Authorized Wireless Charging System based on Double-Frequency-Hopping for Mobile Devices

Yangjae Lee[1], Dongmin Yang[2], Taek-Young Youn[3]*, and Ki-Woong Park[4]†
[1]Sejong University SysCore Lab, Seoul, Republic of Korea
leelambjae@gmail.com
[2]Chonbuk University Jeonju, Republic of Korea
dmyang@jbnu.ac.kr
[3]ETRl, Daejeon, Republic of Korea
taekyoung@etri.re.kr
[4]Sejong University, Seoul, Republic of Korea
woongbak@sejong.ac.kr

Abstract

As the number of mobile devices used in everyday life increases, interest in wireless charging technology for continuous use anytime and anywhere is increasing. The existing wireless charging method transmits power to all mobile devices within the transmission distance, which causes unauthorized users to gain access to the service, thus causing security problems. Therefore, a technology for verifying the usage right to filter unauthorized users is emerging as a main technology of wireless charging technology. In this paper, we propose the security requirements for verifying the authority of the wireless charging users based on the requirements for providing the resources to the authorized users and the technical research for transmitting the power to the existing wireless communication method. Considering the moving target defense technology, we designed and implemented a double-frequency-hopping based wireless charging system for COTS mobile devices, based on the security requirements.

Keywords: Wireless Charging System, Mobile Authentication, Mobile System

1 Introduction

In the modern society, as the number of mobile devices that used in daily life is increasing, people are asking to charge their mobile devices everywhere. To satisfy this requirement, the unmanned wire smartphone charging device [6], which can charge smartphones in the public place is developed. However, limitation of the wire makes people hold in the wire, so charging the device in a public place cannot satisfy the requirement of people. For these reasons, many people's attention is moving to wireless charging system from the former wired charging system.

There are three ways to wireless charging. The first wireless charging technology is Magnetic Inductive Coupling [7] that mobile devices are charged in short distance. Although its efficiency is very high, it is inadequate for a wireless charging system which aims to enhance mobility because of its transmission distance. The second technology is the Magnetic Resonant Coupling [4] that mobile devices are charged in the middle distance with high efficiency. The transmission distance of Magnetic Resonant Coupling supports up to several meters. The last technology is Electromagnetic Radiation that energy

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 9 (September 15, 2018)
*Corresponding author: ETRI, 138, Gajeongno, Yuseong-gu, Daejeon, 34129, Korea, Tel: +82-(0)10-6851-3238
†Corresponding author: Sejong University, 98, Gunja-dong, Gwangjin-gu, Seoul, Korea, Tel: +82-(0)2-6935-2453, Web: http://home.sejong.ac.kr/~woongbak

Table 1: Wireless Power Transfer Technology

Name	Magnetic Inductive Coupling	Magnetic Resonant Coupling	Electromagnetic Radiation
frequency Table	110KHz $\sim$ 205KHz (Qi Standard)	tens of KHz $\sim$ a few MHz	2.45GHz, 5.8GHz
Distance	$\sim$ 2 inch	$\sim$ a few yard	$\sim$ tens of mile
Charachers	sensitive to position	every same frequency is affected	harm for human
Transmitted Power	$\sim$ 10 W	10W $\sim$ tens of W	High

can be transmitted very long distance. Electromagnetic Radiation is used in satellites which transmit solar energy from space to earth [9]. However, its efficiency is too low compared to another technology, and it needs a huge equipment. When many aspects such as distance, efficiency, and characters are considered, *MRC* (Magnetic Resonant Coupling) technology is adequate for wireless charging in public place. However, when the *MRC* technology is used, because of its character that every device which has the same frequency are charged, unauthorized users who know the frequency can charge in the transmission distance. Therefore, an additional technique that identifies authority of the user is required to apply pay as you go pricing model in *MRC* technology. However, until now researches which considering pay as you go pricing model on *MRC* is little. If wireless charging service starts without a definite authentication process, unauthorized users also can charge as same energy as the authorized users. Therefore, a wireless charging system for COTS mobile devices must transfer energy only Users who have the authority. Overall generation process is shown in Figure 1.

In this paper, we implemented authentication process and *D-FHSS*(Double-Frequency-Hopping Spread Spectrum) to graft pay as you go pricing model in Magnetic Resonant Coupling, considering the inherent problems of *MRC*. Double-Frequency-Hopping Spread Spectrum technology is modified version of original *FHSS*(Frequency-Hopping Spread Spectrum) technology that prevents jamming and eavesdropping by hopping the frequency very frequently. By using the special value that deploy the schedule, *D-FHSS* enhance the security in wireless power transfer. The goal of this paper is to maximize the charging speed gap between authorized users and unauthorized users by limiting the information. Additionally, using a hash chain and reverse hash chain, we make users be able to charge only for a pre-defined time.

