Assume that $l_k = l$, the n-order transfer function matrix $P(s)$ of the cooperative charging system satisfies

$$P(s) = v\Psi(s)^{-1}, \tag{6}$$

where

$$\Psi(s) = \begin{bmatrix} sl + r + \dfrac{1}{sc} & r + \dfrac{1}{sc} & \cdots & r + \dfrac{1}{sc} \\ r + \dfrac{1}{sc} & sl + r + \dfrac{1}{sc} & \cdots & r + \dfrac{1}{sc} \\ \vdots & \vdots & \cdots & \vdots \\ r + \dfrac{1}{sc} & r + \dfrac{1}{sc} & \cdots & sl + r + \dfrac{1}{sc} \end{bmatrix}. \tag{7}$$

Remark 2.1: Based on (6) and (7), we get n-order transfer function matrix $P(s)$ as

$$P(s) = \begin{bmatrix} P_1(s) & -P_2(s) & \cdots & -P_2(s) \\ -P_2(s) & P_1(s) & \cdots & -P_2(s) \\ \vdots & \vdots & \cdots & \vdots \\ -P_2(s) & -P_2(s) & \cdots & P_1(s) \end{bmatrix}, \quad (8)$$

where

$$\begin{cases} P_1(s) & = & v\dfrac{cls^2 + (n-1)crs + (n-1)}{cl^2s^3 + ncrls^2 + nls}, \\ P_2(s) & = & v\dfrac{crs + 1}{cl^2s^3 + ncrls^2 + nls}. \end{cases} \quad (9)$$

B. Causes of Fault Data

The cooperative charging system charges for supercapacitors basing on the assumption that the transfer data is correct. However, transfer data is not always accurate, for fault data being inevitable. The causes of fault data can be summarized as follows:

1) The vulnerabilities of hardware and software peripherals will cause produce malfunctions and measuring errors after hardware has been used for a long time.
2) Malicious modifications to the integrated circuits based computing hardware will also cause fault data.
3) External attacks may intercept or destroy the transfer data, attackers may even posed as a charging module to deliberately deliver fault data.

Though there are many attack detections and identifications proposed to recognize the attackers or fault data, the fault data which changes randomly in a small range is still stealthy and undetectable.

C. Effects of Fault Data

Consider the cooperative charging system with fault data, apart from the part with reference current and neighboring modules, there is a new part in deviation Q, which is caused by fault data.

$$Q = (L + G)(I_0 - I) + R, \quad (10)$$

where $R = [r_1, r_2, ..., r_n]^T$ represents the gaps between fault data and actual values. If the module with fault data is a neighboring module of module k, $r_k = r$, otherwise, $r_k = 0$. We can obtain the relationships among charging currents I and reference current I_0, gaps R as

$$I = [E + PC(L + G)]^{-1}PC[(L + G)I_0 + R], \quad (11)$$

where E is n-order identity matrix. We can see that charging currents cannot be settled in reference current any more with fault data as long as $R \neq 0$. No matter r is random value caused by hardware failure or special distribution caused by attackers, fault data will always keep charging currents from following reference current. To analyze the worst effect of fault data, we suppose that r is a positive random value which may cause power-loading problem.

The system under fault data turns into a closed-loop control system with disturbance. The disturbance makes the charging system unstable and the output become oscillating. With disturbance, the charging currents can be higher than reference current for a long time. In this case, the fault data causes high-power-loading problem which makes the charging system paralysis or even destroys the supercapacitors.

