Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 7 pp. 325-330, 2017

https://doi.org/10.5762/KAIS.2017.18.7.325
ISSN 1975-4701 / eISSN 2288-4688

블루투스 4.0 기술을 이용한 차량용 보안인증 시스템 설계

유환신
호원대학교 자동차기계공학과

Design of Vehicle Security Authentication System Using Bluetooth 4.0 Technology

Hwan-Shin Yu
Department of Automotive Mechanical Engineering, Howon University

요 약 블루투스 4.0은 다양한 기기간의 통신에 활용되어 사물 인터넷에 적합한 기술이다. 자동차와 접목하여 서비스를 창출에 적합하다. 본 논문에서는 사물 인터넷 서비스의 구현 사례로, 블루투스 4.0 기술과 차량용 시스템을 연계하여 보안 인증 체계를 설계한다. 보안 인증을 위한 절차를 설계하고, 데이터 서버를 활용한 인증 방법을 제안한다. 보안 인증 기능을 제공시, 위험 알림, 사용자 행동 이력에 대한 정보 수집 기능을 활용하여 다양한 부가 서비스를 창출할 수 있다. 또한 블루투스 기술과 기술의 표준화 및 발전 과정에서 소비전력을 낮춘 저전력 상에서 통신이 가능하고 접근성을 높인 무선통신 기술인 BLE(Bluetooth Low Energy) 기술을 접목하여 RFID 또는 NFC 방식을 활용하여 배터리 수명을 개선하고 인식 가능한 범위를 확장하였다. 비접촉식으로 인증 가능한 범위를 확장되어 보안 서비스를 확대할 수 있다. 본 논문에서 제안한 시스템을 활용하면 기존 무선 주파수(Radio Frequency) 기반 시스템의 문제점과 휴대성 및 배터리 사용 문제를 극복하면서, 맞춤형 서비스를 제공할 수 있다.

Abstract Bluetooth 4.0 is a technology suitable for the Internet of things that is used for communication between various devices. This technologyis suitable for developing aservice by combining with automobiles. In this study, a security authentication system was designed by linking Bluetooth 4.0 technology and a vehicle system as an implementation example of an object internet service. A procedure was designed for security authentication and an authentication method is proposed using a data server. When the security authentication function is provided, various additional services can be developedusing the information collection function of the risk notification and user action history. In addition, BLE (Bluetooth Low Energy) technology, which is a wireless communication technology that enables low-power communication and low-power communication in the process of the standardization and development of Bluetooth technology and technology, improves the battery life through the use ofRFID or NFC This studyexpanded the range possible. The security service can be extended by expanding the scope of authentication by the contactless type. Using the proposed system, a customized service can be provided while overcoming the problems of an existing radio frequency (RF)-based system, portability, and battery usage problem.

Keywords : Automotive, algorithm, bluetooth, embedded system, security

1. 서론

근래에 차량은 다양한 IT기기들을 장착하며, 지능화되고 첨단화되고 있다. 엔진과 관련된 제어, 운전자 편의 사양, 네비게이션 및 엔터테인먼트 시스템, 어라운드 뷰 모니터링 시스템[1] 그리고 차량용 블랙박스 및 주행보

본 논문은 2017년도 호원대학교 교내학술연구비의 지원에 의해 수행되었음.
*Corresponding Author : Hwan-Shin Yu(Howon Univ.)
Tel: +82-61-450-7110 email: hsyu@howon.ac.kr
Received May 23, 2017 Revised June 27, 2017
Accepted July 7, 2017 Published July 31, 2017

조 장치까지 그 분야도 다양하다. IT관련 기기들이 다양한 관심을 가지고 있는 이유는 그만큼 인간의 생활에 꼭 필요하기 때문이다. 이와 관련하여 IT기기를 지원하는 범위가 늘어나고, 통신서비스와의 연동이 늘어나면서, 다양한 형태의 보안 및 유지보수 관리가 필요하게 되었다. 엔진이나 운행과 관련된 제어장치의 해킹 방지 기술, 운전자를 인식하여 운행기록을 하는 기술 들이며, 이 기술들은 통신기술의 발달과 더불어 보안을 유지하고 관리해야 한다.

