Cybersecurity of Electric Vehicles Charging Systems By Using Residual Generation Technique

Mohammad Anvaripour [1], S.M.Mahdi Alavi [2], MARTIN HAYES [1], and Mehrdad Saif [1]

[1]Affiliation not available
[2]University of Windsor

October 30, 2023

Abstract

With the rapid penetration of electric vehicles (EVs), the security of EV charging systems is becoming an important issue. This paper addresses cyber-physical protection of EV charging systems from the perspective of control theory. By using a residual generation technique, an attack-resilient EV charging system is designed, which detects false data injection under the denial of service (DOS) attack. The effectiveness of the proposed attack-resilient EV charging system is verified experimentally by using a hardware-in-the-loop testbed, developed by the IEEE 802.15.4 wireless sensors.

Cybersecurity of Electric Vehicles Charging Systems By Using Residual Generation Technique

Mohammad Anvaripour, S.M.Mahdi Alavi*, Martin J. Hayes, Mehrdad Saif

***Abstract*—With the rapid penetration of electric vehicles (EVs), the security of EV charging systems is becoming an important issue. This paper addresses cyber-physical protection of EV charging systems from the perspective of control theory. By using a residual generation technique, an attack-resilient EV charging system is designed, which detects false data injection under the denial of service (DOS) attack. The effectiveness of the proposed attack-resilient EV charging system is verified experimentally by using a hardware-in-the-loop testbed, developed by the IEEE 802.15.4 wireless sensors.**

***Index Terms*—Cybersecurity, Cyber-physical Systems, Electric Vehicles, Charging Systems, Residual Generation.**

I. Introduction

In the near future, it is expected that a numerous number of electric vehicle (EV) chargers are installed all around the world, [1]. Approximately 80,000 home and public EV chargers were deployed in the United States in 2018 [2]. In China, this number has reached to around 808,000 in January 2019 [3]. Charging points are typically unmanned and partially located in remote areas, where cyber-physical protection is not guaranteed [4]. In order to address this issue, the European network of cyber security (ENCS), and the European distribution system operators' association for smart grids (E.DSO) aimed to standardize cyber-security requirements for EV charging systems [5].

Based on the classification in [5], an EV charging system, as shown in Figure 1, is composed of three main parts: charge points, charge point operators (CPOs), and distribution system operators (DSOs). The charge point is responsible for measurements from EV sensors, control of energy transfer from the charge point to EV, identifying and authorizing EV users via user authentication component, and enabling some remote capabilities such as adjustment of the charge point's maximum energy via the local controller component over a wide area network (WAN). CPO is mainly an interface between the charge point and DSO. Its role is to collect and process the data of charge points. CPO provides charge points with the information about energy limits based on the DSO data. DSO aims to forecast the available capacity of the grid, ensure power supply stability, etc.

EV charging system is susceptible to various cyber-attacks such as denial of service (DOS), and false data injection. In a DOS attack, sending and receiving the data is deteriorated by injection a large volume of data, which worsens data transfer time-delay and packet dropout and impairs the system performance [7], [8], [9], [10]. The false data injection aims to change the states', sensors' and actuators' data and deceive the control system and charge algorithms [7], [8], [9], [10], [11]. Design and implementation of attack-resilient cyber-physical systems have been an important research topic of control theory. Modeling of cyber-attacks has been addressed in [7], [8], [9], [10], [11], [12]. Detectability and identifiability of attacks have been discussed in [9]. Several detection and defense mechanisms have been proposed by using physical watermarking [8], observers [12], residual-based detectors [13], detection and identification filters [14].

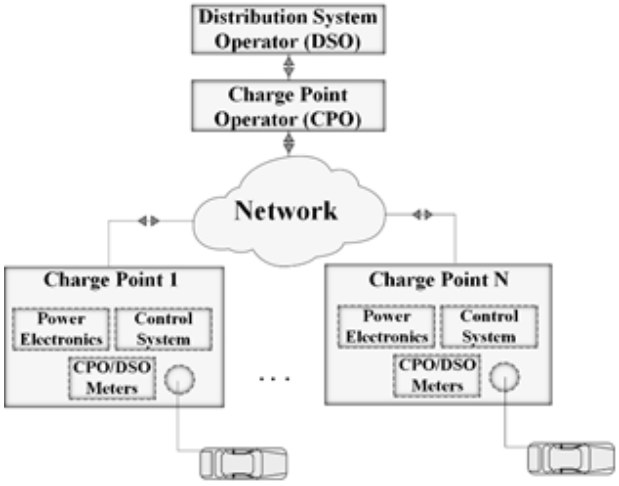

Fig. 1. Schematic of the Electric Vehicle (EV) charging system

This paper focuses on the cyber-physical protection of charge points and CPOs in EV charging systems. An attack-resilient EV charging system is designed by using an H_∞-based residual generation technique, which detects false data injection under the DOS attack. The effectiveness of the proposed attack-resilient EV charging system is verified experimentally by using the IEEE 802.15.4 wireless sensor technology.

