AIP | Journal of Applied Physics

An efficient wireless power transfer system with security considerations for electric vehicle applications

Zhen Zhang, K. T. Chau, Chunhua Liu, Chun Qiu, and Fei Lin

Citation: Journal of Applied Physics **115**, 17A328 (2014); doi: 10.1063/1.4866238
View online: http://dx.doi.org/10.1063/1.4866238
View Table of Contents: http://scitation.aip.org/content/aip/journal/jap/115/17?ver=pdfcov
Published by the AIP Publishing

Articles you may be interested in

Fast security risk assessment of the power system with wind power penetration
J. Renewable Sustainable Energy **6**, 053101 (2014); 10.1063/1.4893571

Experimental investigation of compact metamaterial for high efficiency mid-range wireless power transfer applications
J. Appl. Phys. **116**, 043914 (2014); 10.1063/1.4891715

Transfer efficiency analysis of magnetic resonance wireless power transfer with intermediate resonant coil
J. Appl. Phys. **115**, 17A336 (2014); 10.1063/1.4867125

Quantitative comparison of dynamic flux distribution of magnetic couplers for roadway electric vehicle wireless charging system
J. Appl. Phys. **115**, 17A334 (2014); 10.1063/1.4866882

Wireless power transfer in the presence of metallic plates: Experimental results
AIP Advances **3**, 062102 (2013); 10.1063/1.4809665

[This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to] IP: 147.8.31.43 On: Tue, 06 Jan 2015 07:30:13

An efficient wireless power transfer system with security considerations for electric vehicle applications

Zhen Zhang, K. T. Chau,[a] Chunhua Liu, Chun Qiu, and Fei Lin
Department of Electrical and Electronic Engineering, The University of Hong Kong, Pokfulam Road, Hong Kong, China

(Presented 6 November 2013; received 22 September 2013; accepted 15 November 2013; published online 21 February 2014)

This paper presents a secure inductive wireless power transfer (WPT) system for electric vehicle (EV) applications, such as charging the electric devices inside EVs and performing energy exchange between EVs. The key is to employ chaos theory to encrypt the wirelessly transferred energy which can then be decrypted by specific receptors in the multi-objective system. In this paper, the principle of encrypted WPT is first revealed. Then, computer simulation is conducted to validate the feasibility of the proposed system. Moreover, by comparing the WPT systems with and without encryption, the proposed energy encryption scheme does not involve noticeable power consumption. © *2014 AIP Publishing LLC*. [http://dx.doi.org/10.1063/1.4866238]

I. INTRODUCTION

In recent years, the emerging wireless power transfer (WPT) technology shows promising potentials for various fields. Especially for electric vehicles (EVs),[1] the WPT system can be utilized to provide wireless charging for electric devices located in inaccessible positions inside EVs. Additionally, it shows great potentials to perform emerging energy exchange among EVs as well as between EVs and the grid.[2] In the coordinated EV fleet, the WPT system should be able to prevent unauthorized EVs from obtaining the energy. Thus, the security consideration of the WPT system is an important issue for EV applications.

This paper proposes a secure inductive WPT system to transfer the energy to specific receptors in the multi-objective system. The chaotic energy encryption scheme is proposed to build up a secure energy transfer from the power source to the authorized receptors. The energy of the power source is first encrypted by using a specific chaotic map, which can then be decrypted by the authorized receptors based on the synchronized chaotic map. The proposed WPT system can effectively prevent unauthorized receptors from picking up the transferred energy, therefore providing the security consideration of the WPT system. In addition, the proposed scheme does not involve additional power consumption.

II. ENCRYPTED WPT

As shown in Fig. 1, the WPT system is innovatively applied to the energy management of EVs. On the one hand, the WPT system can be used to wirelessly charge specific electric devices inside EVs. On the other hand, the WPT system can enable sophisticated energy exchange between EVs. Hence, it is anticipated that the WPT for EVs will be extended from the parking lot to the urban road in foreseeable future.