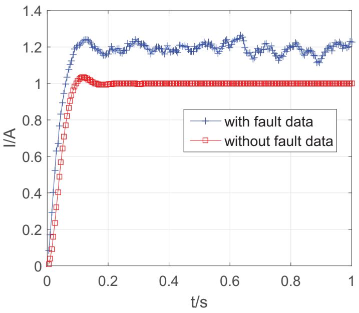


Fig. 3. The Affect of Fault Data to Charging Current

TABLE I

THE PARAMETERS OF THE THREE-MODULE CHARGING SYSTEM

v	c	r	l	K	T
24V	100F	5m	10mH	1.5	1/60

We suppose that all the charging modules receive the fault data during the charging process. We design a three-module charging system whose parameters are sited as Table I. We set reference current as $I_0 = 1A$ and the range of the random value r_k as $(0, 0.2)$. In the system, any two modules are neighboring modules of the rest module. Thus the Laplacian matrix L and pinning matrix G are given by

$$L = \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}, G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (12)$$

The value of the data received in module 1 and module 2 is randomly bigger than the actual value of module 3, which is used to simulate the fault data. The result of comparison between the charging current with fault data and that without fault data of module 1 is showed in Fig. 3.

It is observed that the charging current of the cooperative charging system with fault data is oscillating while that without fault data following the reference current $1A$. The charging current with fault data is fluctuating and is always higher than the reference current. In this case, the threat to the charging system and supercapacitors increases and the high current may cause high-power-loading problem, which also increases the risk of disabling the charging system.

III. RCCP AGAINST FAULT DATA

For the fault data being always bigger than actual value, it is easy to design a simple strategy. When a charging module receives the data from its neighboring modules, it judges whether the charging current is higher than the reference current. If the charging current itself is higher than the reference current, the module refuses to use the data. Otherwise, the module uses the data to obtain its control signal normally. That means after the charging current has surpassed reference current, the module only uses the reference current. This strategy can effectively defend the system from fault data which is higher than actual charging currents.

However, this strategy has a bad performance in reducing overshoot and imbalance of the charging currents because it is not a cooperative charging system any more when the charging current exceeds the reference current. Therefore, we propose a reliable cooperative charging protocol (RCCP) which combines the superiorities of this secure strategy and CCP. RCCP only adds a data screening mechanism into CCP, so it has a low computational complexity.

A. *Reliable Cooperative Charging Protocol*

The charging currents are supposed to track the reference current which is a constant, so we design a data screening mechanism in each charging module after receiving the data from its neighboring modules. Firstly, the module checks that whether the gap between the charging current of itself and the reference current is bigger than that on the previous sampling time. If the former is smaller, which means that the charging current is narrowing the gap with the reference current, so there is no need to add extra part while calculating the deviations. Otherwise, the module use the data whose value is between the charging current of itself and reference current. In this way, the module only uses the data which promotes the charging current to track the reference current and avoid excessive integral effects. The information checking process is described as follows.

1) For module k, if the gap between its charging current and the reference current is decreasing which means $|i_k(j) - i_0(j)| < |i_k(j-1) - i_0(j-1)|$, j represents the j_{th} sampling time, there is no need to add extra part while calculating the deviation. Then the deviation is obtained as follows
$$q_k = i_0 - i_k. \qquad (13)$$
2) Otherwise, to narrow the gap between charging current and reference current and avoid current imbalance, we should use the data from neighboring modules. If the charging current of module k is smaller than the reference current, module k uses the data of neighboring module m which satisfies $i_k < i_m < i_0$ to calculate the deviation. In this way, the charging module uses the data from module m to accelerate the charging current of module k to follow the reference current. The module abandons the data from module m to calculate the deviation of module k which avoids the excessive integral effect of module k.
3) Similarly, if the charging current of module k is bigger than the reference current, module k uses the data of neighboring module m which satisfies $i_0 < i_m < i_k$ to calculate the deviation.

B. *Algorithm of RCCP*

We describe the detail of RCCP in Algorithm 1 which is based on the cooperative charging system. For module k, we definite the j_{th} sampling time by j, and the set of neighboring modules by M_k.