특히 운전자를 인식하고 관리하는 기술은 다양한 형태의 차량에 반드시 접목되어야 하는 기술이 되고 있다. 현재는 RFID 또는 NFC 유사한 형태의 스마트 키 시스템을 사용하여, 차량의 스마트 키 기술을 지원하고 있으나, 그 인식거리는 매우 짧고 사용이 제한적이다. IOT 기술 구현을 위해 대표적으로 사용되는 블루투스 비콘 기능을 활용하여, 원거리에서도 효율적으로 차량의 운전자를 인식하고, 보안 인증 및 안전한 작동을 시킬 수 있는 시스템의 설계 및 개발이 필요하다. 본 논문에서 이 시스템의 설계 및 구현 방향을 제시하고자 한다.

본 논문의 구성을 다음과 같다. 2장은 관련연구로 설계 시스템의 필요성과 중요성에 대하여 논하고 설계 시스템의 대표적인 응용 사례에 대해 기술한다. 또한 최근의 최근 시스템 동향을 살펴본다. 3장에서는 본 논문에서 제안하는 인증 알고리즘 모델에 대해 자세하게 기술하며, 임베디드 시스템의 설계를 제안한다. 4장에서는 설계된 시스템들을 임베디드 환경에서 실시한 성능 평가에 대해 논한다. 5장에서는 본 연구가 갖는 한계점 및 향후 연구에 대한 결론을 기술한다.

2. 본론

2.1 차량용 임베디드 시스템

차량에 장착되는 보조 장치로는 차량용 블랙박스, 어라운드 뷰 모니터링 시스템, 추돌방지 시스템 등과 함께 운전 중에 자주 활용되는 시스템이다. 차량용 블랙박스의 경우[2], 24시간 녹화를 하며, 운행 또는 주차 중에 계속해서 영상을 기록하고, 필요시에 여러 가지 증거 자료로써 활용된다. 또한 주행 중에는 녹화되는 영상을 활용하여 차선을 인식하여 운전 중 위험상황을 알려주는 기능[3]까지 추가되었다. 그러나 사용자의 운행기록 또는 출입 통제를 위한 시스템은 각각의 단말기를 별도로 연동하여 Fig. 1과 같이 모듈을 각각 장착하여 연결한다.

이와 같은 구성은 장치가 많고, 모뎀, NFC(RFID)태그, GPS 등의 부속이 장치별로 불량이 발생하거나, 하나의 장비 연결이라도 훼손될 경우, 시스템의 운영에 지장을 초래한다. 또한 많은 단말장치를 운영함으로써, 차량의 배터리 방전에 대한 위험성도 있다. RFID는 복사되기가 쉽기 때문에, 개인정보의 유출과 도용이 우려된다. 인식기능을 위한 RFID와 보안 인증을 위한 통신모듈을 블랙박스 시스템과 결합하여 차량의 보안과 인증을 담당하는 통합 시스템으로 설계할 필요성이 있다.

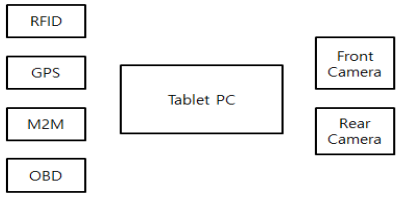

Fig. 1. Merging embedded system

2.2 BLE 시스템

블루투스 4.0 기술은 안드로이드 스마트 폰과 아이폰 등 최신의 스마트폰에서 사용이 가능하다. 프린터, PC, 스마트 폰, 가전제품 등을 쉽게 연동할 수 있는 장점이 있어 보급이 확산되고 있다[4]. 또한 기술의 표준화 및 발전 과정에서 소비전력을 낮춘 저전력 상에서 통신이 가능하고 접근성을 높인 무선통신 기술인 BLE(Bluetooth Low Energy) 기술을 포함한다. 동전 모양의 CR2032 코인 배터리로 장시간 사용할 수 있을 정도로 사용성이 우수하다.

