International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.13-20
http://dx.doi.org/10.14257/ijsia.2016.10.10.02

Evaluation of the Effectiveness of NFC-based Anti-Theft Security System for Motorbike

Taeseok Jin[1]

[1]*Department of Mechatronics Engineering, Dongseo University*
jints@dongseo.ac.kr

Abstract

This paper proposes a method for the immobilization of motorbike brakes in conjunction with near-field communication (NFC) technology in order to meet the increasing demand for security and convenience of motorbike drivers. The immobilizer proposed in this paper improves previous detachable immobilizers based on mechanical locks in order to provide a fundamental solution to theft prevention. By adopting NFC, the system offers user authentication and personalization services in a secure manner. The author presents the principle of operation of the proposed method, and configuration of the immobilization device based on secure authentication.

In this paper, a solenoid valve design is proposed to remotely perform lock/unlock operation with the aid of the motorbike immobilizer and information security system. The author presents the NFC secure authentication method for unlocking the immobilizer upon identifying the mobile terminal of the user, the method of automatic or manual control of the brake fluid pressure of a stopped motorbike, and the experimental mechanical prototyping results.

Keywords*: Near-Field Communication, Security, Lock system, ECU, Solenoid*

1. Introduction

Because of the recent increase in the number of high-end fuel-based or electric motorbikes, numerous systems for security and convenience are being developed and supplied to the market, following a similar trend in cars. In particular, in the case of motorbikes, numerous cases of theft have been reported both in South Korea and the rest of the world. Most cases of theft involve physically unlocking the handle lock and subsequently dragging the motorbike away, whereas in some cases, the stolen motorbike is loaded onto another vehicle. Therefore, devising a solution is of immediate need, particularly one that fundamentally disables theft by immobilizing the motorbike. Although the demand for a security system to prevent motorbike theft is increasing worldwide, the current implementation of anti-theft lock is merely a fixed mechanical device that only offers physical immobilization. In this regard, the author proposes an anti-theft system that fundamentally prevents such physical dismantling or separation, and a lock/unlock system that employs Internet of Things (IoT)-based wireless authentication.

In order to realize the lock/unlock of an electronic lock based on near-field communication (NFC) technology. The author equipped a keyless entry system that is increasing in use as part of IoT technology. NFC technology is growing in functionality because its equipment is commonly found in smartphones, and various NFC services are now offered in conjunction with credit, mileage, and gift cards through mobile service providers. There is a general increasing trend in the number of commercial products with such security and authentication functionality. In particular, NXP (www.nxp.com), a German semiconductor company, developed “smart keys” by adopting NFC technology in car keys. Continental, a car electronics manufacturer, presented a concept car during

ISSN: 1738-9976 IJSIA

MWC 2011 that is equipped with a keyless entry system based on the NFC technology of NXP. This concept car presented numerous functionalities, including unlocking doors upon contact of a user's NFC-enabled smartphone with the car door, and a personalized greeting and seat adjustment functionality resulting from an active authentication cycle between the security chip of the smartphone and car.

Figure 1. Concept for Application of NFC in Anti-theft Systems

2. Anti-theft System

2.1. System Configuration

In this paper, the author develops a motorbike immobilization and information security system that allows fundamental theft prevention, and offers user authentication and personalization through NFC. The system configuration developed in this paper is represented as shown in Figure 1. In order to establish both user-friendliness and security, the system consists of the motorbike data collection and electronic control unit (ECU) module, immobilizer module with brake fluid pressure control ability, a smartphone application (APP) for motorbike data management and personalization, and NFC interface authentication module.

Each system component performs the functions described in this paragraph. The motorbike immobilization module is equipped with: 1) a mobile electronic key that receives the user authentication information and system configuration commands through wireless communication at both near (within 10 meters) and far (within 100 meters) fields; 2) a user authentication controller that identifies the user from the authentication information received by the mobile electronic key; and 3) a solenoid that interacts with the brake line of the motorbike in order to control the brake fluid pressure and brake pad operation. Here, the brake pad engagement is actuated by the brake fluid pressure, whereby the use of solenoid allows the control of this brake fluid pressure.

In this implementation, the commercial off-the-shelf (COTS) solenoid, HDA021S, is adopted. The principle of operation is that when 12 V are applied to the solenoid, it generates a magnetic field that imposes an attractive force to the metal door of the valve, thus opening and closing the valve electronically. The use of a solenoid valve is also seen in bus doors, which is actuated by the control of compressed air, and the automatic lock on hot and cold water taps of water dispensers.

