ENERGY ENCRYPTION FOR MEDIUM FIELD OF WIRELESS POWER TRANSFER SYSTEM

NUR HAZWANI BINTI HUSSIN

UNIVERSITI MALAYSIA PERLIS
2017

ENERGY ENCRYPTION FOR MEDIUM FIELD OF WIRELESS POWER TRANSFER SYSTEM

by

NUR HAZWANI BINTI HUSSIN
1630912058

A thesis submitted in fulfillment of the requirements for the degree of
Master of Science (Electrical System Engineering)

School of Electrical System Engineering
UNIVERSITI MALAYSIA PERLIS

2017

THESIS DECLARATIONS

UNIVERSITI MALAYSIA PERLIS

DECLARATION OF THESIS

Author's full name : ………………………………………………………………………………..........................

Date of birth : ……………………………………

Title : ………………………………………………………………………………..........................

………………………………………………………………………………..........................

………………………………………………………………………………..........................

Academic Session : ……………………………………

I hereby declare that the thesis becomes the property of Universiti Malaysia Perlis (UniMAP) and to be placed at the library of UniMAP. This thesis is classified as :

□ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

□ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

□ **OPEN ACCESS** I agree that my thesis is to be made immediately available as hard copy or on-line open access (full text)

I, the author, give permission to the UniMAP to reproduce this thesis in whole or in part for the purpose of research or academic exchange only (except during a period of _____ years, if so requested above).

Certified by:

_______________________	_______________________
SIGNATURE	**SIGNATURE OF SUPERVISOR**
_______________________	_______________________
(NEW IC NO. / PASSPORT NO.)	**NAME OF SUPERVISOR**
Date : _________________	Date : _________________

NOTES : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentially or restriction.

ACKNOWLEDGEMENTS

First and foremost, I am thankful to Allah SWT for His Mercy and Compassion that I managed to complete this study successfully. I would like to thank my parents for their exclusive attentions and thoughts they have given me without fail not only during the course of my study but throughout my entire life as I remember it.

I have accumulated many debts in completing this thesis over few years, since 2015, and it is a pleasure to acknowledge them. The most important persons are the study supervisors Dr Muhammad Mokhzaini Azizan, Madam Azuwa Ali and Dr Mahmoud A.M. Albreem. From day one they stood hand in hand with me and continually supporting and guiding me as a students as well as a person in general. It is an honour to work together with these unbelievably dedicated people.

At School of Electrical System Engineering UNIMAP, I have been blessed with great personalities all around and that makes life much easier socially and in term of conducting research works. Their expert guidance regarding my work are highly appreciated. The technical competence levels are beyond any reasonable doubt is among the few facilities that are hold in high regards.

The debt is also owned to many strangers who become close friends. It is unfortunate for me to not be able to name every single one of them here, but they know who they are. I have been blessed with great friends all along my life and they certainly belong in that category. Finally, I would like to acknowledge Ministry of Higher Education for funding my study here through the MYBRAIN'15 scheme. Without their presence, none of this is possible to finish my study. It is my time to lend a hand back to the nation. Insya Allah.

TABLE OF CONTENTS

CHAPTER 3 RESEARCH METHODOLOGY

CHAPTER 4 RESULTS AND DISCUSSION

CHAPTER 5 CONCLUSIONS AND FUTURE WORK

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

C	Capacitor
C_p	Primary capacitor
C_r	Resonance capacitor
C_s	Secondary capacitor
f_o	Frequency resonance
f_r	Resonant Frequency
I_p	Primary current
I_r	Resonance current
I_s	Secondary current
K	Mutual Inductance
L	Inductor
L_P	Primary inductive
L_r	Resonance inductive
L_s	Secondary inductor
P_{in}	Input DC Power
P_{out}	Output DC Power
r_p	Primary resistance
r_r	Resonance resistance
r_s	Resonance secondary
Z_p	Primary impedance
Z_r	Resonance impedance
Z_s	Secondary impedance