Table 1. Comparison of NTC(RFID) and BLE

Spec.	NFC	BLE
Communication	RFID	Bluetooth (BLE)
System	using NFC module	using Bluetooth 4.0 module
Maximum distance	10cm	50m
Indoor offset	Not Available	Available
Duplex	Duplex (Payment Information)	Duplex (New Standard)

기존의 스마트키 시스템은 RFID 방식의 이모빌라이저 키 방식을 기반으로 한다. Table. 1을 살펴보면, NFC(RFID) 방식은 거리제약과 전용 RX-TX 부품을 가지며, 근거리에서만 인식이 가능한 단점이 있다. 최근의 스마트키 시스템은 Bluetooth 4.0 기반의 통신을 활용하여 차량의 다양한 정보를 송수신 한다. 본 시스템은 차량과 결합하영 활용하는 서비스가 가능한 시스템을 설계해야 하며, 50m까지 도달이 가능한 BLE를 활용하여, 차량의 인증을 보다 원거리에서부터 실현할 수 있는 기술적 이점이 있으며, 정교한 위치 파악이 가능한 기술[5]을 활용하여, 인증 장치를 추적하여 차량의 운행과 관련된 보안 기능을 향상시킬 수 있다.

2.3 보안 인증 알고리즘

BLE 통신을 이용한 통신은 페어링을 하지 않는다. 따라서 통신 연결 범위안의 다수의 디바이스 간의 데이터 통신이 가능하다. 이와 관련 통신 프로토콜을 분석하여 해킹하는 사고가 발생할 수 있기 때문에 보안 인증하는 방법이 필요하다. 대응하는 기술로써 OTP(One Time Password) 방식[6]의 기법이 제안되었다. 인증코드와 암호가 지속적으로 바뀌게 되어 해킹으로부터 보안이 강화될 수 있다. 본 논문에서 설계 및 제안하는 단말장치에 보안을 위해 사용하기 적합한 인증 절차이다. 보안 인증을 한 결과 데이터는 서버에 DB로 암호화 하여 저장한다. 비콘 기반의 버스 자동 승하차 시스템 구현 사례[7]에서 볼 수 있듯이 태그가 필요 없는 사용이 편리한 시스템이 될 수 있다.

3. 시스템 설계 및 구현

3.1 서비스 구성 설계

기존의 접촉식 RFID기반의 무선태그는 보안 취약성이 있으며, 정교한 위치 파악이 불가능하다. 본 논문에서 제안하고자 하는 시스템은 비접촉식으로 보안 인증 알고리즘이 구현 된 단말장치이다. 또한 인증과정이 접촉지점까지 도달하기 전에 이루어지기 때문에 편리성이 있다. 이러한 단말 장치는 공유 차량을 사용하는 렌터카, 법인 차량, 버스, 화물차 등에서 유용하게 사용이 가능하다.

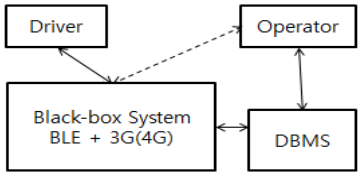

Fig. 2. Integration of control system of embedded system

Fig. 2의 제어 설계와 같이, 운전자는 블랙박스 시스템과 통신을 하고, 블랙박스 시스템은 모바일 무선 인터넷 망을 이용하여, 관제 서버에 인증 정보를 통지한다. 개인 운전자 시스템의 경우는 관리자가 본인이 되어, 차량을 인증한 결과를 확보하게 되며, 관리가 필요한 차량의 경우, 관리자가 인증된 정보를 취합하여 관리하게 서비스를 설계한다.

3.2 시스템 구성 설계

차량용 블랙박스 시스템은 영상의 처리와 데이터의 저장[8]이 중요한 기능이다. 이에 시스템의 자원의 대부분을 소모한다. CPU가 통신 모듈을 별도의 프로세싱 블록으로 가져갈 경우, 통신을 위한 통신을 수행하게 되어 시스템의 부하가 발생하게 된다. 이에 Fig. 3과 같이 CPU core에 BLE 모듈과 3G(4G)모듈을 직접 연결하여 시스템을 구성한다.

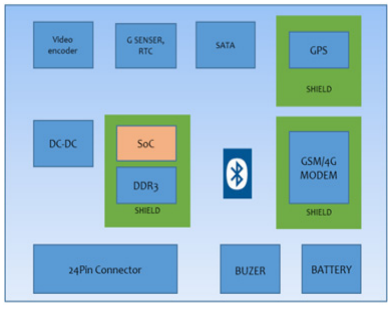

Fig. 3. Embedded system design proposal

제안한 시스템의 설계 구성은 Fig. 4와 같이 PCB를 실제로 구성하여, 블랙박스 시스템으로 디자인 한다. 차량용 블랙박스 시스템으로 구성하고 보안 인증 기능의 결합을 통해 단말 장치의 은폐성이 요구되어, 카메라와 GPS등은 외부로 나올 수 있는 소형 시스템으로 설계한다.

