Comparison Performance Based on Distance of Energy Encryption in Medium Field for Wireless Power Transfer System

Nur Hazwani Hussin, Muhammad Mokhzaini Azizan, Azuwa Ali, Mahmoud A. M. Albreem

Abstract: ***Energy encryption is one of medium for the security of wireless power transfer (WPT). Generally, the encryption technique is most im-portant thing are used to protect energy transmission channels from an unauthorized receiver. Besides, the encryption technique in medium field of WPT system also can be used to transmit the data securely. In the research on the effects of security key for secure of energy trans-fer to authorized receiver is important of the encryption techniques of WPT. Furthermore, chaos theory are proposed to the energy encryp-tion scheme of WPT system. In chaos theory, to chaotically regulate the switching frequency the logistic map are applied to proposed securi-ty key. In addition, the power and distance performance are effect on the characteristics of chaos theory. Accordingly, this paper explore mainly adequate distance based on mobile charging application. Energy encryption in medium field for WPT system are focusing on dis-tance performance of this research. Meanwhile, this research is deal on the comparison of performance in distance based on mobile charging application.***

Index Terms: Chaos Theory, Energy Encryption, Mobile Charging Application, Security, Wireless Power Transfer,

I. INTRODUCTION

In transferring electrical power from source transmitter to load receiver with interconnected wire is one of the technique in WPT system. WPT innovation holding great potential to switch the way individuals lead their lives by contributing new levels of accommodation, mobility and security. Essentially, there are three sorts of WPT which is near field, medium field and far field. WPT can be classified into inductive coupling, capacitive coupling, magnetic resonant coupling and electromagnetic radiation [1], [2], [3]. The benefit of near field and medium field is protected and not being consumed by the beneficiary. In near field, the main strategy for separation are chosen for short range application and no radiation on the procedure to exchange control. At that point, the distance for medium field are chosen in mid-range application furthermore no radiation. In this way, for far field are being in long scope of distance and it has radiation amid process exchange control.

Revised Manuscript Received on December 30,2018.

Nur Hazwani Hussin, School of Electrical System Engineering, Universiti Malaysia Perlis 02600 Arau, Perlis, Malaysia.

Muhammad Mokhzaini Azizan, School of Electrical System Engineering, Universiti Malaysia Perlis 02600 Arau, Perlis, Malaysia.

Azuwa Ali, School of Electrical System Engineering, Universiti Malaysia Perlis 02600 Arau, Perlis, Malaysia.

Mahmoud A. M. Albreem, Department of Electronics and Communication Engineering, College of Engineering, A'Sharqiyah Universsity (ASU)

400 Ibra, Oman.

Along these lines, it is not good for the health on the environment and surrounding people. WPT optimization criteria are needed for two uses, namely, continuous uninterruptable power delivery and periodic charging. For continuous charging, whether under the stationary (EVs) or moving states (mobile charging), wireless communication should be fast, reliable, and energy efficient [4]. The WPT system is increasingly attracting attention in various fields, such as charging portable electronic devices and implanting medical devices [5]. WPT also suitable for electric vehicles (EVs) application, such as battery charging for normal vehicular operation and energy exchange [6], [7], [8].

The wireless communication channels in encryption is more fundamental and vital in the present than previously. The data must be all around encrypted during transmission so the data safely exchange over the wireless medium. Energy is required to exchange to particular receiver and turn off other unapproved energy transmission channels. Hence, the security of energy transmission is truly a one of critical issue in WPT system [9]. Few sorts of procedures are utilized as a part of encrypting the energy encryption, for example, password system, radio frequency signal and the new one is chaos theory. The most up to date innovation and as of now being investigate is chaos theory technique. Keeping in mind the end goal to encode energy encryption of WPT, the chaos theory flighty conduct controlled to produce interesting security key by decreasing the unpredictability of condition. The nearness of disarray is affirmed by computation of the Lyapunov examples [10]. In this manner, this paper will concentrate more on chaos theory technique for scrambling the encrypting energy concentrate on medium field WPT system.

