International Journal on Advanced Science Engineering Information Technology

Vol.7 (2017) No. 5
ISSN: 2088-5334

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

N.H Hussin [#], M.M Azizan[#], A Ali, M.A.M Albreem[*]

[#] *School of Electrical System Engineering, University Malaysia Perlis, 02600 Arau, Perlis, Malaysia*
E-mail: nurhazwanihussin@yahoo.com; mokhzainiazizan@unimap.edu.my; azuwa@unimap.edu.my;

**Department of Electronics and Communication Engineering, College of Engineering, A'Sharqiyah Universsity (ASU), 400 Ibra, Oman*
E-mail: ma_braim@hotmail.com

***Abstract*— Encryption is a very important technique used to protect energy transmission channels from an unauthorized receiver. It can be utilized to transmit data securely over the wireless medium. Encryption techniques of wireless power transfer (WPT) are important in the research on the effects of security key for security of energy transfer to the authorized receiver. The energy encryption scheme of WPT is proposed to chaos theory. Chaos theory is applicable to the logistic map to propose as a security key to chaotically regulate the switching frequency. Furthermore, for chaos theory characteristic effect power and distance performance. Therefore, this paper investigates mainly effective power based on mobile charging application. This research is focusing on performance on power of energy encryption in medium field for wireless power transfer system. This research is dedicated to the comparison of performance in power based on mobile charging application. The optimization to transport the power in this research based on comparison of power is 10W. The research utilized MATLAB simulation to compare the performance.**

***Keywords*— chaos theory; energy encryption; mobile charging application; security; wireless power transfer.**

I. INTRODUCTION

WPT is one of the techniques for transferring electrical power from source transmitter to load a receiver without interconnected wire. WPT technology is holding good potential to switch the way people lead their lives by contributing new levels of convenience, mobility and safety. Basically, there are three types of WPT which are near-field, medium field and far field. WPT can be classified into inductive coupling, capacitive coupling, magnetic resonance and electromagnetic radiation [1]. The advantage of the near field and medium field is safe and not being absorbed by the receiver. In near-field, the principal method of distance are selected for short range application and no radiation on the process to transfer power. Then, distance for medium field is selected in mid-range application and also no radiation. Thus, for far field are being in extensive range of distance and it has radiation during process transfer power. So, it is not good for the health of the environment and surrounding people. WPT optimization criteria are needed for two uses, namely, continuous uninterrupted 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 efficiency [2]. The WPT system is increasingly attracting attention in various fields, such as charging portable electronic devices and implanting medical devices [3]. WPT also suitable for electric vehicles (EVs) application, such as battery charging for normal vehicular operation and energy exchange [4-6]. Recent evolutions had shown a renewed interest in commercial development of WPT using magnetically-coupled resonant circuits (MCRC) for energy encryption such as security in short and medium range WPT. Distance between source and load is typically in between 1-2 meters.

Encryption in wireless communication channels is more vital and necessary in the present than in the past. Data need to be well encrypted during transmission so the data securely transfer over the wireless medium. Energy is expected to transfer to a specific receiver and switch off other unauthorized energy transmission channels. Thus, the security of energy transmission is really a one of important issues in WPT system [7]. Few types of techniques are used in encrypting the energy such as a password system, radio frequency signal and the new one is chaos theory. The newest technology and currently being explored is chaos theory technique. In order to encrypt energy of WPT, chaos theory unpredictable behaviour manipulated to generate unique security key by reducing the complexity of equation. The presence of chaos is supported by calculation of the

Lyapunov exponents [8]. Therefore, this paper will focus more on chaos theory technique for encrypting the energy mainly concentrate on medium field WPT system. Nonetheless, the magnetic resonant coupling for medium field WPT system by using chaos theory technique explored in this thesis. Next, a resonator block for single resonator WPT systems with single transmitter and receiver is to be recommended. Thus, the method for analysis of such systems is designed. The medium field has several factors to be considered which are frequency, distance and application. Finally, the validation of the models have been carried on systems by using simulation.