2.2. System Operation

The system is implemented based on a model of the motorbike immobilization mechanism and a brake applied to the motorbike in the parking state. The author designed an RF and LF wireless communication circuit and microcontroller-based control

circuit to electronically control the parking brake, and conducted experiments on these circuits. Printed circuit boards (PCB) are designed and manufactured based on the specifications established during the housing design phase. Basic controls operations are performed using AVR and Arduino microcontrollers operated as the device driver for each module. Using the front or rear brake during the parking mode of the motorbike, the motorbike brake fluid pressure can be controlled in order to prevent turning the wheel.

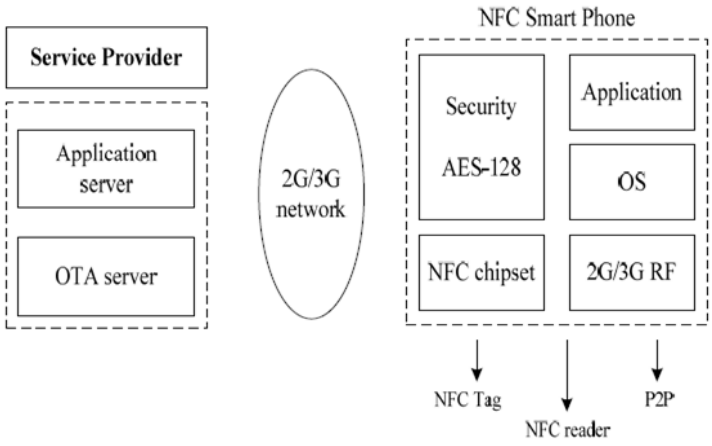

Figure 2. Configuration Diagram for NFC Secure Authentication

Figure 2 shows the control unit for this system action to be executed based on the signal received related to the motorbike state. Here, the immobilizer control unit is connected to the actuator control unit that controls the actuator equipped in the motorbike brake line, based on the signals from the user authentication unit, ECU, and wired communication unit that transmits and receives the control and state signals. Moreover, by actuating the lock/unlock state of the brake line through NFC authentication, motorbike operation is prevented, unless the control unit approves user authentication.

Furthermore, if the ECU receives authentication information that is different from that stored, this is regarded as an attempt of theft, and thus the brake pad is actuated and motorbike operation is prevented. Meanwhile, the immobilization unit selectively locks or unlocks the motorbike wheels, based on the commands from the ECU.

3. NFC Authentication and Encryption

3.1. NFC Security

Because the advanced encryption standard (AES) is already available as an encryption standard for NFC, based on the information accumulated from RFID and IC card technology, AES was adopted as the encryption standard for the wireless key of the motorbike immobilization device. This standard is an encryption algorithm used for military security maintenance application, especially for sensitive, but non-classified, information. Because of it, it is widely used in commercial applications within the civil domain, and it is understood as the de facto standard.

In the proposed immobilization device, NFC is adopted as the key to be employed by users to approve unlocking the immobilizer. As a result, not only is it possible to safely exchange user personal information, but the need to carry previous immobilization devices, such as locks and keys, are removed.

3.2. Encryption Algorithm

NFC wireless communication, used here as the wireless key for the immobilization device, is an asymmetric encryption algorithm used in various encryption packages. AES-128, used in NFC, is defined in the ISO/IEC 18033-3 standard. Furthermore, AES is the first algorithm to be publicly available that is also approved by the US National Security Agency for use in top-secret applications. Furthermore, the AES algorithm specified by FIPS-197 fixes the input plaintext at 128 bits in length, but allows a cipher text length choice of 128, 192, and 256 bits. For application as a wireless key for motorbikes, encryption is designed such that it is safe from all known cryptanalysis methods for block ciphers, and it is efficient in terms of speed and code compactness comparable to smart cards during hardware or software implementation. Furthermore, the design considers the appropriateness of interfacing with NFC network environments with authentication features.

The authentication functionality is fortified by combining the hash functions MAC and MDC in the algorithm. Although the AES encryption algorithm is followed, the predictable input-output relationship in the hash functions is avoided in order to enhance authentication performance and integrity. Moreover, an AES-128 algorithm with simultaneous use of MAC and MDC with blocked handshake method is adopted for application in N:1, 1:N, and N:N network environments.