The rest of this paper is as follows. In Section 2, we investigate precede researches that charge only authorized user. And our research and related researches are differentiated. In Section 3.1, we discuss overall system architecture and design. In Section 3.2, an algorithm that generates an authentication code is presented. In Section 3.3, we described an algorithm that identifies users in the process of the creating the necessary value. In Section 3.4, an algorithm that makes scheduling rules using the key code for transmitting the energy is presented. In Section 4, to prove security from attackers, some attacks are analyzed.

2 Related Work

Spread spectrum technique[8] is used to protect data from attackers in wireless communication. Spread spectrum technique is not only to prevent frequency collision between users but also enhance the security abilities such as anti-jamming and anti-eavesdropping. [3] There are two typical types of spread spectrum techniques *DSSS* (Direct Sequence Spread Spectrum) and *FHSS* (Frequency Hopping Spread Spectrum). In *DSSS* technique, the digital signal is spread. *DSSS* is superior to *FHSS* in power efficiency and bandwidth efficiency. *DSSS* has been used in cordless telephones, cellular telephones, and

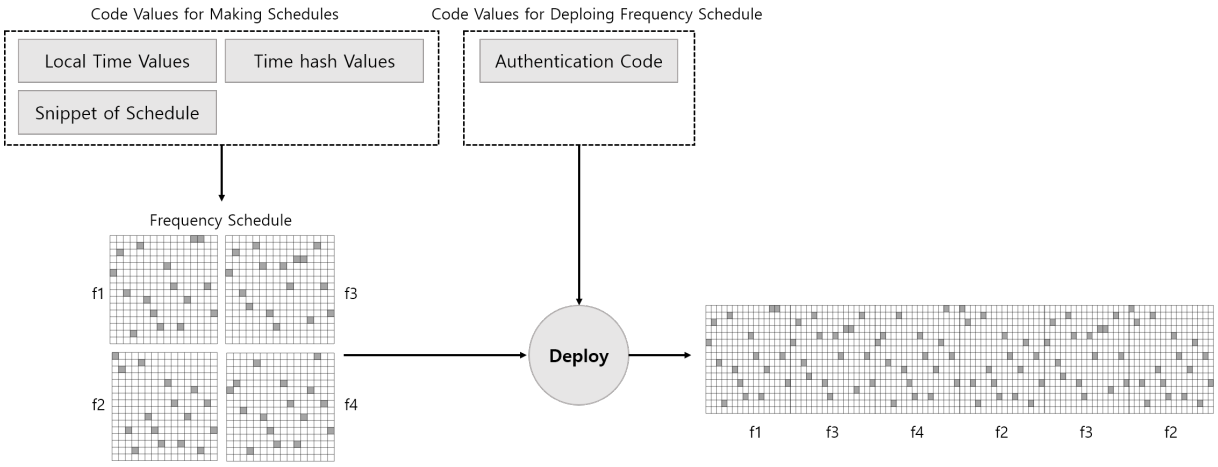


Figure 1: Overview of Double-Frequency Hopping Spread Spectrum

LR-WPAN(Low Rate Wireless Personal Area Networks) [2]. *FHSS* technique prevents jamming and eavesdropping attack by hopping the frequency. Only those who know the frequency hopping schedules can receive the data or energy. *FHSS* has been used in the physical layer of sensor networks to increase security [12] and used when implementing secure data communication transmitter [5].

Our goal is to maximize the charging speed gap between authorized users and unauthorized users. There are some studies which maximize the charging speed gap between authorized users and unauthorized users.

Dunworth et al. proposed systems and methods for selective wireless power transfer [1]. In this patent, Using the time-dependent pseudo-random sequence, authorized receiver varies its impedance and receives wireless power.

Zhang et al. proposed energy encryption for wireless power transfer [11]. In this paper, they implement secure energy transmission channels using Magnetic Resonant Coupling. Power supply encrypts the energy by chaotically regulating the frequency of the power source. Then, the authorized receptor receives the energy based on the security key.

Zhang et al. proposed an efficient wireless power transfer system with security considerations for electric vehicle applications [10], which makes a secure inductive *WPT*(Wireless Power Transfer) system to transfer the energy to specific receptors in the multi-objective system.

Our research is similar to [1], [11], [10] but, our study based on characters of *MRC* and *FHSS*, so do not need additional authentication. Because *MRC* only charge energy with the same frequency, the different frequency is not charged. In this regard, if the frequency is hopped using *FHSS*, only those who know the frequency scheduling rules will be able to charge. Because we use characters of *MRC* and *FHSS* instead of additional authentication, our research can reduce additional overhead from authentication.