In 1901, Nikola Tesla started constructing his famous Wardenclyffe Tower near Long Island [9]. The tower was used to broadcast sound by employing wireless communication and transmitting power without utilizing conducting wires [9]. Tesla's work was impressive when it's given the lack of radio wave technologies at that time, the experiment was unsuccessful even though it attempted to demonstrate its feasibility. In the late 20th century, the near-field inductive power transfer would become a concern when cordless charging of consumer devices gained popularity [10]. The aim is to seek ways for effectively transmitting power from a source to a device using the principle of electromagnetic induction, such as the operation of a transformer on the inductive power transfer. The system is non-radiative as it does not rely on propagation of electromagnetic waves [11].

In the inductive power transfer applications of a few kilowatts (kW), such as charging of Electric Vehicles (EVs) and mobile phone, 90% of transmission efficiency can be achieved by increasing the operating frequency and more than 70% of efficiency can be reached for low power, such as the maximum 5W mobile phone charging [12]. Moreover, the operating frequency range of the inductive coupled technique is generally from 20 kHz to several MHz [12]. However, when efficiency is achieved, coil distances further enlarge or have more freedom in positioning the source and load relative to each other. Then, to solve the problem, the Massachusetts Institute of Technology (MIT) research group examined many techniques for transmitting power over medium-range distances and developed a non-radiative resonance coupled scheme to enhance transmission efficiency [11-12]. Compared with electromagnetic radiation, resonant coupling has advantages, such as higher efficiency in omnidirectional transmission and insensitivity to the surrounding environment [13]. The operating frequency range from 10 kHz to approximately 200 MHz has been used in several studies on resonant coupled WPT [13]. However, electromagnetic radiation can be classified into unidirectional and omnidirectional radiation based on energy transmitting direction [14]. The far-field approaches balance between directionality and transmission efficiency [15]. Radio frequency (RF) and microwave systems are examples that can benefit from the transfer power over a distance of several kilometers at 90% efficiency by using high-gain antennas [15].

In summary, the WPT system can be divided into three concepts according to technology, transmission, and applications. These three concepts are near-field WPT through electrical and magnetic induction, medium-field WPT through coupled resonant circuits, and far-field WPT through microwave on RF rectifier circuits.

II. MATERIAL AND MEHOD

In order to model the energy encryption scheme of WPT systems, Figure 1 shows in the block diagram for the overall systems operation which divided to several part. The system is power up by specific value of the power source. The power transmitted to the receiver wireless to power up the load. In traditional WPT system, the operation is broken down as described above. For medium field application, in magnetic resonant categorizes is basically having two coil system is added with resonant coil. The resonant coil employed to transfer power for long distance range. Therefore, in order to add security in WPT system, chaos theory technique is applied. Generally, chaos theory is a mathematically algorithm which will be integrated into the WPT system.

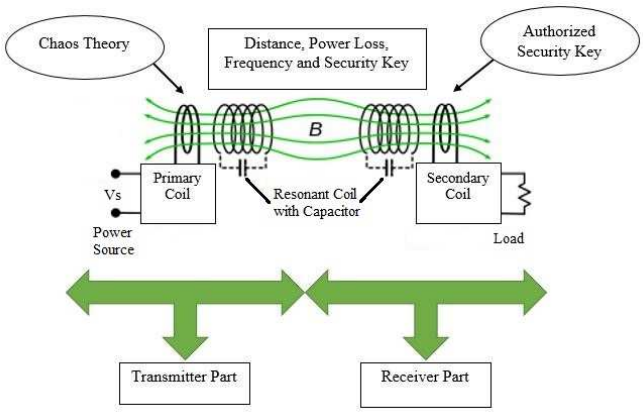

Fig.1 Block Diagram for Energy Encryption of Medium Field WPT Systems

Figure 2 shows the circuit design for magnetic resonant coupling of WPT. This circuit shows how the magnetic resonant coupling of WPT works to transfer power from the transmitter to the receiver. The circuit is divided in three parts, namely, power supply, transmission channel, and load. In the power supply, DC power goes through the DC/AC inverter. The DC/AC inverter transforms DC power to AC power supply. Then, the input voltage will supply the primary unit, which is composed of the resistance, capacitor, and inductance. All these variables together are known as impedance.