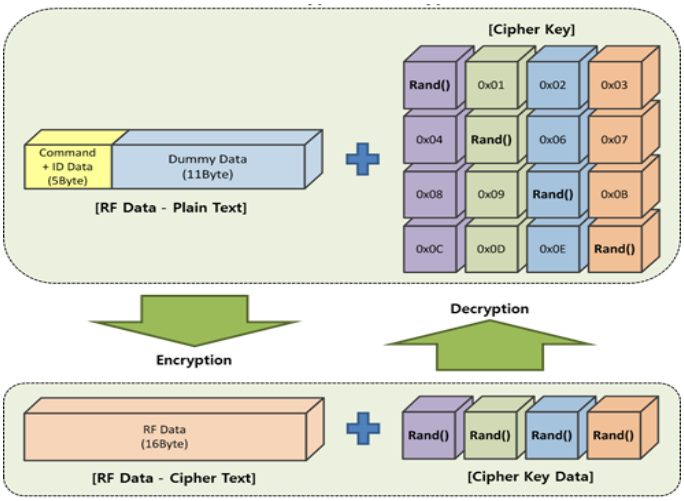

Figure 3. System Encryption Algorithm

The adopted AES encryption consists of dividing the plaintext into units of 128-bit length, encryption, and decryption. Calculations are performed by representing each unit of 128 bits as 4×4 matrices. As shown in Figure 3, the intermediate results of the encryption and decryption process, represented by 4×4 matrices, are referred to as states, and each 32-bit column of matrices forms a word. In AES, computation is performed in byte units, and each byte is represented as a polynomial over the finite field GF (29). Furthermore, the AES encryption and decryption processes consist of byte-wise addition and multiplication. Moreover, byte-wise addition during the AES encryption and decryption processes refers to the bit-wise XOR operation. Byte-wise multiplication refers to multiplication over modulo-8 irreducible polynomials.

The confusion that exists among immobilization devices and external cryptanalysis attempts is prevented by an encryption modeling process. The system is configured such that important information, including user ID, is transmitted through RF data; then, POB is transmitted through RF data following encryption through use of AES-128, and ECU decrypts the RF data and processes the decrypted information.

The encryption code is structured in the form of CMD (1 byte) + ID (4 bytes) + Dummy (11 bytes), such that a total of 16 bytes of data generate 16 bytes of encrypted data based on a 16-byte cipher key.

4. Experiment and Results

4.1. Control Processor

Figure 4 shows the overall flowchart for inspection of the NFC immobilization device and the control method used in the experimental prototype. As seen in Figure 4, the prototype is inspected according to the steps described in the paragraphs that follow Figure 4 in order to test ECU.

First, EOT PBA or CASING inside the connector is connected. From the TEST list on the monitor, EOT PBA or CASING is selected, and power is supplied. Second, the vibration sensor and LF transmitter are tested under the vibration that occurs from the attempt of forced disassembly. A test is configured such that the vibration sensor is activated by touching the EOT board, and operation of the Ref. FOB within the shield box can be visually confirmed through an LED. Third, in order to test RF reception, Ref. FOB transmits the RF signal S/G to S/TY, and S/TY is transmitted to TEST E(3) following the modulation. TEST ECU confirms that an accurate RF signal is received.

Figure 5 shows the strength of the RF wave with respect to the distance between the tag and reader. As a mean of authentication with security requirement, we can see that identification occurs linearly within a range of 0.8 m.