3 System Design

We designed the *D-FHSS* to implement authorizing wireless power transfer service. Our *D-FHSS* design principle is divided into four phases and three algorithms. The first phase is purchasing phase when User purchase code from Seller. The second phase is authentication phase when User generates correct schedule which required for charging on Charging center. Next phase is phase of use when User charges

their mobile devices by using the schedule rules made by the Scheduling algorithm. The last phase is time over phase when Users cannot charge anymore. First algorithm is generation algorithm. In the generation algorithm, Seller makes code according to time, location, and password. Next algorithm is the identification algorithm. User can make authentication code which deploy scheduling rules. The last algorithm is the scheduling algorithm. Using scheduling rules and authentication value, User can deploy this scheduling rules to make D-FHSS scheduling code.

3.1 The *D-FHSS* Architecture Design Principle

User, Seller, and Charging center participate in this process. To prevent attacks and maximize the charging speed gap between authorized users and unauthorized users, *D-FHSS*, which charging the energy only those who know the frequency schedule is implemented. Figure 2 represents overall authentication transaction.

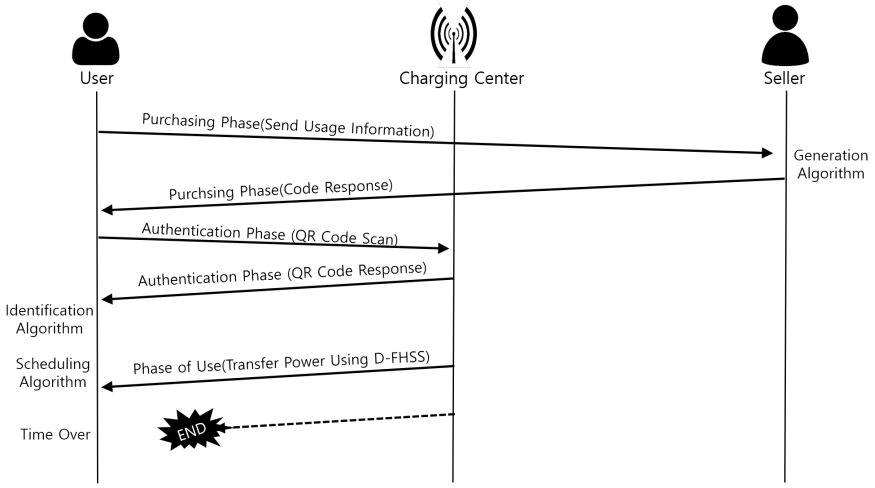


Figure 2: Overall Authentication Transaction of The Proposed Charging System

- **Purchase Phase**
  Purchase phase is shown in Figure 3. When User buy energy charging voucher, User sends **Message 1-1**, which consists of the time, location, password to Seller. Each value will be exchanged to corresponded value in generation algorithm. Specific generation algorithm process is described in Section 3.2. **Message 1-2**, which consists of the Time Hash Value (T), Local Time Value(L), Authentication Value to Send(A_{send}), and Snippet of Schedule(S_{send}) are send to User from Seller.

- **Authentication Phase**
  Authentication phase is shown in Figure 4. In the authentication phase, User scan the QR code in specific area. When User scan the QR code, Charging center check the occupied channels and transmit **Message 2-1**, which consists of series of public key. In identification algoritm, User can identify which public key is fit to the authentication value. Specific identification algorithm is described in Section 3.3.