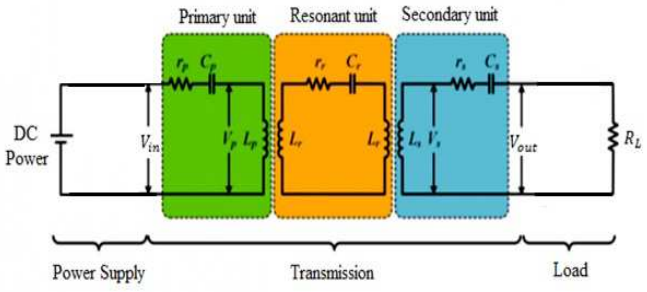

Fig.2 Magnetic Resonant Coupling Circuit of Wireless Power Transfer System

TABLE I
PARAMETERS FOR MRC CIRCUIT OF WIRELESS POWER TRANSFER SYSTEM

Parameters	Values
Inductance of Primary Coil (L_p)	0.09589mH
Resistance of Primary Coil (r_p)	0.2215Ω
Number of Turns for Primary Coil (N_p)	20
Inductance for Resonant Coil (L_r)	0.09477mH
Resistance for Resonant Coil (r_r)	0.07032Ω
Number of Turns for Resonant Coil (N_r)	20
Inductance for Secondary Coil (L_s)	0.009372mH
Resistance for Secondary Coil (r_s)	0.03565Ω
Number of Turns for Secondary Coil (N_s)	10

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

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

where ξi denotes the sequence and A denotes the bifurcation parameter. Phase portraits, of ξi and $\xi i + 1$ exhibit various topological structures along with the increase in A. Moreover, ξi acts as a constant 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 $A \in [3.57,4]$. In addition, inward the logistic map it has the largest Lyapunov exponent as a mathematical expression of the chaotic behavior. Thus, the largest Lyapunov exponent becomes positive when $A > 3.57$ it is because of in chaotic oscillation period and at same time the chaotic behavior occurs if $A = 3.9$ [16]. Therefore, $A = 3.9$ is selected to generate the random bounded security key $\xi i \in (0,1)$ for the energy encryption scheme.

However, the resonant circuit is added at both sides which are resonant for primary and secondary. The resonant circuit is interconnected with the primary and secondary coil for transferring power in long transmission distance with no effecting on the radiation. Although, for adjusting the resonant frequency in magnetic resonant coupling is difficult. Figure 2 to verify that, the resonant magnetic coupling circuit of WPT system works to transfer power from the transmitter to receiver. Table I show the parameters used for Magnetic Resonant Coupling (MRC) circuit of Wireless Power Transfer System. Overall parameters for MRC of Wireless Power Transfer System are fixed to use in this project.

Furthermore, the working frequency can control the transfer power performances. The powerful performances are included in the effective distance, switching frequency and security key. Firstly, distance to transfer power is depending on the application can be used. In this project, mobile charging application is enabled. Therefore, all the specification below is according to mobile charging application. So, distance selected is 4cm with optimal switching frequency of 100 kHz. Then, for power level it varies from 5W to 20W whereby to recognize which value of power have higher performance. The parameter is built on Qi-standard [17]. Table II shows that overall parameters utilized for energy encryption for medium field WPT systems.

TABLE II
PARAMETERS OF ENERGY ENCRYPTION FOR MEDIUM FIELD WPT SYSTEM

Parameters	Values
Optimal Switching Frequency	100kHz
Power Level	5W, 10W, 20W
Transmission Distance	4cm

Nevertheless, for the switching frequency can be regulated by using the algorithm for utilizing the maximum power transfer is made. So that, the transmitter coil, resonant coil and receiver coil resonant at the same frequency. The tolerant different frequency around 5%. If the frequency resonant at different frequency, the system fails to operate. Basically, this process will work simultaneously with security key.

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

where:

ω = Switching frequency
ω_o = Resonant switching frequency

where δ_i is the chaotic security and can be expressed as

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

where:

a = Transmission distance
b = Power level

In addition, the security key also has an algorithm 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 used for power transmission and distance to transfer power of WPT system. These parameters will be manipulated to observe and at the same time to find the best performance with the combination parameter. For the security key, also it should have matched security key from transmitter to receiver. It is to prevent the stolen in power transfer process. The matching process of switching frequency and security key is when it waits a request from the receiver. During that process, if switching frequency and security key is matching synchronize at both part, it is shown that the power transfer to the authorized receiver. In other words, the power is efficiently transferred to correct receiver when the optimal switching frequency occurs. Apart from the same resonant frequency, security key at both transmitter and receiver should be the same value in order for optimal performance. The value of security is either 0 or 1 is purpose.