The rest of this paper is organized as follows. In section II, the cyber-physical problem in EV charging systems is stated and formulated. In section III, a method is proposed for the detection of false data injection under DOS. The results are shown and discussed in Section IV.

M. Anvaripour, S. M. M. Alavi, and M. Saif are with the Department of Electrical and Computer Engineering, University of Windsor, 41 Sunset Avenue, Windsor, ON, Canada, N9B 3P4.

M. J. Hayes is with the Department of Electronic and Computer Engineering, University of Limerick, Limerick, V94 T9PX, Ireland.

*Corresponding author: mahdi.alavi.work@gmail.com

II. Modeling and Problem Statement of Cyber-Physical EV Charging System

The operation of the cyber-physical EV charging system is as follows. Charge points collect and send the information of EV batteries to CPO through a WAN, in real-time. It is assumed that attackers inject a large volume of data, which causes random packet dropout and DOS. Simultaneously, a bias is occurred on the battery sensor, which could be due to either a cyber-attack or hardware/software malfunctions. CPO aims to detect and inform the charge point of the sensor fault in the present of packet dropout.

A. Mathematical Modeling

In this work, state-of-charge (SOC) of the battery is used as the metric for the determination of the battery state. 0% SOC means battery is discharged, and 100% SOC means battery is fully charged. The first-order discrete-time Randles equivalent circuit model [15], [16] of the EV battery is used for the computation of its SOC as follows [17].

$$x_{(k+1)T_s} = Ax_{kT_s} + Mh_{kT_s} + B_1 u_{kT_s} + B_2 f_{kT_s} \quad (1)$$

$$y_{kT_s} = Cx_{kT_s} \quad (2)$$

with

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 - \frac{T_s}{R_1 C_1} \end{bmatrix},\ B_1 = \begin{bmatrix} T_s \\ T_s \end{bmatrix},$$
$$B_2 = \begin{bmatrix} T_s/Q \\ T_s \end{bmatrix},\ C = \begin{bmatrix} 1 & 0 \end{bmatrix}.$$

In these equations, $x = [SOC \quad q]^T$ is the state vector given in terms of battery's SOC and the amount of charge q. The superscript T denotes the transpose operator. u is the battery current, y is the output of the system, Q denotes the charge capacity, and R_1 and C_1 are the Randles circuits parameters, representing electrochemical reactions inside the batteries. The values of these parameters are chosen within the typical range of batteries as follows: $Q = 3921C$, $R_1 = 0.01\Omega$, and $C_1 = 100F$. A, B_1, B_2, and C are system matrices. The variable h accounts for the tolerance of measurements, which can be weighted by the gain of M. In this paper, 1% tolerance is considered on the SOC and q measurements, which is equivalent to $M = 10^{-2}[1 \quad 1]^T$, and a zero-mean random function h is used with the variance of 0.01. The variable f represents the fault due to false data injection or hardware/software malfunctions. T_s is the sampling time, chosen $0.5s$. For simplicity, T_s is omitted from the subscripts hereafter, i.e., $x_(kT_s)$ is written as x_k.

The battery's SOC, y, is digitized and transmitted through WAN to CPO. CPO might not receive the data due to the DOS cyber-attack. The received data at CPO is then formulated as follows:

$$z_k = \alpha_k \text{round}(Cx_k) + D_1 w_k \quad (3)$$

where α_k is a random variable. It is 1 when y_k is successfully received to CPO, otherwise it is 0. It is assumed that the random variable α_k is a Bernoulli distributed sequence with

$$\text{Prob}\{\alpha_k = 1\} = \mathbb{E}\{\alpha_k\} = \alpha \quad (4)$$

where α is a positive real number within the interval $(0, 1]$, and $\mathbb{E}\{\alpha_k\}$ stands for the expectation of the random variable α_k. The packets are then dropped with an expectation of

$$\alpha' = 1 - \alpha. \quad (5)$$

This model of packet drop has widely been used in the networked control and fault diagnosis systems, see [18] and references therein. Due to the exitance of the random variable α, the cyber-physical EV charging system (1)-(4) is stochastic. The signal w_k represents the computational errors due to the rounding function. It is assumed that w_k is white Gaussian number sequence with zero mean and bounded standard deviation.