Algorithm 1 Data Screening Mechanism of RCCP

```
Input: Reference current $i_0(j)$, the charging current of
    module $k$, $i_k(j)$, the charging current of neighboring
    module, $i_m(j)$, $m \in M_k$.
Output: The deviation of module $k$, $q_k(j)$.
$q_k(j) = i_0(j) - i_k(j)$.
if $|i_k(j) - i_0(j)| > |i_k(j-1) - i_0(j-1)|$ then
    if $i_k(j) - i_0(j) < 0$ then
        for $m \in M_k$ do
            if $i_k(j) - i_0(j) < i_k(j) - i_m(j) < 0$ then
                $q_k = q_k + i_m - i_k$
            end if
        end for
    end if
    if $i_k(j) - i_0(j) > 0$ then
        for $m \in M_k$ do
            if $i_k(j) - i_0(j) > i_k(j) - i_m(j) > 0$ then
                $q_k = q_k + i_m - i_k$
            end if
        end for
    end if
end if
```

C. *Stability of RCCP*

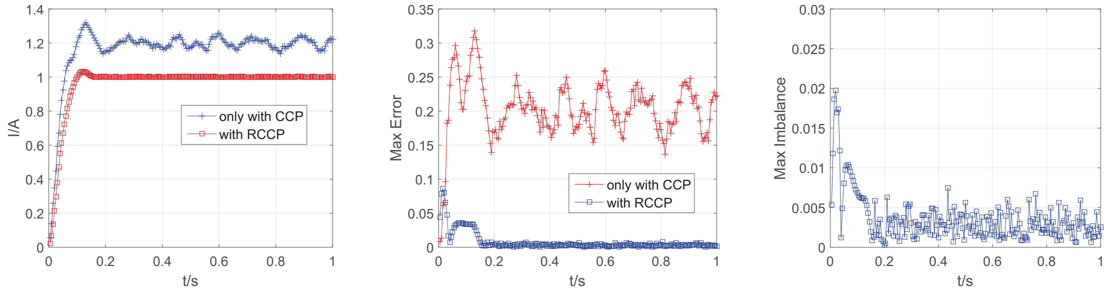
We discuss the deviation q_k in the charging system with RCCP and build a new closed-loop control system. Then, we use Routh Criterion to analyze the stability of the charging system with RCCP.

Theorem 3.1: With RCCP, we can use a λ_k satisfying $1 \leq \lambda_k \leq n$ to simplify q_k as
$$q_k = \lambda_k(i_0 - i_k), \qquad (14)$$

Proof: Consider the charging system with RCCP no matter whether there exists fault data or not. If there is no need to use the data from neighboring modules, the deviation is given by (13). There are two situations under which the charging module will use the data from neighboring modules in RCCP. For module k, only when $i_k < i_m < i_0$ or $i_0 < i_m < i_k$ will it use the data from module m.

When $i_k < i_0$, the deviation is given by
$$q_k = i_0 - i_k + \sum_{m \in M_k} (i_m - i_k), \qquad (15)$$
$$M_k = \{m | i_k < i_m < i_0, \text{module m is the neighboring module of module k}\}.$$

From the conditions of module m which passes the data screening mechanism, it can be seen that $i_0 - i_k > i_m - i_k > 0$. Then, the range of q_k is changed as
$$i_0 - i_k \leq q_k \leq n(i_0 - i_k). \qquad (16)$$
We define that q_k is λ_k times $(i_0 - i_k)$. Then, we obtain
$$q_k = \lambda_k(i_0 - i_k), 1 \leq \lambda_k \leq n. \qquad (17)$$
The condition is similar when $i_k > i_0$. Therefore, it is feasible to use (17) to represent q_k. ■



(a) Charging Current under Fault Data (b) Maximum Error under Fault Data (c) Maximum Current Imbalance

Fig. 4. Simulation Results of the Charging System with RCCP

With Theorem 3.1, we simplify the Laplace Matrix L and the pinning matrix G to Λ, where $\Lambda = \mathrm{diag}\{\lambda_k\}_n$. In this case, RCCP zooms in the proportion coefficient, K, in a bounded range even with fault data. Thus, the charging currents will still follow the reference current which is a constant. Then, we get a new closed-loop block diagram shown in Fig. 5 during each sampling time. In this case, the closed-loop control system is simpler and the characteristic equation is less difficult to be solved.