For simplicity, a basic series-series topology as shown in Fig. 2 is adopted to demonstrate the methodology of the proposed secure inductive WPT system, where R_1 and R_2 denote the primary and secondary resistances, C_1 and C_2 denote the primary and secondary adjustable capacitances, L_1 and L_2 denote the primary and secondary inductances, L_m is the mutual inductance, C is the output capacitance to stabilize the rectified DC voltage, and R_L is the load resistance. Previous studies[3] indicated that the power transfer efficiency is significantly sensitive to the switching frequency f of the AC power source, namely, the efficiency may dramatically drop down to less 10% when f slightly deviates from the optimal switching frequency f_{opt}. Based on this unique characteristic, a chaotic sequence is utilized to purposely regulate f around f_{opt} in order to build up a secure WPT channel. Without knowledge of the chaotic sequence, unauthorized devices or vehicles cannot receive the wirelessly transferred energy from the power source.

The aforementioned chaotic encryption can be realized by using the Logistic map,[4] which exhibits the random-like behaviors within an adjustable bounded domain. In the proposed encryption scheme, the Logistic map is used to generate a one-dimensional discrete-time chaotic sequence, which is given by

$$\xi_{i+1} = A\xi_i(1-\xi_i), \quad A \in [0, 4], \tag{1}$$

where ξ_i denotes the sequence and A is the bifurcation parameter. Fig. 3(a) depicts its 3-D scatterplot where the phase portrait of ξ_i and ξ_{i+1} exhibits various topological structures with respective to different A. In addition, Fig. 3(b) depicts the largest Lyapunov exponent diagram to mathematically illustrate its nonlinear dynamical behaviors. It shows that the largest Lyapunov exponent becomes positive when $A > 3.57$, which quantitatively confirms that the infinitesimally close trajectories in the phase space exponentially diverge as time going, namely, the chaotic behavior occurs. For $\xi_i \in (0, 1)$, $A = 3.9$ is thus selected to encrypt the wirelessly transferred energy.

Consequently, the chaotically regulated frequency f_{reg} can be obtained by multiplying the chaotic regulator δ_i, which is expressed as

[a]Electronic mail: ktchau@eee.hku.hk.

 © 2014 AIP Publishing LLC

[This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to] IP: 147.8.31.43 On: Tue, 06 Jan 2015 07:30:13

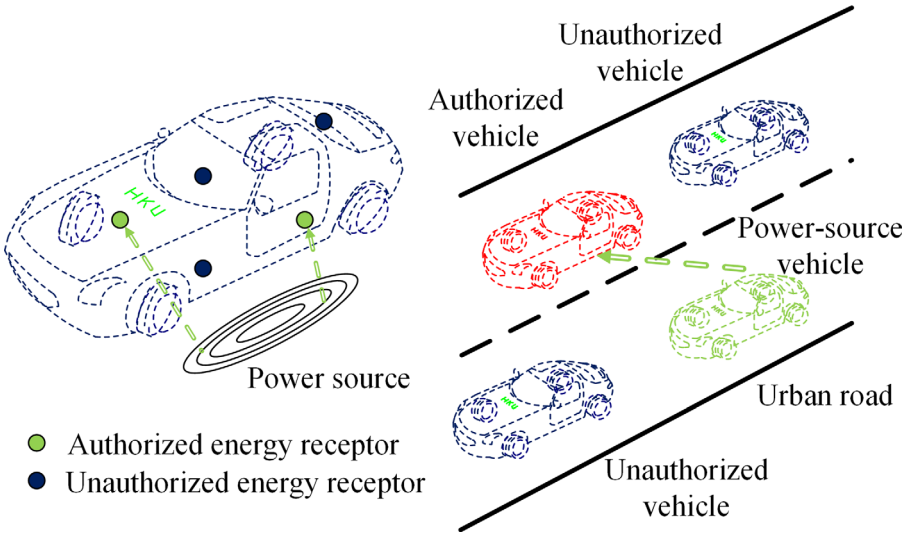

FIG. 1. Secure wireless power transfer system for EV applications.

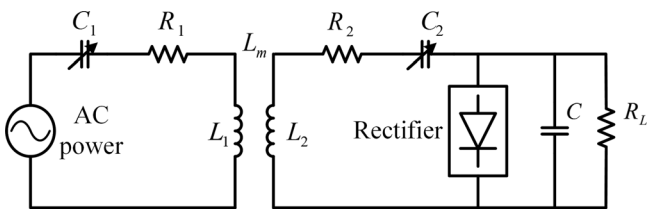

FIG. 2. Basic topology of secure WPT system.