LIST OF ABBREVIATIONS

A	Bifurcation Parameter
ξi	Constant Value
$\xi i + 1$	Logistic Map
δ_i	Chaotic Security
ω	Switching frequency
ω_o	Resonant switching frequency

TENAGA PENYULITAN UNTUK BIDANG PERTENGAHAN DALAM SISTEM KUASA PENGHANTARAN TANPA TALIAN

ABSTRAK

Pada masa kini, pemindahan kuasa tanpa talian (WPT) pada aplikasi pengecasan mudah alih adalah proses memindahkan kuasa menggunakan teknologi WPT dan sedang berkembang pesat. Pelancaran mudah alih tertanam dengan sistem WPT menjadikannya teknologi yang paling mencabar buat masa ini. Dalam WPT, isu utama yang sedang disiasat memberi tumpuan kepada kecekapan pemindahan kuasa (PTE), jarak berkesan, saiz pemancar dan penerima sendiri. Selain itu, keselamatan pemindahan kuasa yang sangat penting dari penghantar kepada penerima yang dipilih mesti benar-benar selamat. Kegagalan untuk menjamin sistem WPT telah menjejaskan proses untuk memindahkan kuasa dari penghantar kepada penerima yang betul. Tesis ini membentangkan kaedah yang memanipulasi teori huru-hara untuk memastikan keselamatan tenaga disulitkan untuk memindahkan kuasa dan didapati sebagai cagaran pada penerima yang betul cekap dengan keselamatan yang lebih tinggi. Dalam teknik teori huru-hara, tidak mempunyai unsur kelakuan huru-hara yang sedang terbenam menggunakan peta logistik dan Lyapunov eksponen untuk keselamatan tambahan dengan padanan kekerapan penukaran daripada pemancar dan penerima. Kelakuan huru-hara dicetuskan pada setiap ciri dalam teori huru-hara adalah Lyapunov eksponen, Peta logistik dan menukar kekerapan. Untuk kajian ini, penggunaan WPT memberi tumpuan kepada permohonan caj mudah alih dan kecekapan keselamatannya diuji melalui teori huru-hara. Oleh itu, kajian terperinci dijalankan dengan mengubah operasi kuasa, jarak PTE berkesan dan gabungan pemuat. Sistem ini disimulasikan menggunakan pengaturcaraan MATLAB dengan mencipta dan mewujudkan persekitaran tempat WPT. Simulasi itu telah mengambil segala ciri-ciri dan spesifikasi permohonan pengecasan mudah alih yang terdapat di dalam pelbagai bidang sederhana. Kekerapan operasi adalah sekitar 100 kHz, kuasa operasi 10 W dan jarak diselaraskan dari 3 cm sehingga 5 cm. Simulasi yang dilakukan oleh sampel mengambil kira bahawa ciri teori huru-hara pada peta logistik, Lyapunov eksponen, yang hampir sama menukar kekerapan dan yang hampir sama kunci keselamatan. Lyapunov eksponen yang mencetuskan proses kekerapan yang hampir sama mesti lebih besar daripada 3.50. Bagi kajian ini, nilai eksponen Lyapunov dipilih oleh rawak dan ia adalah lebih besar daripada 3.50. Dari hasil pensampelan menunjukkan bahawa, kuasa itu dengan selamat dipindahkan oleh data berikut: menyampaikan kuasa 10 W, yang hampir sama frekuensi 102 kHz (± 2% pada 100 kHz) dan masing-masing yang hampir sama kunci keselamatan untuk pemancar dan penerima 1.02 dan 0.86. Sebagai kesimpulan, keputusan menunjukkan bahawa teknik teori huru-hara berkesan digunakan untuk keselamatan proses penyulitan tenaga. Ia juga berjaya memindahkan tenaga daripada penghantar kepada penerima yang dimaksudkan. Ini terbukti dengan penggunaan teknik teori huru-hara kuasa pemancar disulitkan rendah pada jarak 4 cm antara pemancar dan penerima.