III. RESULTS AND DISCUSSION

This section discusses the findings from the simulation. The computer simulation is carried out by using MATLAB

programming to evaluate the security and performance of the resonant magnetic suggested coupling WPT system.

Table 3 presents the results of energy encryption in medium field WPT system on the mobile charging application system. This paper varies the possible taking power based on mobile charging application as reference for minimum and maximum value of power. So, it will conclude that, the best power level that can be transmitted are used and identify at which power level has optimal performance. Therefore, through simulation it proposed a comparison of the result.

The minimum and maximum power for the simulation is taken from 5W, 10W and 20W to realize the best execution in the system. Table III demonstrates the information of energy encryption of medium field WPT system for different power.

In 5W power, it can be demonstrated that, from section selector 0 until 7, the value of security key at the transmitter increase, while the logistic map value fluctuates. Moreover, switching frequency data start again when the section selector from 1 until 7. From the general information at table 3, the best performance synchronize switching frequency and security key is section selector 1. The best switching frequency is at 109 kHz and the security key value at the transmitter and receiver is 1.09 (transmitter) and 0.86 (receiver).

In 10W power, it can be seen that, from section selector 0 until 7, the security key value at transmitter increase, while the logistic map still inconsistently. In addition, switching frequency data raise from the section selector 0 until 7. From the usual statistics at table 3, the best execution synchronize switching frequency and security key is section selector 0. The best switching frequency is 102 kHz and security key at the transmitter to the receiver is 1.02 (transmitter) and 0.86 (receiver).

In 20W power, from the section selector 0 until 7, the security key at the transmitter is varied and the same goes to the logistic map value. Also, the switching frequency information raise from the section selector 0 until 7. With the general data of table 3, the outcome for power 20W does not achieve great execution. It is a result of the switching frequency and security key not coordinating with the transmitter and receiver. Thus, when no coordination for switching frequency and security key, the system cannot be exchange for the power.

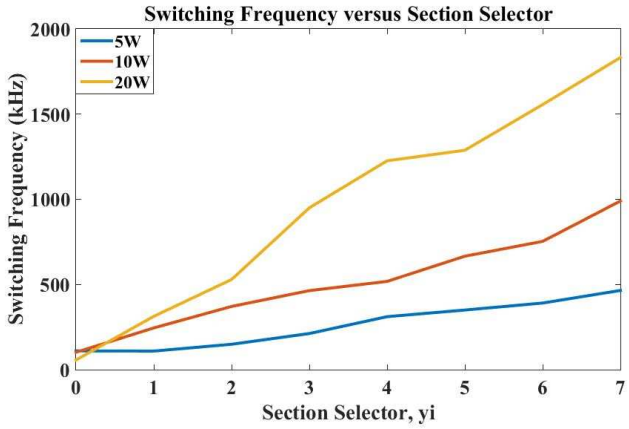

Fig.3 Comparison Result for Switching Frequency

Figure 3 demonstrate the comparison results for switching frequency. It can be realized that, the matching switching frequency with optimal switching frequency is accurate power 10W when frequency at 102 kHz of 100 kHz compared to 5W and 20W. Thus, the matching process success when the switching frequency and securely key occur simultaneously. In addition, at the receiver part of the security key value is 0.86 and maintain constant for 5W, 10W and 20W. Then, at the transmitter part of the security 8key value almost closed to the receiver which at 1.02 for 10W compared to 5W and 20W. For overall data for comparison of security key for transmitter and receiver part can be illustrated on Figure 4. Based on the result from simulation that was conducted, it can be concluded that when increasing the value of power, the matching process for switching frequency and security key is automatically fluctuated based on the complexity in the system. The effective power is 10 W and distance 4 cm in energy encryption for medium field of wireless power transfer system.