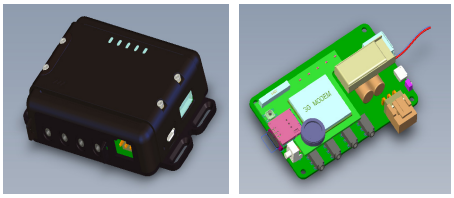

Fig. 4. Embedded system rendering

Table 2. Design basis of H/W

Item	Spec.	Unit
VDD	-0.3~+4.8	V
DEC2	~2	V
Storage Temperature	-40~+125	℃
ESD HBM	~4	kV
ESD CDM	~750	V
MSL	2	-
Endurance	~20000	Write/Erase Cycle
Number of times address can be written between erase cycles	~2	-
Detection Time	~3	Second

3.3 시스템 하드웨어 설계

Table. 2는 설계하고자 하는 하드웨어 시스템의 제원이다. 전원은 차량의 시스템이 12V와 24V를 사용하는데, 시스템의 동작 안정성을 위해 48V를 사용한다. 고온과 저온(-40℃~+125℃)에서의 AEC-Q100과 ISO 26262를 지원하는 오류방지 조건에서 동작[9]하도록 설계해야 한다. 사용 중에 시스템의 불량을 막기 위해서, ESD 보호규격을 내장한다. 또한, 보안 인증 USER 데이터의 기록과 보호를 위해, 암호화 영역의 Storage 내구성도 20,000회 이상 유지되도록 한다.

Table 3. Design basis of BLE

Item	Spec.	Unit
Maximum output power	~4	dBm
RF power control range	20~24	dB
RF power accuracy	±4	dB
20dB bandwidth for modulated carrier (2Mbps)	1800~2000	HKz
2nd Adjacent Channel Transmit Power. ±4MHz (2Mbps)	~-45	dBC
Maximum consecutive transmission time, ftol < ±30ppm.	~16	ms
Sensitivity (0.1% BER) at 2Mbps.	~-85	dBm
C/I co-channel	~12	dB
IMD performance, 2Mbps, 3rd, 4th, and 5th offset channel	~-41	dBm
Detection Distance	50	Meter

Table. 3은 보안 인증을 위해서 적용되어야 하는 BLE의 설계 제원이다. 외부에 별도의 안테나 설계 없이, 내장 RF설계가 이루어져야 한다. 보안 인증의 시작이 50m에서부터 시작하도록 시스템이 설계되어야 보안 인증 기능이 원활하게 동작할 수 있다.

3.4 인증 알고리즘 설계

운전자를 인식하기 위해서 운전자의 스마트 폰 또는 BLE 전용 단말기를 사용할 있다. 사용자의 보안 인증 정책상 주기적으로 암호화 데이터를 업데이트해야 하기 때문에, 스마트 폰을 기준으로 인증 알고리즘을 설계한다. Fig. 5와 같이 시스템을 연동하게 된다. 연동과정에서 BLE 데이터는 시간동기화를 기준으로 OTP방식을 적용하여, 단말기와 운전자가 인증되도록 한다.

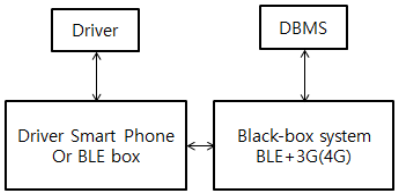

Fig. 5. Authentication design using smart-phone

Fig. 6의 인증을 위한 절차는 다음과 같다. (1)서버 또는 관리자는 차량에 대한 인가정보를 운전자에게 통지한다. (2)운전자는 스마트폰 또는 BLE인증 단말기에 관리자로부터 부여받은 인증 암호화 값을 저장한다. (3)운전자 인증정보가 포함된 단말장치가 블랙박스 시스템에 접촉되면 모바일 통신을 시작한다. (4)모바일 통신을 통해서, DBMS의 KEY값을 가져온다. (5)차량의 내부에 탑승 전까지 인증여부를 확인하여, 인증 성공 시, DBMS는 운전자에게 차량인증 성공에 대한 알림 문자를 전송한다. (6)인증 실패 또는 인증 전 운행 시도 시, 관리자와 인가된 운전자에게 경보를 전송한다.