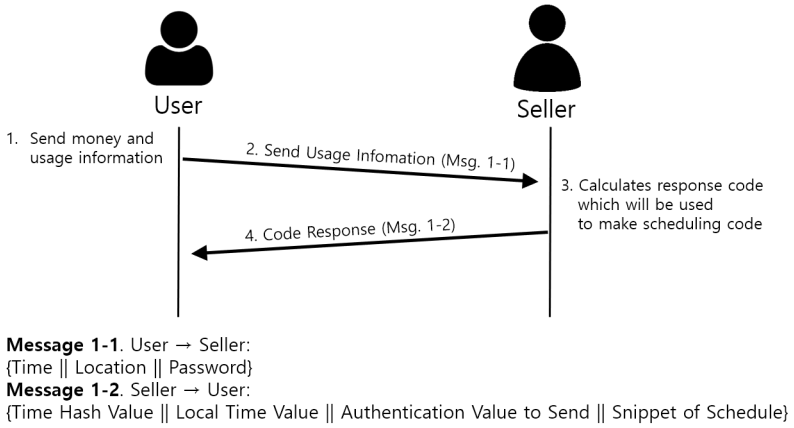


Figure 3: Message Transaction of Purchase Phase

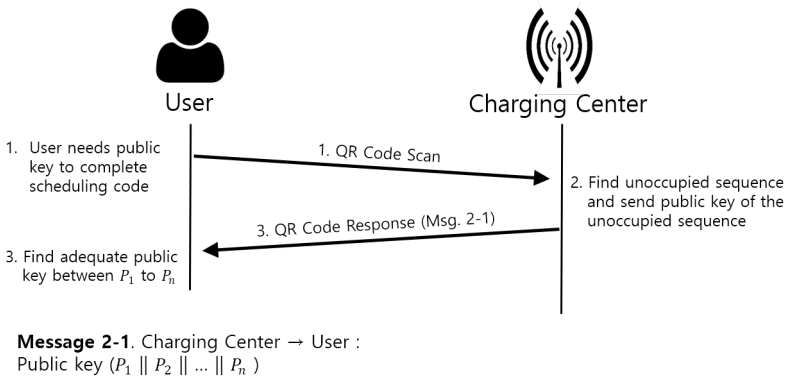


Figure 4: Message Transaction of Authentication Phase

- **Phase of Use**
  Phase of Use is shown in Figure 5. Time Hash Value (T), Local Time Value(L), Authentication Value, and Schedule Rules are entered in scheduling algorithm so that User can make *D-FHSS* scheduling code, which used to charge mobile devices.

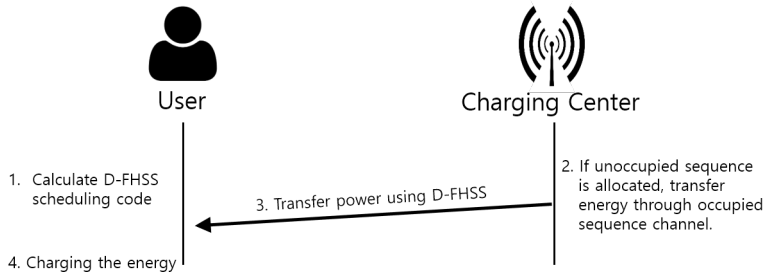


Figure 5: Energy Transfer of Phase of Use

- **Time Over Phase**
  Phase of Use is shown in Figure 6. User cannot charge devices because they didn't have the next

Time Hash Value. If no one use the particular energy transfer channel, Charging center stops transferring energy.

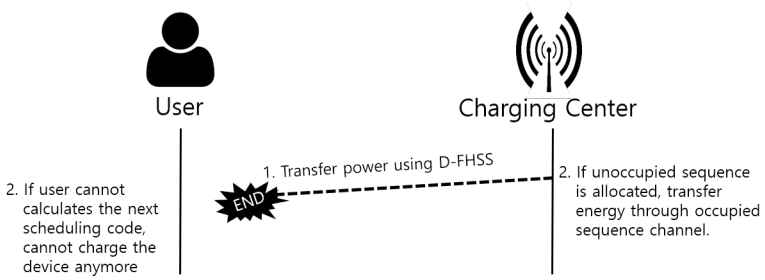
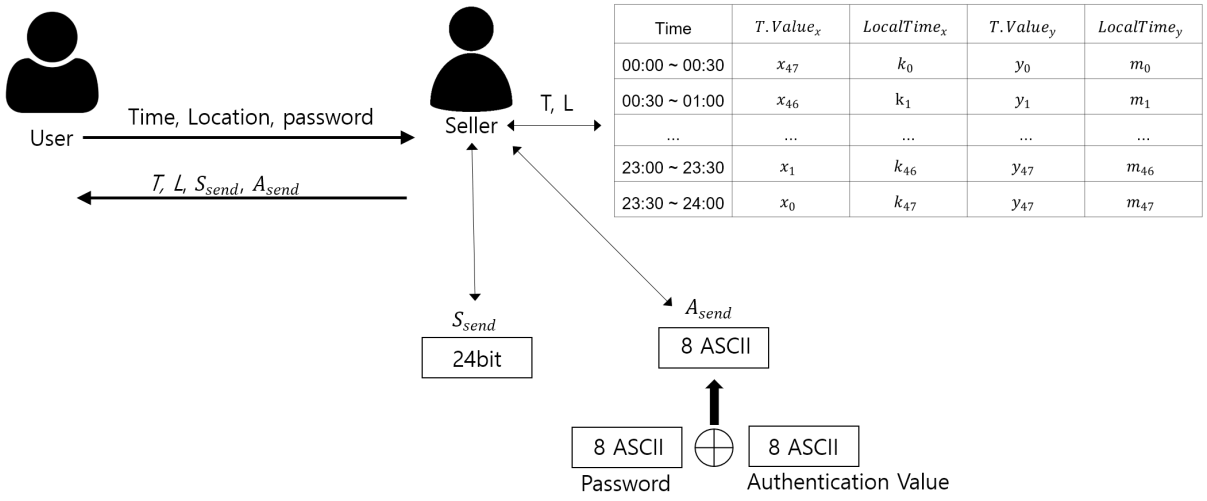