1. Design on Energy Encryption Scheme of WPT Systems

According to design the energy encryption scheme of WPT system, Figure 1 shows the block diagram for the system configuration. The system are divided to several part which is transmitter and receiver part. By the specific value of power source the system is power up. In conventional WPT system, the operation is as depicted previously. Basically, in magnetic resonant categorizes has two coil system are added with resonant coil for medium field application. In long distance range, the resonant coil used to transfer power on the WPT system. Thus, in order of chaos theory technique is implemented to add security key in WPT system.

Generally, mathematically algorithm which will be embedded in the WPT system by using chaos theory technique.

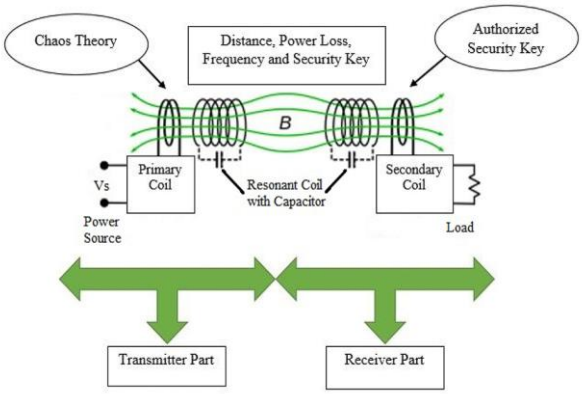

Figure 1. Block Diagram for Energy Encryption of Medium Field WPT Systems

Based on Fig. 1, the main part is transmitter part and receiver part. In transmitter part, it is embedded from power source to primary coil. The discrete time chaotic values are generate by using logistic map algorithm in chaos theory technique. Otherwise, in logistic map it has the Lyapunov exponent to generate security key which is 0 and 1 for secure the system. For initialize logistic map by using equation (1) below:

$$\xi i + 1 = A\xi i(1 - \xi i), A \in [0,4] \quad (1)$$

Where ξi indicates the sequence and A means the bifurcation parameter. The phase portraits of ξi and $\xi i + 1$ display different topological structures alongside with the expansion in A. In addition, ξi goes about as a consistent value for $A \in [0,1)$, a period 1 oscillation for $A \in [1,3)$, a period n oscillation for $A \in [3,3.57)$, and a chaotic oscillation for $A \in [3.57,4]$. Likewise, inward the logistic map it has the largest Lyapunov exponent as a mathematical expression of the chaotic behavior. Hence, the biggest Lyapunov exponent gets to be distinctly positive when $A > 3.57$ it is a result of in chaotic oscillation period and at same time the chaotic behavior happens if $A = 3.9$ [11]. In this way, $A = 3.9$ is chosen to create the irregular limited security key $\xi i \in (0,1)$ for the energy encryption scheme.

Notwithstanding, the resonant circuit are included at both side which is resonant for primary and secondary. The resonant circuit are interconnected with primary and secondary coil for transfer power in long transmission distance with no affecting on the radiation. In spite of the fact that, for changing the frequency resonant in magnetic resonant coupling is troublesome.

Besides, the working frequency can controlled the transfer power exhibitions. The distance exhibitions are incorporate the viable power, switching frequency and security key. Firstly, the distance to transfer power is rely on upon the application can be utilized. In this project, mobile charging application is chosen. Subsequently, all the detail of specification is as indicated by mobile charging application. Along these lines, the power chose is 10W with ideal optimal switching frequency of 100 kHz. At that point, for distance level it vary from 3cm to 5cm whereby to perceive which estimation of distance have higher execution. The parameter depends on Qi-standard [12], [13], [14]. Table I demonstrates that general parameters utilized for energy encryption in medium field WPT system.