보안인증 시 사용하는 BLE의 거리 추적기능을 활용하기 위해서, 설계된 시스템은 Fig. 7과 같이 배치되어야 (1)운전석 내부의 가용거리를 측정할 수 있으며, (2) 운전자가 인증을 시작할 수 있는 거리의 기준을 잡을 수 있다. 거리를 측정하는 방법은 3변 측량법을 적용하는 것이 유리하나, 제안된 시스템은 한 대의 차량을 기준으로 측량해야 하기 때문에, BLE 인증 단말장치와 운전자 단말장치의 RSSI 강도를 측정하여, 70m에서부터 1m단

위로 측정한다. 통계적 기법으로 운전자 단말장치의 접근거리를 계수화 한다.

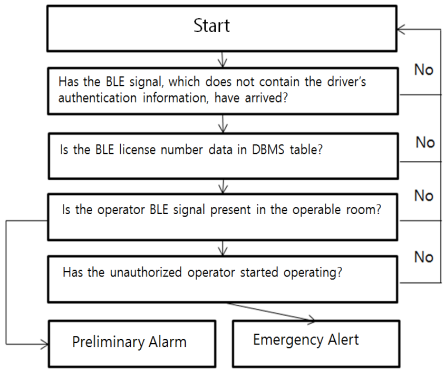

Fig. 6. Algorithm for BLE Authentication and Warning

다수의 차량을 관리하는 서비스 제공자 또는 차량이 밀집된 주차장에서는 의도치 않은 오류가 발생할 수 있다. 경보 처리의 제한 조건을 구체화하여 판단할 필요가 있다. 사전 알람 단계에서는 BLE 인증이 시도되는 단말장치가 발견되었고, 거리가 지속적으로 가까워질 때, 사람 또는 차량이 접근하는 것으로 판단할 수 있다. 이때 보안 인증 장치에서 블랙박스 또는 관리 시스템에 예보를 보내 상황을 모니터링 할 필요성을 판단할 수 있다. 경보 알람 단계에서는 인증이 완료되지 않은 상황에서, 차량의 문이 개폐될 때, 긴급 경보를 진행시킬 수 있다.

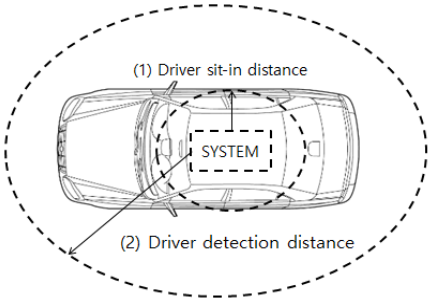

Fig. 7. Layout of system for BLE distance measurement

4. 구현 성능 평가

제안된 방식을 이용할 경우, 인증이 시작되어, 운전자가 인식되지 전까지 극소의 전력과 시스템 자원을 사용하게 된다. 이에 따라 주차 중 차량용 배터리를 최소로 사용하며, 경보를 전송하거나 인증을 진행할 때에 모뎀을 활성화하기 때문에 차량용 블랙박스 기능에 더해 배터리 부하를 최소화 한다.

Table 4. Designed terminal device function evaluation

Item	Result		Test way
	Hybrid System	Black-box System	
Power Consumption	~360Hour	6~12Hour	Using DC12V Vehicle Battery
User Authorization Speed	~5sec	5~10sec	After authorization, server certificated
User Authorization Distance	~50m	~5cm	Authorization Distance per 1m

Table. 4와 같이 설계한 시스템의 구성을 측정한 결과 차량용 블랙박스와 인증장치로 구성되는 기존의 단말장치 시스템의 경우 시동이 걸리지 않은 상태에서 6~12시간 녹화 후 시스템이 종료되나, 영상녹화기능 제외한 본 단말의 경우 충분한 대기 시간을 보여준다. 또한 사용자 인증을 시작한 이후, 모뎀을 연결하여 서버 인증하는데 걸리는 시간은 5초 내외이다. 또한 기존의 구성은 RFID 인증 방식을 사용하여 태그에 접촉했을 때, 인증을 시작하지만, 제안한 시스템은 차량에 다가가면서 인증이 시작된다.