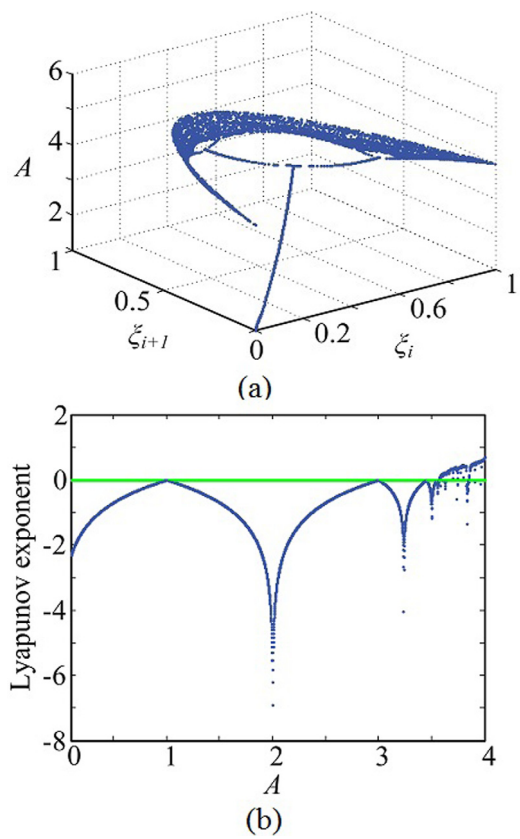

FIG. 3. Logistic map: (a) 3-D scatterplot; (b) largest Lyapunov exponent.

$$\delta_i = 0.95 + 0.1\xi_i. \tag{2}$$

In order to make the encrypted WPT system work in the optimal transfer efficiency, C_2 can be adjusted by

$$C_2 = \frac{1}{\delta_{2i}} \cdot \frac{1}{4\pi^2 f_{opt}{}^2 L_2}, \tag{3}$$

where δ_{2i} denotes the chaotic regulator for the authorized energy receptor. Based on the equivalent circuit, in addition, C_1 can be chosen as

$$C_1 = \frac{1}{\delta_{1i}} \cdot \frac{1}{4\pi^2 f_{opt}{}^2 L_1}, \tag{4}$$

where δ_{1i} denotes the chaotic regulator for the power source. By using the chaos synchronization technique,[5] δ_{1i} and δ_{2i} can be synchronized to have an identical chaotic sequence. Thus, C_1 and C_2 are simultaneously adjusted for the optimal WPT efficiency.

III. VERIFICATION

To evaluate the security and efficiency performances of the proposed inductive WPT system, computer simulations are carried out by using MATLAB/SIMULINK. The key parameters of the circuit topology are listed in Table I.

As shown in Fig. 4, the load voltage that can be obtained at the authorized receptor is about 7 V, whereas the unauthorized receptor's load voltage is only about 0.3 V. It illustrates that the proposed energy encryption scheme can effectively to prevent the unauthorized receptor from stealing the energy, therefore providing the desired security consideration of the WPT system. Fig. 5 compares the power

TABLE I. Circuit parameters of inductive WPT system.

Symbol	Value	Symbol	Value	Symbol	Value
C	350 μF	R_L	5.83 Ω	L_m	0.00447 mH
C_1	18 nF	R_1	0.05 Ω	L_1	0.1375 mH
C_2	147 nF	R_2	0.05 Ω	L_2	0.01293 mH

[This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to] IP: 147.8.31.43 On: Tue, 06 Jan 2015 07:30:13

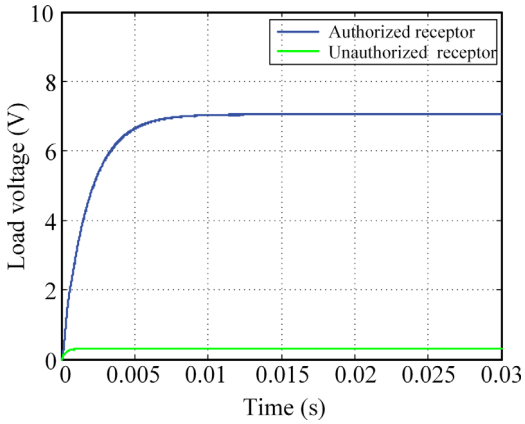

FIG. 4. Comparison of load voltages.