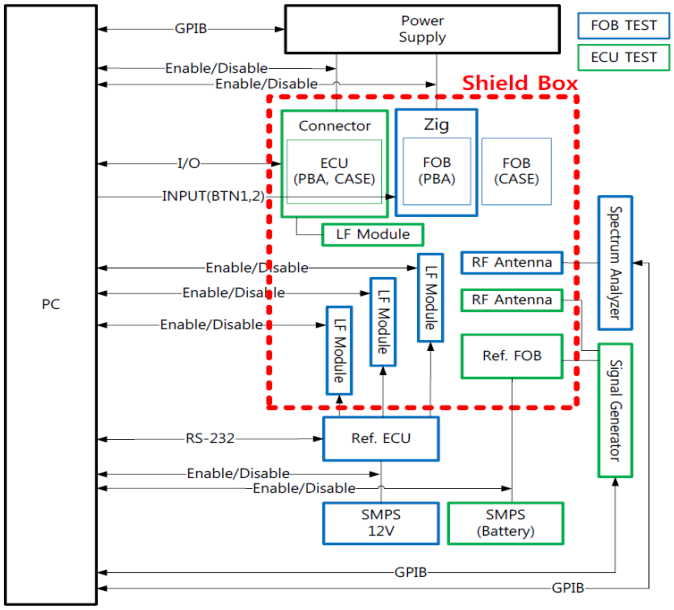

Figure 4. Flowchart for Inspection of Motorbike Immobilizer

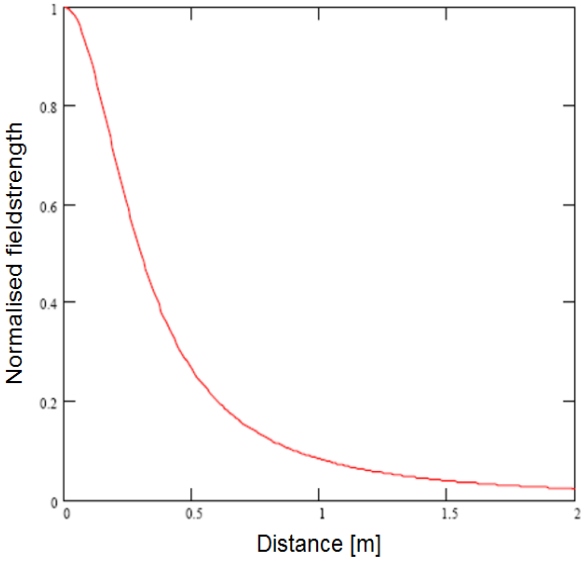

Figure 5. RF Wave Strength with Respect to Distance

4.2. Implementation and Testing

Figure 6 shows the equipped controller for implementation test using the final experimental prototype. In this figure, we can see the solenoid that controls the flow through the fluid pressure hose that connects the brake lever and disk, the equipped ECU for the external NFC communication and authentication, and the wiring of various control signal lines.

Figure 6. Performance and Implementation Test

5. Conclusion

This paper presented the results of system manufacture of a motorbike immobilization and information security system with NFC-based user authentication ability in order to provide a fundamental motorbike anti-theft solution and improve previous detachable mechanical lock-type immobilizers. The information security system for the immobilization of motorbikes was introduced during the technology realization process, and NFC communication and encryption methods were proposed for unlocking the immobilizer. Moreover, the author presented the principle of operation, circuitry, and manufactured prototype of the brake fluid pressure controller to actualize the motorbike immobilizer.

Acknowledgements

This research was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2015 (Grants No. C0273252).

References

[1] W. Rhodes and R. Kling, "Evaluation of the Effectiveness of Automobile Parts Marking and Anti-Theft Devices on Preventing Theft", Abt. Associates, Inc, **(2003)**, pp. 1-44.
[2] K. Lemke, A. R. Sadeghi and C. Stüble, "An Open Approach for Designing Secure Electronic Immobilizers", Horst Görtz Institute, Ruhr-Universität Bochum, Germany **(2005)**, pp. 230-242.
[3] Y. I. Cho, "Development of Digital Menu Plate linking with POS System using NFC installed Smart Phone", Korean Institute of Intelligent Systems, Proceedings of KIIS Fall Conference, vol. 24, no. 1, **(2014)**, pp. 147-148.
[4] I. T. Lim, "Optimal Parameter Selection of Q-Algorithm in EPC global Gen-2 RFID System", Journal of information and communication convergence engineering, vol. 7, no. 4, **(2009)**, pp. 469-474.
[5] S. Kasuya, T. Taniguchi, K. Tsukamoto, M. Hayabuchi, M. Nishida and A. Suzuki, "AISIN AW New High Torque Capacity Six-Speed Automatic Transmission for FWD Vehicles", SAE Paper 2005-01-1020, **(2005)**.
[6] D. Y. Im, H. R. Cha, I. H. Oh and C. S. Kang, "Development of Valve Controller using Wireless Communication", Proceeding of korean Institute of Intelligent Systems, vol. 19, no. 2, **(2009)**, pp. 271-272.
[7] J. S. Kim, "Hierarchical Private Credit Assessments based on FCM Inference", Proceeding of korean Institute of Intelligent Systems, vol. 22, no. 1, **(2012)**, pp. 285-288.
[8] S. Kasuya, T. Taniguchi, K. Tsukamoto, M. Hayabuchi, M. Nishida and A. Suzuki, Aisin AW Co., Ltd. AISIN AW New High Torque Capacity Six-Speed Automatic Transmission for FWD Vehicles. SAE Paper 2005-01-1020, **(2005)**.
[9] NFC Forum (What is NFC?). http://www.nfc-forum.org/aboutnfc/
[10] Zigbee Alliance (Understanding ZigBee). http://www.zigbee.org/About/ UnderstandingZigBee.aspx

Authors

Prof. Tae-Seok Jin, he received his Ph.D. degrees from Pusan National University, Busan, Korea, in 2003, in electronics engineering.

He is currently an associate professor at Dongseo University. From 2004 to 2005, he was a Postdoctoral Researcher at the Institute of Industrial Science, The University of Tokyo, Japan. His research interests include network sensors fusion, mobile robots, computer vision, and intelligent control. Dr. Jin is a Member of the KIIS, KIEE, ICROS, and JRS.