5. 결론 및 향후 과제

차량의 내부에 배터리는 유한하기 때문에, 최소의 전력으로 시스템 및 차량이 대기하고 있어야 하기 때문에, 추가적으로 전력 소비를 줄이는 것이 중요하다. 본 논문의 성능 평과결과 단말장치의 전력 사용의 효율성을 증가하였다. 그리고 사용자 인식 능력도 향상하였다. 이를 기반으로 다양한 서비스의 확장이 가능하다.

차량용 단말장치의 증가와 IoT기술의 활용은 보안 인증기술의 수요를 증가시키고 있다. 이에 다양한 기술과 기법이 도입되고 있는 상황이다.

본 논문에서는 차량용 블랙박스 시스템을 활용하여, 보안 인증기술을 추가하여 시스템의 동작을 확장 발전시키는 방법에 대한 설계 방법을 제안 한다.그러나 제안 시스템에서 적용된 거리 측정기법이 최적화 되지 않았다는 점에서 본 연구의 한계를 찾을 수 있다. 따라서 이를 극복하기 위한 연구를 본 논문의 향후 과제로 한다.

References

[1] H. S. Yu and E. B. Jeoung, "The Lane Recognition Enhancement Algorithms of Around View Monitoring System Based on Automotive Black Boxes", *Journal of KIIT*, vol. 13, no. 10, pp. 9-15, Sep. 2015.
DOI: https://doi.org/10.14801/jkiit.2015.13.10.9

[2] H. S. Yu, E. B. Jeoung, "The optimized file system designed for vehicle black box system", *Journal of KIIT*, vol. 14, no. 2, pp. 1-6, Feb. 2016.
DOI: https://doi.org/10.14801/jkiit.2016.14.2.1

[3] H. S. Yu, E. B. Jeoung, "The lane departure warning algorithm optimized for automotive black-boxes and compact system", *Journal of KIIT*, vol. 13, no. 10, pp. 9-15, Oct. 2015.
DOI: https://doi.org/10.14801/jkiit.2015.13.10.9

[4] H. S. Kim, "Design of tour guide system using Bluetooth 4.0 and WiFi sensor technology", *Journal of Korea academia-Industrial cooperation Society*, vol. 16 no. 10, pp. 6888-6894, 2015.
DOI: http://dx.doi.org/10.5762/KAIS.2015.16.10.6888

[5] J. W. Son, K. R. Cho, B. K. Jang, "Beacon-Management scheme using the moving route", *Proceedings of KIISE*, pp. 379-380, Dec. 2015.

[6] H. H. Jung, D. R. Shin, K. S. Cho, C. S. Num, "BLE-OTP authrization mechanism for iBeacon network security", *Journal of KIISE, vol. 42, no. 8*, pp. 979-989, Aug. 2015.
DOI: https://doi.org/10.5626/JOK.2015.42.8.979

[7] J. H. Kim, S. W. Lee, "The development of automatic boarding and alighting bus system", *Proceedings of KIISE*, pp. 1390-1391, Jun. 2015.

[8] H. S. Yu, "File system recovery and search enhancement algorithm of automotive black-boxes", *Journal of KIIT*, vol. 14, no. 10, pp. 133-140, Oct. 2016.
DOI: https://doi.org/10.14801/jkiit.2016.14.10.133

[9] S. R. Do, H. S. Han, "Establishing of requirement and design development process for assuring quality of automotive semiconductor", *Journal of KIISE*, vol. 41 no. 9, pp. 625-632, Sep. 2014.
DOI: https://doi.org/10.5626/JOK.2014.41.9.625

유 환 신(Hwan-Shin Yu) **[정회원]**

- 1993년 2월 : 동국대학교 전자공학과 전자공학과과 (공학사)
- 2006년 2월 : 국민대학교 자동차전자제어 (공학박사)
- 1993년 10월 ~ 1997년 11월 : (주)기아자동차
- 2006년 3월 ~ 현재 : 호원대학교 자동차기기계공학과 교수

<관심분야>
무인자율차량, 센서시스템, 영상처리