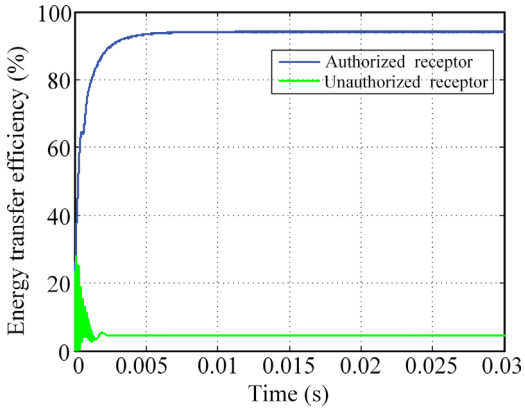

FIG. 5. Comparison of power transfer efficiencies.

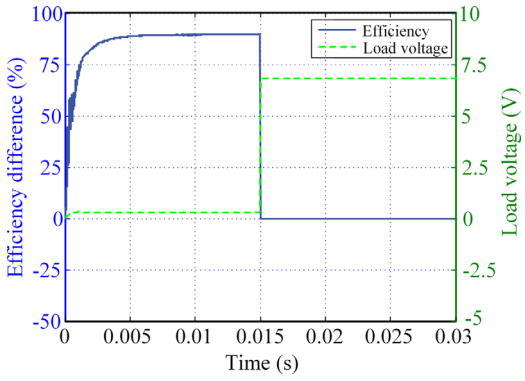

FIG. 6. Comparison between proposed and traditional WPT systems.

transfer efficiencies between the authorized and unauthorized receptors. It shows that the authorized receptor can receive the wirelessly transferred energy from the power source with the efficiency of about 94%, whereas the unauthorized receptor has the efficiency of less than 5%, which explicitly demonstrates the security performance of the proposed WPT system.

Furthermore, the power transfer efficiencies between the proposed and traditional inductive WPT systems are simulated at which the synchronized decoding function is activated after $t > 0.015$ s. As depicted in Fig. 6, the efficiency difference is remarkable before the decryption, whereas the difference becomes zero after the decryption. Meanwhile, the load voltage changes from 0.3 V to 7 V once the decryption is activated. It indicates that the proposed energy encryption scheme does not involve additional power consumption or load voltage drop.

Since the above theoretical analysis and computer simulation are based on an idealized condition of the circuit topology and operation, there is an inevitable discrepancy between the calculation and experimental results. First, the actual circuit inductances may slightly vary with the switching frequency, especially at high-frequency operation, which will affect the state of resonance and hence degrade the power transfer efficiency. Second, an accurate online tuning of the circuit capacitances is challenging, which will also dynamically affects the state of resonance. Third, the unnecessary reactive power drawn by unauthorized receptors essentially decreases the input power factor, which will cause additional power loss. Nevertheless, all these factors will only influence the power transfer efficiency and have no impact on the mechanism of the proposed energy encryption scheme.

IV. CONCLUSION

This paper proposes an energy encryption scheme to establish a secure inductive WPT system for EV applications such as charging the electric devices inside EVs or performing energy exchange between EVs. The Logistic map is utilized to chaotically regulate the switching frequency of the power source, which can prevent unauthorized devices or vehicles from stealing the transmitted energy. Meanwhile, the synchronized chaotic sequence is used to decode the encrypted energy by simultaneously adjusting the capacitors of the power source and the authorized receptors, hence achieving the optimal power transfer efficiency. Computer simulation results confirm the feasibility of the proposed secure inductive WPT system.

ACKNOWLEDGMENTS

This work was supported by a grant (Project No. HKU SPF 201109176034) from the Committee on Research and Conference Grants, The University of Hong Kong, Hong Kong.

[1]C. C. Chan and K. T. Chau, *Modern Electric Vehicle Technology* (Oxford University Press, 2001).
[2]C. Liu, K. T. Chau, D. Wu, and S. Gao, IEEE Proc. **101**, 2409 (2013).
[3]J. T. Boys, G. A. Covic, and A. W. Green, Proc. IEE Electr. Power Appl. **147**, 37 (2000).
[4]K. T. Chau and Z. Wang, *Chaos in Electric Drive Systems: Analysis, Control and Application* (Wiley-IEEE Press, 2011).
[5]L. Jin, X. Wang, and L. Li, J. Appl. Phys. **113**, 093506 (2013).

[This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to] IP: 147.8.31.43 On: Tue, 06 Jan 2015 07:30:13