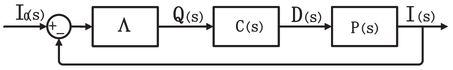


Fig. 5. Block Diagram of the System with RCCP

Add RCCP to the three-module charging system whose parameters are set as Table I, we get

$$\begin{cases} P_1(s) &= \dfrac{4800(s^2+s+2)}{2s^3+3s^2+6s}, \\ P_2(s) &= \dfrac{2400(s+2)}{2s^3+3s^2+6s}. \end{cases} \tag{18}$$

and

$$\Lambda = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}. \tag{19}$$

The closed-loop characteristic equation(CLCE) is the equation formed by the denominator of closed-loop transfer function matrix. So we obtain the CLCE of the charging system with RCCP as

$$\det(E + P(s)C(s)\Lambda) = 0, \tag{20}$$

From (3), (8), (18) and (19), the CLCE is obtained as

$$a_6s^6 + a_5s^5 + a_4s^4 + a_3s^3 + a_2s^2 + a_1s^1 + a_0 = 0, \tag{21}$$

where

$$\begin{cases} a_6 &= 2, \\ a_5 &= 3 + 120\sum_{n=1}^{3}\lambda_n, \\ a_4 &= 6 + 7320\sum_{n=1}^{3}\lambda_n + 7200\sum_{n=1}^{3}\lambda_1\lambda_2\lambda_3/\lambda_n, \\ a_3 &= 4.3\times10^5(2\sum_{n=1}^{3}\lambda_1\lambda_2\lambda_3/\lambda_n + \lambda_1\lambda_2\lambda_3), \\ a_2 &= 2.6\times10^7(\sum_{n=1}^{3}\lambda_1\lambda_2\lambda_3/\lambda_n + 3\lambda_1\lambda_2\lambda_3), \\ a_1 &= 4.7\times10^9\lambda_1\lambda_2\lambda_3, \\ a_0 &= 9.3\times10^{10}\lambda_1\lambda_2\lambda_3, \end{cases} \tag{22}$$

and $1 \le \lambda_1, \lambda_2, \lambda_3 \le 3$.

We use Routh Criterion to analyze the stability of the system. By rigorously calculating, we find that whatever the values of $\lambda_1, \lambda_2, \lambda_3$ are between 1 and 3, the elements in first row of the Routh-Hurwitz Table are always positive. According to Routh Criterion, during each sampling time, the system of (21) is stable. Therefore, by using RCCP in the three-module charging system, the charging current of each module is going to follow the reference current even under fault data.

Although the analysis of stability is based on the three-module charging system, the proof of the stability for n-module charging system is similar. Thus RCCP is generally reliable and can be used in any dimension charging systems.

IV. Simulation and Experiment Result

Both simulation and experiment are conducted to demonstrate the effectiveness of RCCP.

A. Simulation Results

We have a discrete simulation in MATLAB, the parameters are set as showing in Table I. The results are showed in Fig. 4(a), Fig. 4(b) and Fig. 4(c).

Figure. 4(a) shows that under the fault data, the charging current with RCCP tracks the reference current whose value is $1A$ while that without RCCP is fluctuating. The overshoot of the output with RCCP is 2.9%, much smaller than that with fault data but without RCCP. We definite the maximum error with the maximum deviation between the charging current of each single charging module and the reference current. In Fig. 4(b), the maximum error under fault data without RCCP is extremely big and unstable. The big and unstable error may cause great dangers for charging system. The maximum error with RCCP rapidly turn to 0, which means RCCP can avoid the big and unstable error. Fig. 4(c) shows that the maximum current imbalance of the charging system under RCCP is always smaller than 2% so that RCCP reduces the threat of big current imbalance. The simulation results show that RCCP is effective in resisting fault data.