Figure 6: End of Charging

3.2 Generation Algorithm

Time value which selected by User is substituted to the correspond time hash value in the timetable in table 2. Then corresponded value is transmitted to User. Location Value is used to select local time table of Charging center. Location value is unique to a certain area. Password consist of 8 ASCII codes and Seller generates A_{send} which can make authentication value if XOR with the password value. Using the time hash value and location value and S_{send}, the user makes four schedules: f1, f2, f3, f4.



Time	$T.Value_x$	$LocalTime_x$	$T.Value_y$	$LocalTime_y$
00:00 ~ 00:30	x_{47}	k_0	y_0	m_0
00:30 ~ 01:00	x_{46}	k_1	y_1	m_1
...	...	...	...	...
23:00 ~ 23:30	x_1	k_{46}	y_{47}	m_{46}
23:30 ~ 24:00	x_0	k_{47}	y_{47}	m_{47}

Figure 7: Overall Generation Algorithm Process

3.2.1 Time Table

Time table supports users to charge at the expected time. For example, if 24 hours are divided into 30-minute units, time table will consist of 48 rows as shown in Table 2. 24 hours can be divided according to the time precision the administrators wants. Using the *PRNG*(Pseudo Random Number Generator), random values x_0 and y_0 is created every day at midnight. In this study, the SHA256 hash function is

used to generates reverse hash chain table and hash chain table.

Two hash chain table is created at midnight and the x value is hashed from 23:30 to 00:00 inversely. The y value is hashed from 00:00 to 23:30. $T.Value_x$ means end of the charging time, and $T.Value_y$ means the start of the charging time. After that, Seller sends $T.Value_x$ and $T.Value_y$ to User. To identify the charging place, $LocalTime_x$ and $LocalTime_y$ is used. When User calculates next hash, unique $LocalTime_x$ and $LocalTime_y$ is appended in the hash value. The prcoess of generating hash chain is shown in Figure 8.

Table 2: Time Table

Time	$T.Value_x$	$LocalTime_x$	$T.Value_y$	$LocalTime_y$
00:00 ∼ 00:30	x_{47}	k_0	y_0	m_0
00:30 ∼ 01:00	x_{46}	k_1	y_1	m_1
...	...	...	...	...
23:00 ∼ 23:30	x_1	k_{46}	y_{46}	m_{46}
23:30 ∼ 24:00	x_0	k_{47}	y_{47}	m_{47}

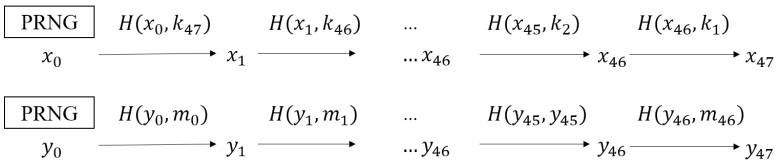


Figure 8: The Process of Generating Hash Chains

In the Figure 9, User buy 00:00 ∼ 01:00 voucher. The x_{46}(`2AB2C643...`) and Local time at 00:30 ∼ 01:00 (k_1) is given to User. Using these values, User can calculate next hash x_{47}(`2D711542...`). Similarly, User receive y_0 (`A1FCE436...`) and 00:30 Local time at 00:00 ∼ 00:30 (m_0). Using these values, User can calculate next y_1(`D3CC0DF2...`).

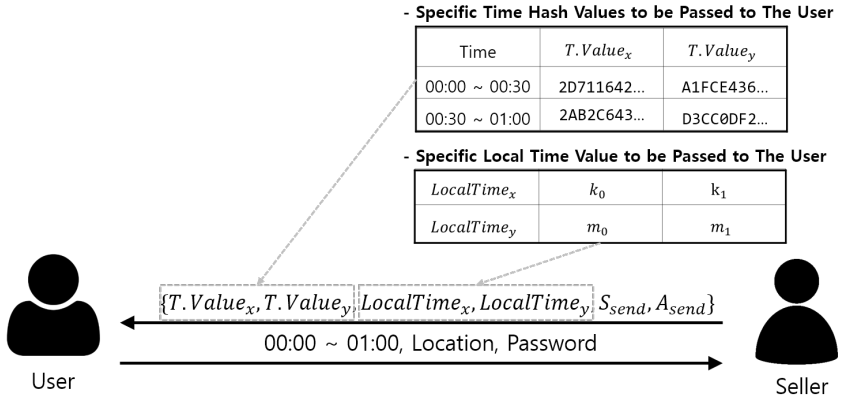


Figure 9: The Generation Algorithm Which User Buy the Voucher 00:00 ∼ 01:00

3.3 Identification Algorithm

User receive sequence value which consists of multiple public keys from Charging center. Each public key consists of 24 bits and only one public key can make schedule code. To find the adequate public key, User XOR snippet of schedule and every public key. If last 8 bits are same as the first character of $T.Value_y$, it is correct public key. First 16 bits will be used to make schedule rule and last 8 bits will be used to check.