B. Problem Statement

The problem is then stated as follows: *By using the received data z_k, CPO aims to detect f_k under random packet drop with the probability α.*

C. Assumptions

In this work, It is assumed that h_k is bounded with respect to x_k, i.e., there is a matrix H which yields

$$\|Mh_k\| \leq \|Hx_k\|. \quad (6)$$

It is also assumed that the battery model (1)-(2) is asymptotically mean-square stable.

Definition 1: (Definition 1 in [18]) The stochastic system (1)-(4) is said to be asymptotically mean-square stable if there exist real scalars $0 < \phi \leq 1$, $\mu_1 \geq 0$ and $\mu_2 > 0$, such that:

$$\mathbb{E}\left\{\|x_k\|^2\right\} \leq \mu_1 + \mu_2(1-\phi)^k, \text{for } k \in \mathbb{I}_0^+. \quad (7)$$

where, $\mathbb{I}_0^+$ is the set of positive integers including zero, i.e., $\mathbb{I}_0^+ = \{0, 1, 2, 3, \cdots\}$. The notation $\|x_k\|$ refers to the Euclidean vector norm of x_k which is $\|x_k\| = \left(x_k^T x_k\right)^{1/2}$. □

In fact, the embedded controller within the charge point is designed to make (1)-(4) asymptotically mean-square stable.

III. Detection Method Using Residual Generation

In the proposed method, a residual filter is designed, which aims to track f_k. The residual filter takes feedback from z_k and generates a residual signal r_k as follows:

$$\hat{x}_{k+1} = A_f \hat{x}_k + B_f z_k \quad (8)$$

$$r_k = C_f \hat{x}_k \quad (9)$$

where, $\hat{x}_k$ is the state vector of the residual filter. Let us assume that both x_k and $\hat{x}_k$ belong to teh same space $\mathbb{R}^2$. A_f, B_f, and C_f are matrices of the residual filter. This paper presents a method for the design of these parameters.

In practice, it is sometimes desired to weight the variable f as follows [19]:

$$\bar{x}_{k+1} = A_t \bar{x}_k + B_t f_k \quad (10)$$

$$\bar{f}_k = C_t \bar{x}_k + D_t f_k \quad (11)$$

where $\bar{x}_k$ is the state vector of the weighting function. A_t, B_t, C_t, and D_t are matrices of the weighting function, which

are determined prior to the design, based on the nature of the system and design requirements. It is simple to show that the combination of (1)-(11) results in the following compact state-space equations [18]:

$$\eta_{k+1} = \hat{A}\eta_k + (\alpha_k - \alpha)\,\tilde{A}\eta_k + \hat{M}\hat{h}_k + \hat{B}d_k + (\alpha_k - \alpha)\,\tilde{B}d_k \tag{12}$$

$$e_k = \hat{C}\eta_k + \hat{D}d_k \tag{13}$$

where,

$$e_k = r_k - \bar{f}_k, \tag{14}$$

and,

$$\eta_k = \begin{bmatrix} x_k \\ \hat{x}_k \\ \bar{x}_k \end{bmatrix},\ \hat{h}_k = \begin{bmatrix} h_k \\ 0 \\ 0 \end{bmatrix},\ d_k = \begin{bmatrix} w_k \\ v_k \\ f_k \end{bmatrix}, \tag{15}$$

$$\text{round}(Cx_k) - Cx_k = v_k,\ \hat{A} = \begin{bmatrix} A & 0 & 0 \\ \alpha B_f C & A_f & 0 \\ 0 & 0 & A_t \end{bmatrix},$$

$$\tilde{A} = \begin{bmatrix} 0 & 0 & 0 \\ B_f C & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ \hat{M} = \begin{bmatrix} M \\ 0 \\ 0 \end{bmatrix},$$

$$\hat{B} = \begin{bmatrix} B_1 & 0 & B_2 \\ B_f D_1 & \alpha B_f & 0 \\ 0 & 0 & B_t \end{bmatrix},\ \tilde{B} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & B_f & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\hat{C} = \begin{bmatrix} 0 & C_f & -C_t \end{bmatrix},\ \hat{D} = \begin{bmatrix} 0 & 0 & -D_t \end{bmatrix}.$$