Table 1. Parameters for Energy Encryption in Medium Field of WPT Systems

Parameters	Values
Optimal Switching Frequency	100kHz
Power	10W
Transmission Distance Level	3cm, 4cm, 5cm

All things considered, for the switching frequency can be directed by utilizing algorithm for using the greatest power transfer is made. So that, the transmitter coil, resonant coil and receiver coil resonant at a similar frequency. The tolerant different frequency around ± 5%. On the off chance that the frequency resonant at different frequency, the system neglect to work. Fundamentally, this process will work synchronize with security key.

$$\omega = \delta_i \omega_o \quad (2)$$

Where:

ω = Switching frequency

ω_o = Resonant switching frequency

$$\delta i = a + (b - a)\xi i, 0 < a < b \quad (3)$$

Where:

δ_i = Chaotic security key

a = Transmission distance

b = Power level

Moreover, the security key likewise has a calculation in equation (3) and related each other with switching frequency in equation (2). In equation (3), the value a and b are the parameter to be utilized for power transmission and distance to transfer power of WPT system. These parameter will be controlled to recognize and at same time to locate the best performance with the mix parameter. For the security key likewise it must have matching security key from transmitter to receiver. It is to avoid from the stolen in power transfer process. The matching process of switching frequency and security key is the point at which it hold up a request from the receiver. As that process, if switching frequency and security key is matching synchronize at both part, it is demonstrate that the power transfer to authorized receiver. As it were, the power is productively transfer to right receiver when the ideal switching frequency happens. Aside from same resonance frequency, security key at both transmitter and receiver should have a same value all together for best performance. The value of security is either 0 or 1 are purpose in energy encryption for WPT system.

II. RESULT AND DISCUSSION

This segment examines the outcomes from the simulation. The simulation are done by utilizing MATLAB programming to evaluate the security and performance of the proposed magnetic resonant coupling in medium field for WPT system.Table 2 demonstrates the consequences of energy encryption in medium field WPT system on the mobile charging application system.

This paper change the taking distance based of mobile charging application as reference for least and most value of distance. Along these lines, it will reason that, the best distance range that can be transmitted are utilized and recognize at which control level has best performance. Thusly, through simulation it proposed a comparison of the outcome.

The best performance in the system can be realize with the minimum and maximum distance for simulation are taken from 3cm, 4cm and 5cm. Table 2 illustrates the data of energy encryption of medium field WPT system in different distance.

In 3cm distance, it can be demonstrate that, from section selector 0 until 7, the value of the value of security key at transmitter increase, while the logistic map value fluctuate. Moreover, the switching frequency data start gain when the section selector from 0 until 7. From the general information at Table 2, the best performance synchronize switching frequency and security key is section selector 0. The best switching frequency is at 100 kHz and the security key value at transmitter and receiver is 1.00 (transmitter) and 0.86 (receiver).

In 4cm distance, it can been seen that, from section selector 0 until 7, the security key value at transmitter increase, while the logistic map still inconsistently. In addition, the switching frequency data raise from the section selector 0 until 7. From the general statistics at Table 2, the best execution synchronize switching frequency and security key is section selector 0. The best switching frequency is 102 kHz and security key at transmitter to receiver is 1.02 (transmitter) and 0.86 (receiver).

In 5cm distance, from the section selector 0 until 7, the security key at transmitter is vary and same goes to the logistic map value. Also, the switching frequency information raise from the section selector 0 until 7. From the general data at Table II, the outcome for distance 5cm does not to achieving great performance. It is a result of the switching frequency and security key not matching with transmitter and receiver. Thus, when no matching for switching frequency and security key, the system cannot be exchange the powerigure 2 demonstrate the comparison result for switching frequency. It can be realize that, the matching switching frequency with optimal switching frequency is accurate at distance 4cm when frequency at 102 kHz of 100 kHz compared to 3cm and 5cm. Thus, the matching process success when the switching frequency and security key occur simultaneously. In addition, at the receiver part the security key value is 0.86 and maintain constant for 3cm, 4cm and 5cm. Then, at the transmitter part the security key value almost closed to the receiver which at 1.02 for 5cm compared to 3cm and 5cm. For overall data about comparison of security key for transmitter and receiver part can be illustrate on Figure 3.