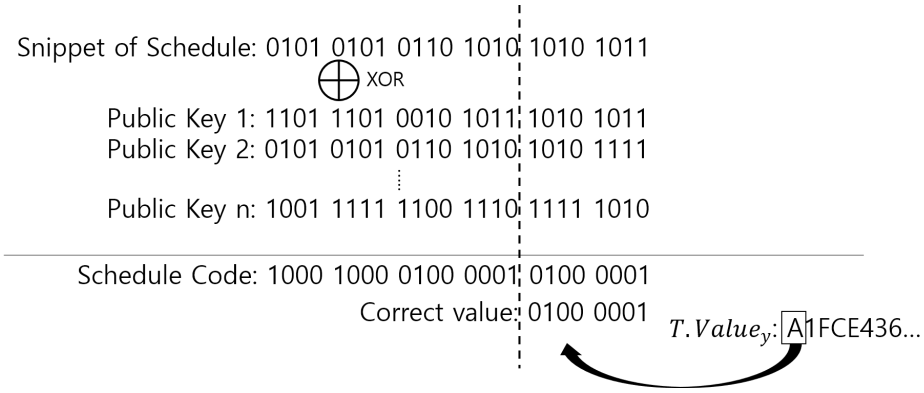


Figure 10: The process of finding correct public key

Using the first 16 bits of schedule code, time hash value, and local time value, schedule rules can be generated in Section 3.4. Figure 10 shows the calculation of snippet of schedule and public key. To find schedule code, User XOR snippet of schedule code and public key P_1 to P_n. For example, if first character of $T.Value_y$ is A and last 8 bits of XOR operation result is `0100 0001`, then that value is correct public key.

3.4 Scheduling Algorithm

Each ASCII code of hash x and hash y are extracted according to the schedule value. This process is repeated four times to make four schedule rules: f1, f2, f3, f4. Because sha256 hash consist of 256 bits, it is possible to divide 256 bits into 64 bits. It is also possible to use other hash algorithms. Schedule rules are drawn from the Table 3 by extracting equivalent frequency. The process which draw schedule rules are shown in Figure 11. In the Figure 11, x hash and y hash are extracted according to schedule value and used to make frequency schedule by referring the Table 3.

Table 3: Frequency Table

0000	0001	0010	0011	0100	0101	0110	0111
50 MHz	100 MHz	150 MHz	200 MHz	250 MHz	300 MHz	350 MHz	400 MHz
1000	1001	1010	1011	1100	1101	1110	1111
450 MHz	500 MHz	550 MHz	600 MHz	650 MHz	700 MHz	750 MHz	800 MHz