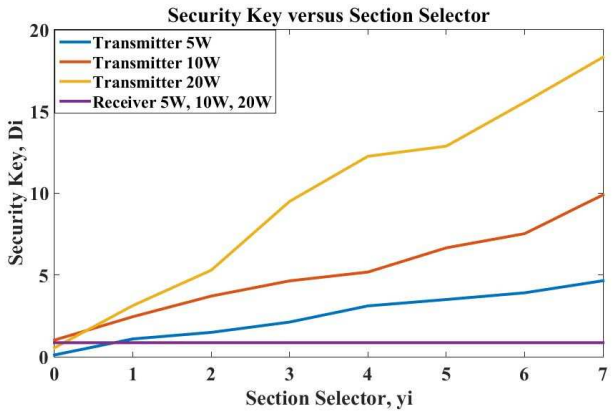

Fig.4 Comparison Result for Security Key

Figure 5 represent the comparison results for the logistic map. In logistic map process, it has lypunov exponent process to clarify a positive number and a non positive number from the logistic map. Thus, lyapunov exponent has the description which is a positive number. So, chaotic behaviour will occur when the lyapunov exponent becomes positive. The relation in Figure 5 is shown that, the logistic map at 10W produce larger positive value compared to 5W and 20W.

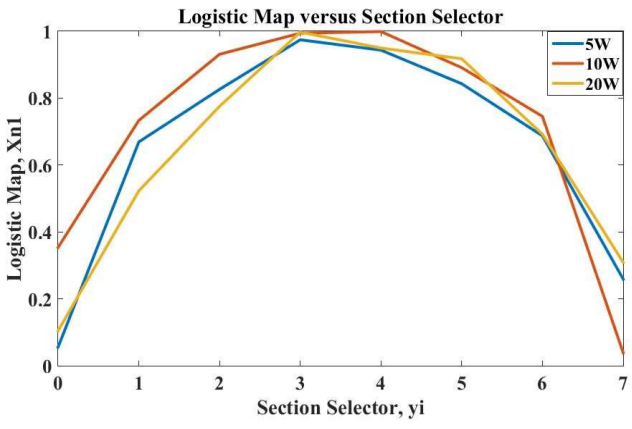

Fig.5 Comparison Result for Logistic Map

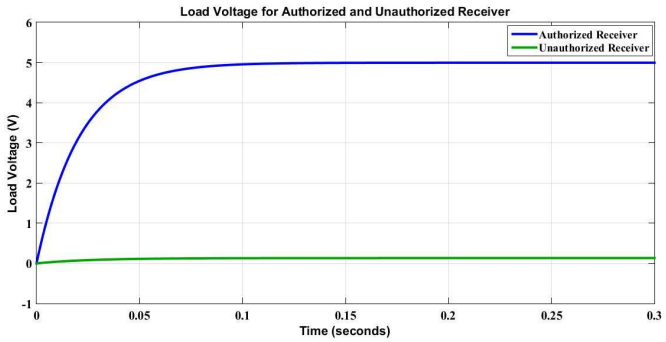

Fig.6 Comparison Load Voltage of Authorized and Unauthorized Receiver

Figure 6 tabulate the comparison load voltage of authorized and unauthorized receiver. The load voltage is 5V for authorized receiver while, for unauthorized receiver is around 0.15V. Furthermore, the authorized receiver differentiate depends on value of load voltage for transferring the power.

Based on the simulation finding above, the best performance in powering the mobile charging application system is 10W. It is because of the overall specification of 10W are fulfilled. The specification that has been investigated and proved earlier is made based on the three characteristics of chaos theory which are switching frequency, security key and the logistic map.

TABLE III
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, Transmitter	Receiver	Logistic Map, Xn1
0	5	4	100	110	0.1101	0,86	110
	10			102	1.02		102
	20			57	0.5471		57
1	5	4	100	109	1.09	0,86	0.6690
	10			245	2.45		0.7333
	20			313	3.13		0.5228
2	5	4	100	149	1.49	0.86	0.8262
	10			371	3.71		0.9311
	20			529	5.2916		0.7755
3	5	4	100	212	2.12	0.86	0.9744
	10			464	4.64		0.9942
	20			950	9.50		0.9973
4	5	4	100	311	3.11	0.86	0.9435
	10			518	5.18		0.9990
	20			1226	12.26		0.9497
5	5	4	100	350	3.50	0.86	0.8430
	10			666	6.66		0.8910
	20			1288	12.88		0.9176
6	5	4	100	391	3.91	0.86	0.6873
	10			753	7.53		0.7454
	20			1556	15.56		0.6919
7	5	4	100	465	4.65	0.86	0.2591
	10			990	9.90		0.0388
	20			1832	18.32		0.3090

All the characteristics is important to realized the energy encryption of medium field for wireless power transfer system and in order to achieve the main objective of this research which is protect the system form the unauthorized receiver.