ENERGY ENCRYPTION FOR MEDIUM FIELD OF WIRELESS POWER TRANSFER SYSTEM

ABSTRACT

Nowadays, the wireless power transfer (WPT) on mobile charging application of power transfer is the process of transferring power using WPT technology are progressing rapidly. The launching of more mobile embedded with WPT system make it as currently most demanding technology. In WPT, the main issue that being investigated are focused on power transfer efficiency (PTE), effective distance and the size of transmitter and receiver itself. Apart from that, the security of the power transfer is very important from transmitter to selected receiver must be completely secure. The failure to secure WPT system has affected the process to transfer power from transmitter to correct receiver. This thesis presents method which manipulates chaos theory to ensure the security of energy is encrypted to transfer and recovered as security at the correct receiver efficiently with higher security. In chaos theory technique, there are chaotic behaviour element which being embedded using the logistic map and Lyapunov exponent for additional security with matching the switching frequency of the transmitter and receiver. Chaotic behaviour is triggered on each characteristic which are Lyapunov exponent, logistic map and switching frequency. For this research, the application of WPT is focused on mobile charging application and its security efficiency is tested through chaos theory. Thus, detailed study is carried out by varying the power operation, distance of effective PTE and the capacitor combination. The system is simulated using MATLAB programming by creating and simulating WPT environment. The simulation took all the characteristic and specification of mobile charging application which is resides within medium field range. The operating frequency is around 100 kHz, operating power of 10 W and distance are adjusted from 3 cm to 5 cm. The simulation is done by sample taking into account that characteristic of chaos theory which are logistic map, Lyapunov exponent, matching switching frequency and matching security key. Lyapunov exponent which triggered the matching frequency process must be greater than 3.50. As for this research, the Lyapunov exponent value is chosen by random and it is greater than 3.50. The sampling result shows that, the power is securely transferred by the following data: delivered power of 10 W, matching frequency of 102 kHz (±2% at 100 kHz) and matching security key for transmitter and receiver of 1.02 and 0.86 respectively. As the conclusion, results show that chaos theory technique is effectively employed for security of energy encryption process. It also managed to transfer energy from a transmitter to the intended receiver. This is proven by the utilization of chaos theory technique of transmitter encrypted power at distance of 4 cm between the transmitter and receiver.

CHAPTER 1

INTRODUCTION

1.1 Research Background

Wireless power transfer (WPT) is one of the techniques to transfer the electrical power from a transmitter source to load receiver. WPT technology is fast developing as an effective way to transform power delivery applications. The WPT system is increasingly attracting attention in various fields, such as charging portable electronic devices and implanting medical devices (Stielua, O. H., & Covic, G. A., 2000). WPT is also suitable for Electric Vehicles (EVs), such as battery charging for normal vehicular operation and energy exchange (Woojin et al., 2012). In near future, there will be no more wire or cables to deliver power or energy to applications such as mobile charging application and EVs. Hence, the quality of life can be further upgraded in terms of convenience, mobility and safety. Basically, there are two types of WPT which are near-field (non-radiative coupling) and far field (radiative coupling). WPT technologies are categorized into inductive coupling, capacitive coupling, magnetic resonance and electromagnetic radiation (Mou, X., & Sun, H., 2015). The advantage of near field non-radiative coupling are safe, high frequency and long transmission distance by the receiver. In non-radiative coupling, the principal method is selected for short and mid-range WPT systems. WPT requires different optimization criteria for two uses which are continuous power delivery. For continuous charging, the system should be able to perform efficiently in term of fast, reliable, and energy efficient whether under stationary or moving states (Hirai, J., Kim, T. W., & Kawamura, A., 2000).