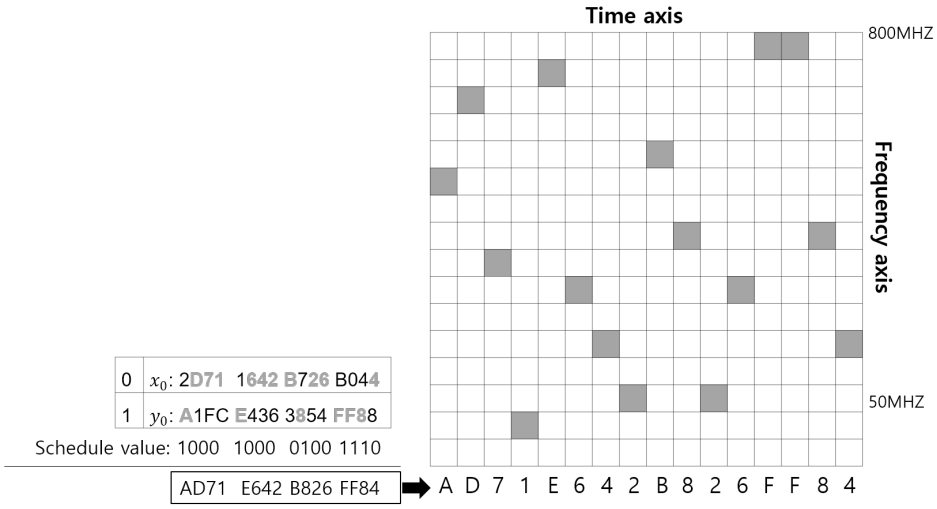


Figure 11: Method to draw schedule rule using schedule value

3.4.1 Authentication Value

When User buys a voucher, User sends 8 ASCII password to Seller. Seller calculates an authentication value that can be calculated by XORing the password and A_{send}. After that, Seller sends A_{send} to User. Authentication value is used to deploy the schedule rules. In the Figure 12, the authentication code is changed to binary and used to deploy the schedule according to the mapping rule. Also, according to the number of mapping rule, the authentication code can be divided. In the Figure 12, authentication value is divided into quad because the number of mapping rule is four.

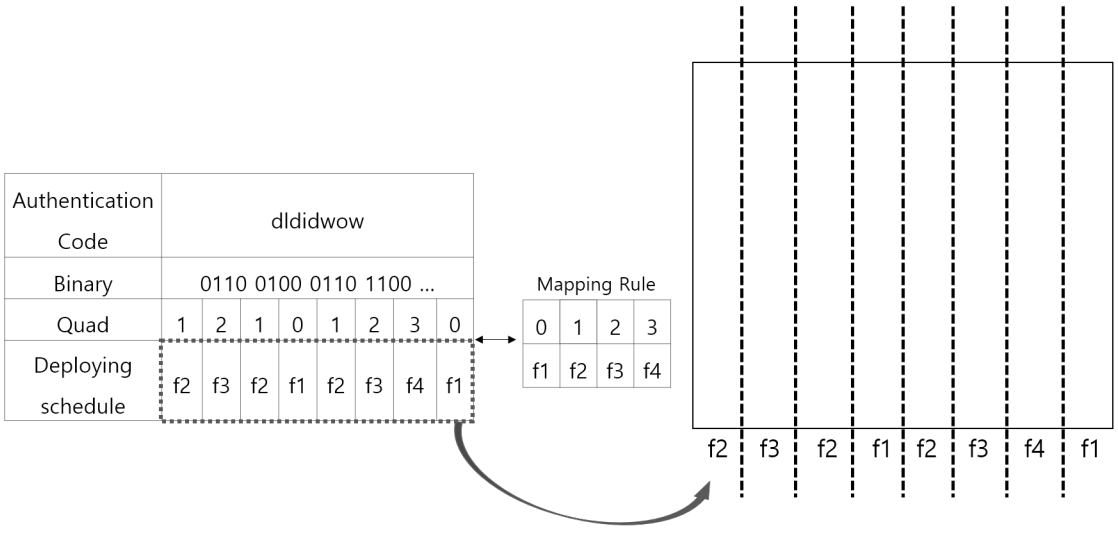


Figure 12: Deploy Shedule Rules According to Authentication Code

4 System Analysis

We analyzed the *D-FHSS* safety by considering replay attacks, collision attacks, and eavesdropping attack. We assumed that the purchasing phase which User sends time, location, and password to Seller transmitted directly; hence, eavesdrop the purchasing phase is impossible. In this section, we prove the safety of our proposed *D-FHSS* authentication process in replay attack, collision attack, and eavesdropping.

Theorem 1. *D-FHSS* is safe from replay attacks

Proof: We implement every value changed from a minimum of 30minutes to a maximum of one day. To make the correct schedule, attackers need . $TimeHash_x$,$TimeHash_y$, $LocalTime_x$, $LocalTime_y$ and authentication code. However, even if attackers reuse whole value used in yesterday, it is impossible to use the following day because TimeHash and$LocalTime_x$ is changed every 30 minutes. Therefore it is impossible to use the formal code for charging.

Theorem 2. *D-FHSS* is safe from Collision attacks

Proof: A collision attack is executed when more than one attacker colludes to use service illegally. To prevent collision attack, *D-FHSS* implemented local time table. If local time values (LocalTime) does not exist, malicious User who buys end part of the Time table (23:30 24:00) can draw every x time hash value. And malicious User who buys start part of the Time table (00:00 00:30) can draw every y time hash value. If they collude with each other in the collusion attack, they can use service all day long illegally. However, because they need local time table for calculate next hash, they cannot gain other time's hash.

Theorem 3. *D-FHSS* is safe from Eavesdropping

Proof: When attackers eavesdrop communication between User and Charging center, attackers can get time hash values (TimeHash) and local time values (LocalTime), and schedule value. However, even if attackers get these values, attackers cannot eavesdrop password because it is transferred directly between User and Seller. Without password of User, attackers cannot get authentication value which used to schedule the schedule. Therefore, the authentication code which deploy the schedule rules cannot be generated.