By using the system dynamics (12)-(15), the cyber-security problem of the EV charging system is formulated as an H_∞ problem as follows:

Problem Formulation in H_∞ framework: Consider the cyber-physical EV charging system (12)-(15). Given a positive constant γ, find the parameters A_f, B_f, and C_f such that the overall system is asymptotically mean-square stable for $d_k = 0$, and the residual filter satisfies

$$\mathbb{E}\left\{e_k^T e_k\right\} - \gamma^2 \mathbb{E}\left\{d_k^T d_k\right\} < 0 \tag{16}$$

for all admissible $w_k,\ v_k$ and f_k.

The parameters of the residual filter (8)-(9) are designed by using the following lemma.

Lemma 1: (Theorem 2 in [18]) By defining $\alpha_1 = \mathbb{E}\left\{(\alpha_k - \alpha)^2\right\} = \alpha(1-\alpha)$, the cyber-physical EV charging system (12)-(15) is asymptotically mean-square stable for $d_k = 0$, and the residual filter satisfies (16) for a given $\gamma > 0$, if there exist $X = X^T \succ 0$, $Y = Y^T \succ 0$, $P_t = P_t^T \succ 0$, $\tau > 0$, $\tilde{A}_f$, $\tilde{B}_f$ and, $\tilde{C}_f$ such that the following LMI holds:

$$\Lambda = \begin{bmatrix} \Lambda_{11} & \Lambda_{12} \\ \Lambda_{12}^T & \Lambda_{22} \end{bmatrix} \prec 0 \tag{17}$$

with Λ_{11}, Λ_{12}, and Λ_{22} given in the box below.

$$\Lambda_{11} = \begin{bmatrix} -I & 0 & 0 & 0 & \begin{bmatrix} 0 & \tilde{C}_f \end{bmatrix} \\ * & -\begin{bmatrix} Y & X \\ X & X \end{bmatrix} & 0 & 0 & \begin{bmatrix} \alpha_1 \tilde{B}_f C & \alpha_1 \tilde{B}_f C \\ 0 & 0 \end{bmatrix} \\ * & * & -\begin{bmatrix} Y & X \\ X & X \end{bmatrix} & 0 & \begin{bmatrix} YA + \alpha \tilde{B}_f C & YA + \alpha \tilde{B}_f C + \tilde{A}_f \\ XA & XA \end{bmatrix} \\ * & * & * & -P_t & 0 \\ * & * & * & * & -\begin{bmatrix} Y - \tau H^T H & X - \tau H^T H \\ X - \tau H^T H & X - \tau H^T H \end{bmatrix} \end{bmatrix}$$

$$\Lambda_{12} = \begin{bmatrix} -C_t & 0 & \begin{bmatrix} 0 & 0 & -D_t \end{bmatrix} \\ 0 & 0 & \begin{bmatrix} 0 & \alpha_1 \tilde{B}_f & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ 0 & \begin{bmatrix} YM \\ XM \end{bmatrix} & \begin{bmatrix} YB_1 + \tilde{B}_f D_1 & \alpha \tilde{B}_f & YB_2 \\ XB_1 & 0 & XB_2 \end{bmatrix} \\ P_t A_t & 0 & \begin{bmatrix} 0 & 0 & P_t B_t \end{bmatrix} \\ 0 & 0 & 0 \end{bmatrix}$$

$$\Lambda_{22} = \begin{bmatrix} -P_t & 0 & 0 \\ * & -\tau I & 0 \\ * & * & -\gamma^2 I \end{bmatrix}$$

Under a feasible solution for (17), the FDF parameters (8)-(9) are obtained as follows:

$$A_f = (X - Y)^{-1}\tilde{A}_f,\quad B_f = (X - Y)^{-1}\tilde{B}_f,\quad C_f = \tilde{C}_f \tag{18}$$

Proof: See [18].