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. Encryption in wireless communication channels is vital and necessary in the present due to security concerns. Data need to be well encrypted during transmission over the wireless medium. Transmitted data that carries energy is transferred from a specific transmitter to desired receiver. It only goes through specific authorized energy transmission channel and guarantee certain amount of security. Thus, the security of energy transmission is an important issue (Bercich, R. A., Duffy, D. R., & Irazoqui, P. P., 2013). There are a few existing methods and techniques of encrypting energy process such as password system and Radio Frequency Identification (RFID). The most novel technique is using chaos theory. Therefore, this project will focus more on chaos theory technique for energy system encryption method. These technique was chosen because the behaviour of security itself is random which means that the system is more secured. Thus, the chaos theory technique also has the principle of stabilizing the system by using logistic map and Lyapunov exponent. The Lyapunov exponent is used to determine the stability of chaotic behaviour in the system. In addition, chaos theory technique is used to build up a secure energy transfer from power source to authorized receivers.

The magnetic resonant coupling for medium field WPT system by using chaos theory technique is 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.

1.2 Problem Statement

Previous research pointed out that energy encryption is very important due to the security aspect between the transmitter and receiver. Password and RFID system have their specific techniques but unfortunately, their efficiency are low. This shows that the two systems are not efficient in process encryption. Chaos theory technique is a complex system with high efficiency in term of encrypting and transmitting energy. Through chaos theory method, the security of power transfer is generated as the transmitter and receiver is matched by creating logistic map, Lyapunov exponent value, matching switching frequency and matching security key. This security process secured the transfer from a specific transmitter to the desired receiver.

1.3 Objective of Research

There are a few objectives this thesis aim to meet upon its completion. They are:

i. To design security based on chaos theory algorithm for energy encryption in medium field WPT system.

ii. To validate the improved chaos theory algorithm for medium field WPT system.

1.4 Scope of Research

In completing this thesis, a few scopes of research are determined in order to gather the attention to the desired focus.

i. The chaos theory algorithm will be used as the encryption technique of WPT. The chaos theory algorithm is modified through logistic map, Lyapunov exponent, switching frequency and security key. The algorithm is create by using MATLAB programming.

ii. Focusing on medium field WPT with range distance in 4 centimetre (Jawad, A. M., Nordin, R., & Gharghan, S. K., 2017) under single receiver at no load conditions in power 10 W for mobile charging application.

1.5 Contribution of Research

This research contributes mainly on design effectiveness and simple energy encryption technique using chaos theory algorithm in medium field for WPT system to encrypt the energy. The implementation of the system is done through simulation to validate the encryption process. Contribution of research is enhanced through hybrid security system. This is done by combining password and chaos theory techniques. This combination further enhances WPT system security.

1.6 Thesis Layout

This thesis can be divided into five main chapters. These main chapters include introduction, literature review, methodology, results and discussion and lastly the conclusion.

Chapter 1 covers on the introduction of this project. Besides that, problem statement, objectives of the project, scopes of the project and report outline are also explained briefly.

Chapter 2 shows the literature review which contain explanations about the background theory of WPT system and chaos theory technique in medium field. It also explains on the advantages and disadvantages of every technique of WPT system and encryption process.

Chapter 3 is about the methodology. This chapter covers on every single step that taken to fulfill this project including the flow chart and all methods required for the project in sequence.

Chapter 4 is the result and discussion. It contains the results acquired after the simulation has been done using MATLAB programming software. The analysis was made from the results obtained.

Chapter 5 is the final conclusion on whole project. It highlights whether the work completed complies with the set objective and the significant of the findings. Problems that have been faced during this whole project are also stated in this chapter including the suggestions on how to solve this problem in the future.

CHAPTER 2

LITERATURE REVIEW

2.1 History of Wireless Power Transfer (WPT) System

In 1901, Nikola Tesla started constructing his famous Wardenclyffe Tower near Long Island (Waser, 2015). The tower was used to broadcast sound by employing wireless communication and transmitting power without utilizing conducting wires (Waser, 2015). Tesla's work was impressive 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 (Karalis, 2008). The aim is to seek ways to 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 (Jonah, O., & Georgakopoulos, S. V., 2013).