IV. CONCLUSIONS

In this paper, to improve the security performance of the WPT the encrypted mobile charging system has been put forward. WPT must employ security measures to protect the system from unknown receptors or receivers. Clearly, many methods of magnetic resonant techniques have been proposed to reduce complexity, but at same time perform IM methods well. Resonant frequency and free positioning methods have low complexity and performance disadvantages. The most useful method is the strongly coupled resonance method because of its advantage in complexity and performance on the magnetic resonant coupling technique. As an encryption technique for WPT, chaos theory is complex, but exhibits good performance.The switching frequency is the key to chaotically regulation of the power supply. Meanwhile, authorized mobile charging system can definitely receive the transfer power to the accomplishment security key. Thus, for unauthorized mobile charging system the power transmission channel can be disabled. A security based on chaos theory algorithm for

energy encryption in medium field of wireless power transfer system is designed and created. At the distance 4 cm with power 10 W, it is capable to operate at the no load condition with matching security key of 1.02 transmitter and 0.86 receiver, also for switching frequency is matching on 102 kHz of 100 kHz working frequency. It also has the logistic map in chaos theory is 0.3539 with positive value of Lyapunov exponent. The simulation results have well agreed with the theoretically analysis and proved the validity of the proposed application of mobile charging system.

However, there are a suggestions provided by this paper in driving this idea forward for the betterment in the future. They are the variations in distances may be considered in order to maximize the power to transfer and increased the frequency consequently. With greater the frequency, may be increased by power to transfer from transmitter to receiver are increasing. In future, there is possibility for the new design of energy encryption for medium field of wireless power transfer system.

In addition, with the idea of designing energy encryption scheme in medium field by using chaos theory technique on the wireless power transfer for the mobile charging application. The similar approach by this research can be undertaken where increased the distance greater than 4cm in medium field also increased the power greater than 10W with new application which is laptop. Thus, in future the main aimed is produced new application with greater power and distance more far than this research.

Otherwise, this research fully work on the software but in future work it is will come out with implementation into hardware for the strong validation with software and also to publish in the industry for the marketing

ACKNOWLEDGMENT

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

[1] X. Mou and H. Sun, “Wireless power transfer: Survey and roadmap,” IEEE Vehicular Technolology Conference, vol. 2015, pp. 1–13, 2015.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Agbinya, Johnson I., "Wireless power transfer," River Publishers, vol. 45, 2015.

[7] 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.

[8] 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.

[9] A. Waser, “Nikola TESLA ’ s Wireless Systems,” English Publishers, pp. 1–14, 2000.

[10] Schuder, John C., "Powering an Artificial Heart: Birth of the Inductively Coupled - Radio Frequency System in 1960," Artificial organs on Electric Power, pp. 909-915, 2002.

[11] Schuder, John C., "Powering an Artificial Heart: Birth of the Inductively Coupled - Radio Frequency System in 1960," Artificial organs on Electric Power, pp. 909-915, 2002.

[12] A. Karalis, J. D. Joannopoulos, and M. Soljacic, “Efficient wireless non-radiative mid-range energy transfer,” Annals of Physics, vol. 323, pp. 34–48, 2008.

[13] S. L. Ho, J. Wang, W. N. Fu, and M. Sun, “A comparative study between novel witricity and traditional inductive magnetic coupling in wireless charging,” IEEE Transactions on Magnetics, vol. 47, pp. 1522–1525, 2011.

[14] W. C. Brown, “The History of Power Transmission by Radio Waves,” IEEE Transactions on Microwave Theory and Techniques, vol. 32, pp. 1230–1242, 1984.

[15] J. O. McSpadden and J. C. Mankins, “Space solar power programs and microwave wireless power transmission technology,” IEEE Microwe Magazine, vol. 3, pp. 46–57, 2002.

[16] K. T. Chau and Z. Wang, "Chaos in Electric Drive System," John Wiley Publishers, 2001.

[17] 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.