IV. Results

In this section the effectiveness of the proposed residual based attack-resilient EV system is evaluated by using a hardware-in-the-loop experimental setup. A general picture of the hardware-in-the-loop testbed is shown in Figure 2, developed by using the IEEE 802.15.4 TelosB wireless sensors technology [20]. The first-order discrete-time Randles equiv-

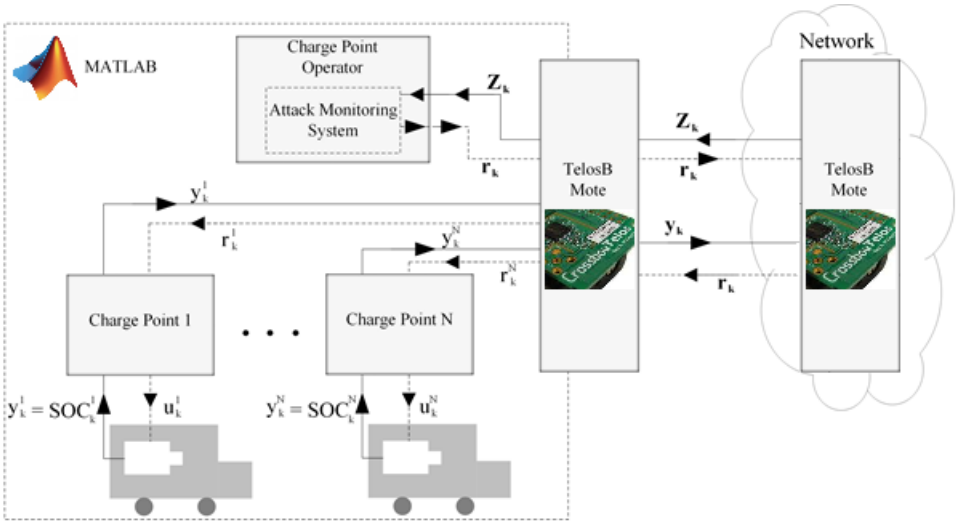

Fig. 2. Cybersecurity of EV charging systems using the residual generation.

alent circuit models of the EV batteries are implemented in MATLAB. At every time step, batteries' SOCs are measured by the charge points' meters, and transmitted to CPO through a wirelesses link. By using the received signals z_k, the residual filters, implemented in CPO, aim to detect the bias of SOC measurement under the DOS attack, which caused random packet dropouts. CPO then sends back the information of biases to charge points, to appropriately adjust the charging currents. In the proposed methodology, one residual filter per charge point is designed in a decentralized fashion. Without loss of generality, the results of the system with one charge point are given and discussed in the following.

In this testbed, the packet drop occurs if the strength of the received signal is low. The strength of the received signal is quantified by a received signal strength indicator (RSSI) in the IEEE 802.15.4 WSN standard [21], [22]. Power outage, shadowing and fading effects, and channel congestion cause low RSSI values. To generate packet dropouts, the AA battery of the TelosB is unplugged manually from the sensor node in this experiment. The actual injected bias is fed back to the residual filter, with no weighting function, i.e,

$$A_t = 0,\ B_t = 0,\ C_t = 0,\ D_t = 1$$

Let assume the packet drop's expectation value is $\alpha = 0.5$. By solving (17), the parameters of the residual filter are obtained as follows:

$$A_f = \begin{bmatrix} 0.5221 & -0.058 \times 10^{-3} \\ -2038.3 & 0.3434 \end{bmatrix},$$
$$B_f = \begin{bmatrix} 0.121 \times 10^{-3} \\ 0.4938 \end{bmatrix},$$
$$C_f = \begin{bmatrix} -3.9814 & 0.8895 \times 10^{-3} \end{bmatrix}.$$

Figure 3 shows the system performance under no packet drop for 25%, 50%, and 75% false-injection biases which occur at $t = 25s$. Figure 3(a) shows a representative snapshot of y_k, and z_k signals under no packet drop, when a 25% bias, $f_k = 0.25$, is injected at $t = 25s$. Figure 3(b) shows the performance of the proposed false-injection detection filter