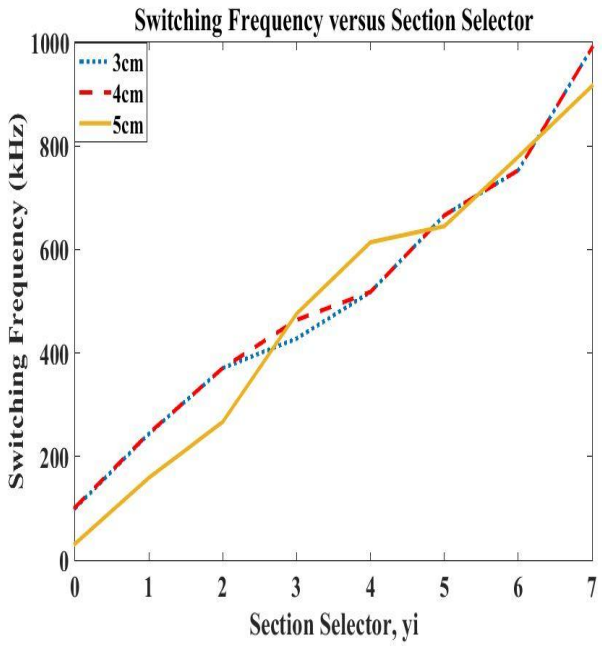

Figure 2. Comparison Result for Switching Frequency

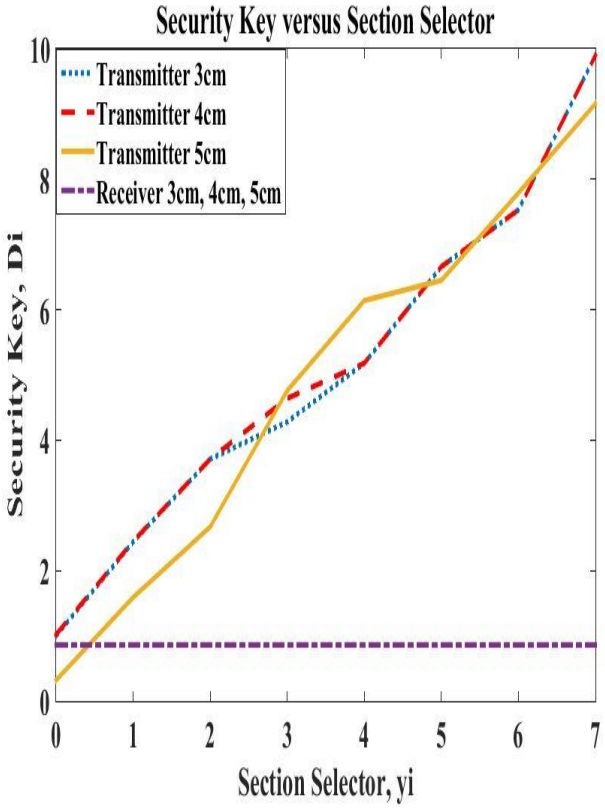

Figure 3. Comparison Result for Security Key

Based on the simulation finding above, the best performance in distance of the mobile charging application system is 4cm. It is because of overall specification in distance 4cm are fulfill. The specification that have been investigated and proved earlier are made based on the three characteristic of chaos theory which are switching frequency, security key and logistic map.

Table 2. Energy Encryption of Medium Field WPT System Result for Power Performance

Section Selector, yi	Power (W)	Distance (cm)	Optimal Switching Frequency, fo (kHz)	Switching Frequency, f (kHz)	Security Key, Di Transmitter	Security Key, Di Receiver	Logistic Map, Xn1
0	10	3	100	100	1.00	0.86	0.3539
		4		102	1.02		0.3539
		5		31.63	0.32		0.1042
1	10	3	100	244	2.44	0.86	0.7333
		4		245	2.45		0.7333
		5		159	1.59		0.5228
2	10	3	100	371	3.71	0.86	0.9311
		4		371	3.71		0.9311
		5		276	2.67		0.7755
3	10	3	100	428	4.28	0.86	0.9782
		4		464	4.64		0.9942
		5		476	4.76		0.9973
4	10	3	100	518	5.18	0.86	0.9990
		4		518	5.18		0.9990
		5		614	6.14		0.9497
5	10	3	100	666	6.66	0.86	0.8910
		4		666	6.66		0.8910
		5		645	6.45		0.9176
6	10	3	100	753	7.53	0.86	0.7454
		4		753	7.53		0.7454
		5		779	7.79		0.6919
7	10	3	100	990	9.90	0.86	0.0388
		4		990	9.90		0.0388
		5		916	9.16		0.3090