B. Experiment Results

Consider the three-module cooperative charging system whose parameters are set in Table I. The experiment platform of the three-module charging system is shown in Fig. 6. The experiment platform consists of a power source, three charging modules, a STM32F207, a computer and supercapacitors.

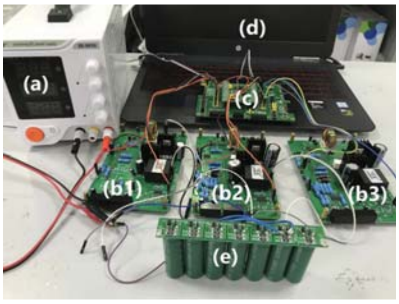
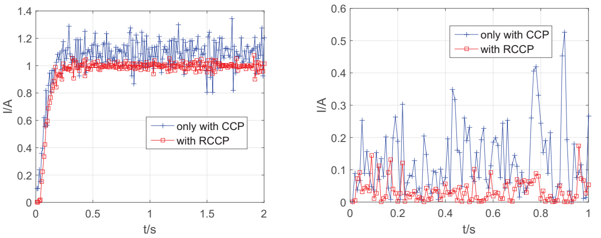


Fig. 6. Experiment Platform of the charging system. (a)Power source. (b1)-(b3)Three charging modules. (c)STM32F207. (d)PC. (e)Supercapacitors.



(a) Charging Current

(b) Maximum Current Imbalance

Fig. 7. Experiment Results with RCCP and Fault Data

We simulate the cooperative communication and PI control in STM32F207. To imitate fault data, we set a random value added to the communication. The experiment result is shown in Fig. 7(a) and Fig. 7(b).

In Fig. 7(a), we can see that without RCCP, charging current is extremely unstable under fault data, and the maximum value is 35% higher than the reference current $1A$. RCCP suppresses the overshoot of the charging current within 5% and the charging current follows closely the reference current. Fig. 7(b) shows that the maximum current imbalance of the charging system with RCCP is always smaller than that only with CCP. The stable charging current guarantees the reliability of the charging system. The experiment results also show that RCCP effectively improves the stability and security of the charging system.

V. Conclusions

In this paper, we study the reliability of the cooperative charging system for onboard supercapacitors of catenary-free trams. Considering fault data caused by vulnerable hardware or malicious attacks, we discuss the effects of fault data to the cooperative charging system by analysis and simulations. Based on the characteristic of the cooperative charging protocol, we propose a reliable cooperative charging protocol with a data screening mechanism to remove the effects of the fault data and improve the reliability of the charging system. We also prove the validity of the protocol. Finally, we show the effectiveness of the reliable cooperative charging protocol by both simulations and experiments.

References

[1] A. L. Allegre, A. Bouscayrol, P. Delarue, P. Barrade, E. Chattot, and S. El-Fassi, “Energy storage system with supercapacitor for an innovative subway,” *IEEE Trans. Ind. Electron.*, 57(12): 4001-4012, Dec. 2010.

[2] Technology briefing paper: Catenary free tram operation, UK Tram, London, U.K., Sep. 2012.

[3] “Union station to georgetown propulsion study: Alternatives analysis for premium transit service,” *Dept. Transp., Deportment Transp.*, Washington, DC, USA, Tech. Rep., Sep. 2013.

[4] M. Li, “Analysis on main technical characteristics of Guangzhou Haizhu Tram,” *Modern Urban Transit*, 3(5): 24-26, 2014.

[5] H. Li, J. Peng, R. Zhou, Z. Huang, and J. Pan, “A cooperative charging strategy for onboard supercapacitors of catenary-free trams,” in *Proc. IEEE ECCE*, 2016.

[6] H. Li, J. Peng, J. He, R. Zhou, Z. Huang, and J. Pan, “A cooperative charging protocol for onboard supercapacitors of catenary-free trams,” *IEEE Trans. Control Syst. Technol.*, 26(4): 1219-1232, July. 2018.