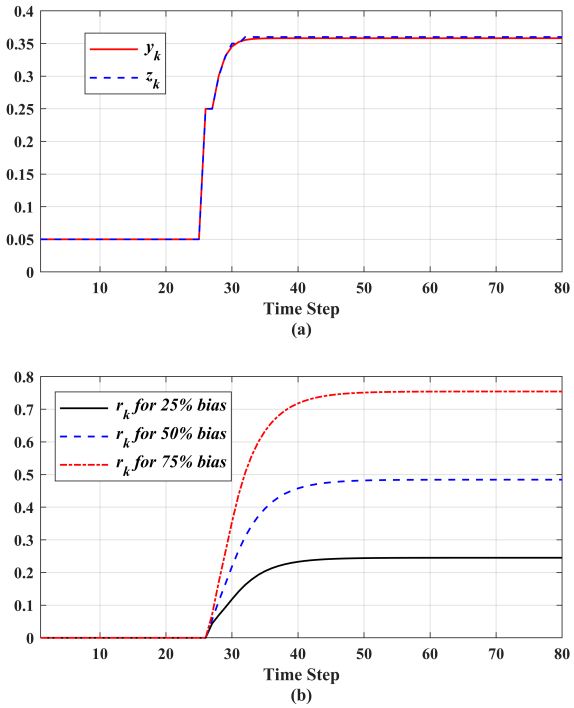

Fig. 3. A representative figure of y_k, and z_k signals under no packet drop, when a 25% bias, $f_k = 0.25$ is injected at $t = 25s$. (b) The performance of the proposed false-injection detection filter for 25%, 50%and 75% biases which occur at $t = 25s$ under no packet drop. This figure shows the generated residual signals r_k, which satisfactorily track $f_k = 0.25,\ 0.5,\ 0.75$.

for 25%,50%, and 75% biases which occur at $t = 25s$ under no packet drop. This figure shows that the generated residual signals r_k's satisfactorily track $f_k = 0.25, 0.5, and 0.75$.

Figure 4 shows the system performance under the DOS attack with 50% pack drop for 25%, 50%, and 75% false-injection biases which occur at $t = 25s$. Figure 4(a) shows a representative snapshot of y_k, and z_k signals under 50% packet

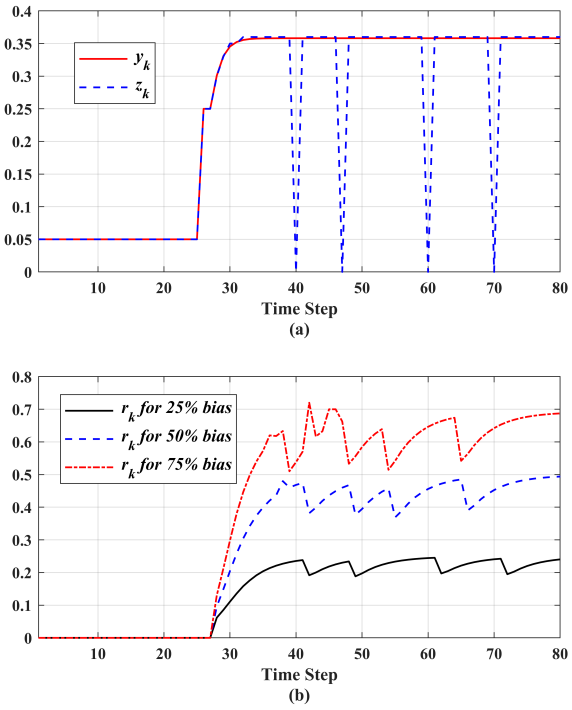

Fig. 4. A representative figure of y_k, and z_k signals under 50% packet drop, when a 25% bias, $f_k = 0.25$ is injected at $t = 25s$. (b) The performance of the proposed false-injection detection filter for 25%, 50%and 75% biases which occur at $t = 25s$ under 50% packet drop. This figure shows the generated residual signals r_k, which satisfactorily track $f_k = 0.25,\ 0.5,\ 0.75$.

drop, when a 25% bias, $f_k = 0.25$, is injected at $t = 25s$. Figure 4(b) shows the performance of the proposed false-injection detection filter for 25%,50%, and 75% biases which occur at $t = 25s$. This figure also shows the generated residual signals r_k's, which satisfactorily track $f_k = 0.25, 0.5, and 0.75$.

Both experiments demonstrate the detection of false-injection biases with and without DOS cyber attacks.

V. Conclusions and Future Works

In this paper, the cyber-physical protection of EV charging system has been addressed. A residual generation technique has been presented to provide an attack-resilient EV charging system which detects false data injection under the DOS cyber attack. The effectiveness of the proposed method was practically evaluated on a hardware-in-the-loop testbed developed by using the IEEE 802.15.4 wireless sensors technology. The results illustrate a satisfactory level of bias estimation under the DOS attack. As the future work, the charge control algorithm at the charge point is modified to compensate possible false data, based on the information received from CPO.