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 5 W mobile phone charging (Karalis, 2008). Moreover, the operating frequency range of the inductive coupled technique is generally from 20 kHz to several MHz (Karalis, 2008). However, when efficiency is achieved, coil distances further enlarge or have more freedom in positioning the source and load relative to each other. In order 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 (Jonah et al., 2013). Compared with electromagnetic radiation, resonant coupling has advantages, such as higher efficiency in omnidirectional transmission and insensitivity to the surrounding environment (Ho, Wang, Fu, & Sun, 2011). The operating frequency range from 10 kHz to approximately 200 MHz has been used in several studies on resonant coupled WPT (Yoon & Ling, 2013). However, electromagnetic radiation can be classified into unidirectional and omnidirectional radiation based on energy transmitting direction. The far-field approaches balance between directionality and transmission efficiency (Mcspadden & Mankins, 2002). Radio frequency (RF) and microwave systems are examples that benefit from the transfer power over a distance of several kilometres at 90% efficiency by using high-gain antennas (Mcspadden & Mankins, 2002).

In summary, the WPT system can be divided into three concepts which are 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.

2.2 Overview of WPT System and Energy Encryption

This section presents the overview of WPT system and energy encryption. This section divided into two part which is WPT system and energy encryption in details.

2.2.1 WPT System

As explained previously, WPT technologies can be categorized into three fields, namely, near field, medium field, and far field. Each field has different ways and techniques to transfer power via WPT.

In near field, the power transfer by magnetic field uses inductive and capacitive coupling between coils and wires (Zenkner, 2010). The fields are non-radiative, and energy stays within a short distance of the transmitter. If no receiving device or absorbing material exists within the material range, then no power will leave the transmitter. In addition, if these fields are short, then the distance depends on the size and shape of antenna devices, which are usually coils of wires. Appropriately, the concept of the near-field WPT centers on a system with short-range power transfer for charging mobile and handheld computing devices, such as cellphones, digital music players and portable computers without being secured to a wall plug (Zenkner, 2010).

In medium field, the range of distance and the technique will be considered in the transfer of power. Generally, magnetic resonance coupling is used for medium field or medium range WPT. In WPT technology using magnetic resonance coupling, impedance matching (IM) is applied to adjust the frequency resonance (Ahmed, 2015). IM can change the frequency for different air gaps and improve the efficiency of power transfer. Energy encryption for the medium field WPT system is an important security issue (Ahmed, 2015).

Meanwhile, the far field WPT is a system with long-range power transfer needed for low-power sensors, networks, and space applications (Beh, Imura, Kato, & Hori, 2010). Far field has a range of better choices for low-frequency antenna, where simple patterns or cut measurements are required (Beh et al., 2010). In addition, far-field power has several practical advantages over inductive powering, which is the accurate alignment of primary and secondary coils for efficient operation. Far field powering uses an alternative wireless powering scheme and requires more understanding of the receiving power capabilities of implantable devices (Costanzo, 2016). For example, microwaves and laser beams are used to transmit power in long distances. Nonetheless, the far field system has to limit the exposure of people and other living things to such power transfer (Matsumoto, 2003).

The differences between each field considered the distance needed to transfer power to the receiver, which is near field in millimeter (mm) to several centimeter (cm), medium field in centimeter (cm) to several meter (m), and far field in kilometer (km) ranges. The advantages and disadvantages of these fields could be seen in the example in near field, whereby the power will transfer only at a short distance, such as charging a mobile phone pad. In addition, the system can transfer only a practical amount of power. Thus, the far field, which is used only for long distances, would require more microwave and laser wave applications. Thus, radiation might be concentrated into a narrow beam aimed at the receiver (Yoon & Ling, 2012). To better understand WPT, Fig. 2.1 shows the WPT circuit, which converts current from alternating current (AC) to direct current (DC).