[7] A. Bidram, F. L. Lewis, A. Davoudi, “Distributed control systems for small-scale power networks: Using multiagent cooperative control theory,” *IEEE Control Syst. Mag.*, 34(6): 56-77, Dec. 2014.

[8] A. Bidram, A. Davoudi, F. L. Lewis, J. M. Guerrero, “Distributed cooperative secondary control of microgrids using feedback linearization,” *IEEE Trans. Power Syst.*, 28(3): 3462-3470, Aug.2013.

[9] V. Nasirian, S. Moayedi, A. Davoudi, F. L. Lewis, “Distributed cooperative control of DC microgrids,” *IEEE Trans. Power Electron.*, 30(4): 2288-2303, Apr. 2015.

[10] S. Moayedi, V. Nasirian,F. L. Lewis, A. Davoudi, “Team-Oriented load sharing in oarallel DC-DC converters,” *IEEE Trans. Ind. Appl.*, 51(1): 479-490, Jan./Feb. 2015.

[11] J. He, L. Cai, and X. Guan, “Preserving Data-Privacy with Added Noises: Optimal Estimation and Privacy Analysis,” *IEEE Trans. Inf. Theory*, 64(8): 5677-5690, 2018.

[12] F. Miao, Q. Zhu, M. Pajic, George J.Pappas, “Coding schemes for securing cyber-physical systems against stealthy data injection attacks,” *IEEE Trans. Cont. Netw. Syst.*, 4(1): 106-117, Mar. 2017.

[13] F. Pasqualetti, F. Dorfler, F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Trans. Autom. Control* , 58(11): 2715-2729, June. 2013.

[14] J. He, P. Cheng, L. Shi, J. Chen, and Y. Sun, “Time Synchronization in WSNs: A Maximum-Value-Based Consensus Approach,” *IEEE Trans. Autom. Control*, 59(3): 660-675, 2014.

[15] Y. Mo, E. Garone, A. Casavola,B. Sinopoli, “False data injection attacks against state estimation in wireless sensor networks,” in *IEEE CDC*, 2010.

[16] F. Hou, Z. Pang, Y. Zhou, D. Sun, “False data injection attacks for a class of output tracking control systems,” in *IEEE CCDC*, 2015.

[17] J. He, L. Cai, P. Cheng, J. Pan, and L. Shi, “Consensus-based Data-privacy Preserving Data Aggregation,” *IEEE Trans. Autom. Control*, doi: 10.1109/TAC.2019.2910171.

[18] K. Lingasubramanian, R. Kumar, N. B. Gunti, T. Morris, “Study of hardware trojans based security vulnerabilities in cyber-physical systems,” in *IEEE ICCE*, 2018.

[19] M.A. Eahman, H. Mohsenian-Rad, “False data injection attacks against nonlinear state estimation in smart power grids,” in *IEEE Power&Energy Society General Meeting*, 2013.

[20] J. Zhao, G. Zhang, Z. Dong, K. Wong, “Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation,” *IEEE Trans. Smart Grid*, 7: 6-8, Jan. 2016.

[21] MA. Islam, S. Ren, A. Wierman, “Exploiting a thermal side channel for power attacks in multi-tenant data centers,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.

[22] T. Ma, H. Yang, and L. Lu, “Development of hybrid batteryCsuper-capacitor energy storage for remote area renewable energy systems,” *Appl. Energy*, 153: 56-62, Sep. 2015.

[23] O. Bohlen, J. Kowal, and D. U. Sauer, “Ageing behaviour of electrochemical double layer capacitors: Part I. Experimental study and ageing model,” *J. Power Sour.* 172(1): 468-475, Oct. 2007.

[24] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Trans. Autom. Control*, 58(11): 2715-2729, Nov. 2013.

[25] R. Cao, “Detecting arbitrary attacks using continuous secured side information in wireless networks,” *IEEE Access*, 5:25927-25945, 2017.