5 Conclusion

To apply pay as you go pricing model in wireless charging service, we implement *D-FHSS* which verify authorization of users. Additionally, to increase the availability of user, we also provide time service which is used to user select time when they want. This *D-FHSS* is secure from attacks such as replay attack, collision attack, eavesdropping attack. However, this technique has a problem. When an unauthorized user scans the QR Code in Charging center, Charging center may waste energy until authorized user coming. Of course, it can be prevented by install the energy scanner which checks the energy use in charging center.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (NRF-2017R1C1B2003957, NRF-2016R1A4A1011761) and supported by Institute for Information communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00420, Development of Serverless Cloud Computing technology for resource allocation and usage measurement by API call unit), Disaster-Safety Platform Technology Development

Program of the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT. (NRF-2016M3D7A1912703)

References

[1] J. D. Dunworth, R. W. Martin, M. Selby, D. Maldonado, K. H. El-Maleh, and Y. Karmi. Systems and methods for selective wireless power transfer, October 2013. US Patent 8,547,057.

[2] M. Hasan, J. M. Thakur, and P. Podder. Design and implementation of fhss and dsss for secure data transmission. *International journal of signal processing systems*, 4(2):144–149, April 2016.

[3] R. Kohno, R. Meidan, and L. B. Milstein. Spread spectrum access methods for wireless communications. *IEEE Communications magazine*, 33(1):58–67, January 1995.

[4] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić. Wireless power transfer via strongly coupled magnetic resonances. *science*, 317(5834):83–86, July 2007.

[5] K. S. Myint and Z. Cho. Wireless data communication with frequency hopping spread spectrum (fhss) technique. In *Proc. of the 2nd International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT'10), Bali, Indonesia*, page 463. Informatics Department Petra Christian University, July 2010.

[6] C. Park. Battery charge apparatus for mobile phone, July 2014. KR Patent 20-0472657.

[7] A. Partovi and M. Sears. Power source, charging system, and inductive receiver for mobile devices, May 2011. US Patent 7,948,208.

[8] R. L. Peterson, R. E. Ziemer, and D. E. Borth. *Introduction to spread-spectrum communications*, volume 995. Prentice Hall, 1995.

[9] Y. Yoon, N. Choe, H. Lee, and J. Choi. Technological trends in space solar power. *Current Industrical and Technological Trends in Aerospace*, 7(2):33–39, December 2009.

[10] Z. Zhang, K. Chau, C. Liu, C. Qiu, and F. Lin. An efficient wireless power transfer system with security considerations for electric vehicle applications. *Journal of Applied Physics*, 115(17):17A328, February 2014.

[11] Z. Zhang, K. Chau, C. Qiu, and C. Liu. Energy encryption for wireless power transfer. *IEEE Transactions on Power Electronics*, 30(9):5237–5246, September 2015.

[12] T. Zia and A. Zomaya. Security issues in wireless sensor networks. In *Proc. of the International Conference on Systems and Networks Communications (ICSNC'06), Tahiti, Tahiti*, page 40. IEEE, October-November 2006.

Author Biography

Yangjae Lee received the B.S. degrees in information security from Sejong University, Korea, in 2018. He is currently an M.S. at Graduate school of Sejong Univerity. His research interests include information security, cryptography, embedded machine, and wireless sensor network security.

Dongmin Yang received his B.S., M.S., and Ph.D. degrees in computer science and engineering from the POSTECH, Korea in 2000, 2003, and 2011, respectively. He is currently an Assistant Professor at Graduate School of Archives and Records Management, Chonbuk National University. From September 2011 to September 2017, he was an Assistant Professor at the Department of Electronics, Information Communications Engineering, Daejeon University. From September 2009 to September 2011, he was with Samsung Electronics Company, Korea, as a Senior Engineer. His current research interests include archives information security, IoT, MANET.

Taek-Young Youn received his BS, MS, and Ph.D from Korea University in 2003, 2005, and 2009, respectively. He is currently a senior researcher at Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea. From 2016, he serves as an associate professor in University of Science and Technology (UST), Daejeon, Korea. His research interests include cryptography, information security, authentication, data privacy, and security issues in various communications.

Ki-Woong Park received the BS degree in computer science from Yonsei University in 2005, and the MS and PhD degrees in electrical engineering from KAIST in 2007 and 2012, respectively. He is currently an assistant professor in the Computer and Information Security Department at Sejong University. He worked as a researcher at the National Security Research Institute in 2012. His research interests include system security issues for cloud and mobile computing systems as well as the actual system implementation and subsequent evaluation in a real computing system. He received a 2009-2010 Microsoft Graduate Research Fellowship. He is a member of the IEEE and the ACM.