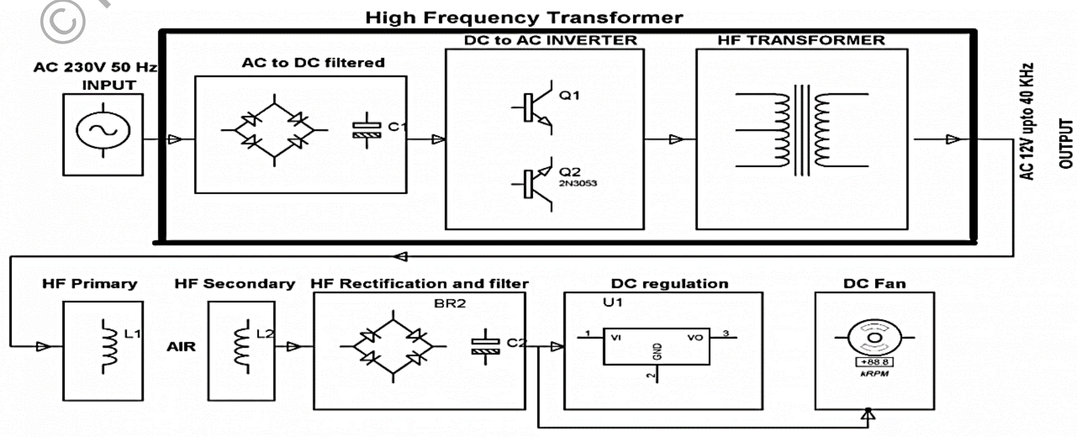

Figure 2.1: Wireless Power Transfer Circuit (Yoon & Ling, 2012).

2.2.2 Energy Encryption

Encryption is one of the most important processes in WPT because this step transforms data into an incoherent form (Xia, 2015). Encrypted data is known as cipher text or the original form of the message (Xia, 2015). This process is considered a secured secret form for anyone who does not have the decryption key (Xia, 2015). Thus, original data can be obtained only by using a decryption process (Xia, 2015). Decryption is the reverse process of encryption. During encryption, two types of algorithms used are symmetric and asymmetric. Fig. 2.2 shows the process of symmetric encryption, and Fig. 2.3 shows the process of asymmetric encryption (Wang, X. A., Ma, J., & Xhafa, 2015).

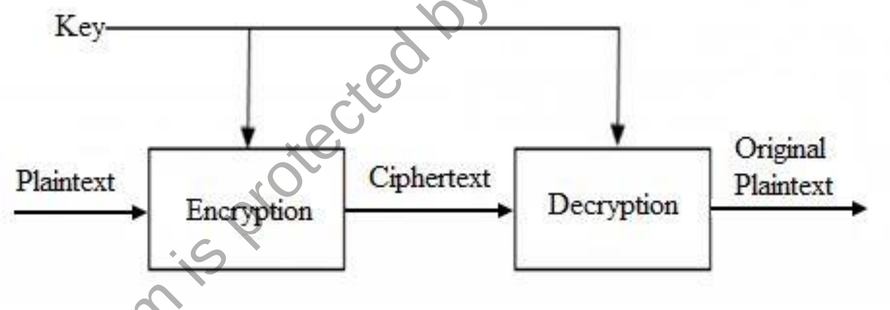

Figure 2.2: Symmetric Encryption (Wang et al., 2015).

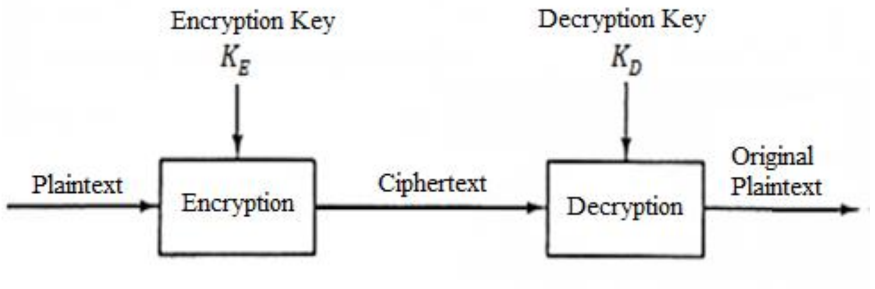

Figure 2.3: Asymmetric Encryption (Zibideh et al., 2014).