III. CONCLUSION

In this paper, to improve the security performance of the WPT the encrypted mobile charging system has been proposed. The switching frequency is the key to chaotically regulate of the power supply. Meanwhile, authorized mobile charging system can definitely receive the transfer power with the accomplish security key. Thus, for unauthorized mobile charging system the power transmission channel can be turned off. The simulation results have well agreed with the theoretically analysis and proved the validity of the proposed application of mobile charging system.

IV. ACKNOWLEDGEMENT

This study was supported by Universiti Malaysia Perlis (UniMAP) and the Ministry of Higher Education (MoH) under a Grant Number UniMAP/ RMIC/ FRGS/ 9003-00-00562.

REFERENCES

2. K. Huang and V. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," IEEE Transactions on Wireless Communications, vol. 13, no. 2, pp. 902–912, February 2014.
3. L. Xie, Y. Shi, Y. Hou, and A. Lou, "Wireless power transfer and applications to sensor networks," IEEE Wireless Communications, vol. 20, no. 4, pp. 140–145, August 2013
4. X. Mou and H. Sun, "Wireless power transfer: Survey and roadmap," IEEE Vehicular Technolology Conference, vol. 2015, pp. 1–13, 2015.
5. J. Hirai, K. Tae-Woong, and A. Kawamura, "Wireless transmission of power and information and information for cableless linear motor drive," IEEE Transactions on Power Electronic, vol. 15, pp. 21–27, 2000.
6. O. H. Stielau and G. a Covic, "Design of loosely coupled inductive power transfer systems," International Conference on Power System Technology Proceedings, vol. 1, pp. 85–90, 2000.
7. W. Chwei-Sen, O. H. Stielau, and G. A. Covic, "Design considerations for a contactless electric vehicle battery charger," IEEE Transaction on Industrial Electronics, vol. 52, pp. 1308–1314, 2005.
8. A. Woojin, J. Sungkwan, L. Wonkyum, K. Sangsik, P. Junseok, S. Jaegue, K. Hongseok, and K. Kyoungchoul, "Design of coupled resonators for wireless power transfer to mobile devices using magnetic field shaping," IEEE International Symposium on Electromagnatic Compatibility, pp. 772–776, 2012.
9. Agbinya, Johnson I., "Wireless power transfer," River Publishers, vol. 45, 2015.
10. R. A. Bercich, D. R. Duffy, and P. P. Irazoqui, "Far-field RF powering of implantable devices: Safety considerations," IEEE Transactions on Biomedical Engineering, vol. 60, pp. 2107–2112, 2013.
11. T. P. Duong and J.-W. Lee, "Experimental Results of High-Efficiency Resonant Coupling Wireless Power Transfer Using a Variable Coupling Method," IEEE Microwave and Wireless Components Letters, vol. 21, pp. 442–444, 2011.
12. K. T. Chau and Z. Wang, "Chaos in Electric Drive System," John Wiley Publishers, 2001.
13. S. J. Gerssen-Gondelach and A. P. C. Faaij, "Performance of batteries for electric vehicles on short and longer term," Journal Power Sources, vol. 212, pp. 111–129, 2012.
14. C. Sanghoon, K. Yong-Hae, S.-Y. Kang, L. Myung-Lae, L. Jong-Moo, and T. Zyung, "Circuit-model-based analysis of a wireless energy transfer system via coupled magnetic resonances," IEEE Transactions Industrial Electronics, vol. 58, pp. 2906–2914, 2011.
15. M. Galizzi, M. Caldara, V. Re, and A. Vitali, "A novel Qi-standard compliant full-bridge wireless power charger for low power devices," pp. 44–47, 2013.