References

[1] M. Sedighizadeh, A. H. Mohammadpour, S. M. M. Alavi, "A daytime optimal stochastic energy management for EV commercial parking lots by using approximate dynamic programming and hybrid big bang big crunch algorithm," *Sustainable Cities and Society*, Vol. 45, pp. 486 – 498, 2019.

[2] https://www.statista.com/statistics/416750/number-of-electric-vehicle-charging-stations-outlets-united-states/

[3] https://www.greentechmedia.com/squared/electric-avenue/china-rapidly-expanding-ev-charging-market

[4] C. Hille, M. Allhoff, "EV CHARGING: MAPPING OUT THE CYBER SECURITY THREATS AND SOLUTIONS FOR GRIDS AND CHARGING INFRASTRUCTURE," *UtiliNet Europe Cyber Security Workshop*, Brussels, Belgium, May 2018.

[5] "*EV Charging Systems Security Requirements*," European Network for Cyber Security, Version 1.01, August 2017.

[6] M. Long, C. Wu, and J. Hung, "Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation," *IEEE Transaction on Industrial Information*, Vol. 1, No. 2, pp. 85 – 96, 2005.

[7] A. Teixeira, K.C. Sou, H. Sandberg, K.H. Johansson, "Secure Control Systems: A Quantitative Risk Management Approach," *IEEE Control Systems Magazine*, Vol. 35, No. 1, pp. 24 – 45, Feb. 2015.

[8] Y. Mo, S. Weerakkody, B. Sinopoli, "Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs," *IEEE Control Systems Magazine*, Vol. 35, No. 1, pp. 93 – 109, Feb. 2015.

[9] F. Pasqualetti, F. Dorfler, F. Bullo, "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," *IEEE Control Systems Magazine*, Vol. 35, No. 1, pp. 110 – 127, Feb. 2015.

[10] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G.J. Pappas, I. Lee, "Design and Implementation of Attack-Resilient Cyberphysical Systems: With a Focus on Attack-Resilient State Estimators," *IEEE Control Systems Magazine*, Vol. 37, No. 2, pp. 66 – 81, Apr. 2017.

[11] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017.

[12] Z.A. Biron, "*A Resilient Control Approach to Secure Cyber Physical Systems (CPS) with an Application on Connected Vehicles*," PhD Thesis, Clemson University, 2017.

[13] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 13:1 – 13:33, 2011.

[14] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715 -– 2729, 2013.

[15] D.A. Howey, S.M.M. Alavi, "Rechargeable Battery Energy Storage System Design," *Wiley Handbook of Clean Energy Systems*, Ed. J. Yan, Vol. 5, pp. 2801–2818, 2015.

[16] S.M.M. Alavi, A. Mahdi, S.J. Payne and D.A. Howey, "Identifiability of generalised Randles circuit models," *IEEE Transactions on Control Systems Technology*, 25 (6), 2112 – 2120, 2017.

[17] M.J. Rothenberger, D.J. Docimo, M. Ghanaatpishe, H.K. Fathy, "Genetic optimization and experimental validation of a test cycle that maximizes parameter identifiability for a Li-ion equivalent-circuit battery model," *Journal of Energy Storage*, Volume 4, pp. 156 – 166, December 2015.

[18] S.M.M. Alavi, M. Saif, "Fault Detection in Nonlinear Stable Systems Over Lossy Networks," *IEEE Transactions on Control Systems Technology*, Vol. 21, No. 6, pp. 2129 – 2142, 2013.

[19] S.M.M. Alavi, R. Izadi-Zamanabadi, M.J. Hayes, "Robust Fault Detection and Isolation Technique for SISO Closed-loop Control systems that Exhibit Actuator and Sensor Faults," *IET Control Theory & Applications*, Vol. 2, No. 11, pp. 951 – 965, 2008.

[20] www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf/

[21] S. M. M. Alavi, M. J. Walsh, M. J. Hayes, "Robust distributed active power control technique for IEEE 802.15.4 wireless sensor networks - A quantitative feedback theory approach," *Control Engineering Practice*, Vol. 17, No. 7, pp. 805 – 814, 2009.

[22] M. J. Walsh, S. M. M. Alavi, and M. J. Hayes, "Practical assessment of hardware limitations on power aware wireless sensor networks—an anti-windup approach," *Int. J. Robust and Nonlinear Control*, vol. 20, no. 2, pp. 194 – 208, 2010.