인크립션 트랜스폰더 타입 이모빌라이져 ECU 소프트웨어 개발

최호준 · 임동진
한양대 제어계측공학과

ECU Software Development for Encryption Transponder-type Immobilizer

Ho-Jun Choi · Dong-Jin Lim
Dept. of Control and Instrumentation Engineering Hanyang University

Abstract - Engine immobilizer is the automobile security system which disables the engine if the secrete code in the transponder embedded in the key knob is not in agreement with the code in ECU of the car. There are many types of immobilizer systems, however, the encryption transponder type system is the most secure system due to the code verification method using an encryption method. As an example of the industry-university cooperation, the software development in the system is introduced in this paper.

1. 서 론

Engine immobilizer 는 자동차의 키에서 무선으로 비밀코드를 발생 시키고 이를 자동차내의 컴퓨터에서 확인하여 이 비밀코드가 일치 하였을 경우에만 엔진의 시동이 가능하도록 하는 시스템으로 자동차의 원래 키가 아니면 자동차의 시동이 불가능 하도록 하는 시스템이다. 본고에서는 산학 협동의 사례로서 기존의 immobilize 시스템에 비해서 월등히 높은 보안성을 갖는 encryptio transponder type immobilizer의 ECU software 개 소개하고자 한다. 이 시스템은 일본이나 미국에서는 벌써 상용화되어 자동차보안 장치로써의 역할을 무난히 해내고 있으며, 앞으로 계속적인 발전을 이루어 시장이 확대될 가능성이 다분히 있다고 하겠다. 뿐만 아니라, 자동차를 수출하는 우리나라 입장에서는 이런 기술을 언제까지나 외국에 의존하여 수입만을 거듭한다는 것은 분명 커다란 손해가 아닐 수 없다. 이런 시점에서 시스템을 동작시키는 소프트웨어의 국내 개발이라는 것은 국내기술의 향상과 수출경쟁력 강화라는 측면에서 그 의의가 있다고 하겠다.

Immobilizer에서 key내 transponder 라고 불리우는 은 이전 시스템에서 사용하던 단순한 데이터(비밀번호)의 저장과 송신 및 수신을 넘어 encrytion number를 지고 통신 중에서의 보안성을 유지하게 된다. 여기서 immobilizer control unit과 transponder의 원활한 통 그 신뢰성이 중요하다고 볼 수 있다. 그리고, 기존의 것에 부가적인 항목을 추가하여 새로운 기능을 더하였다. 물론, 이런 시스템도 벌써 외국에서는 사용되고 있는 현실이다. 그런 상황에서 소프트웨어의 개발은 더욱 절실한 것이다.

2. 시스템 구성 및 주요 알고리즘

2.1 시스템 주요 개념과 구성 및 동작

PATS(Passive Anti Theft System)이라고도 불리우 engine immobilizer system을 장착한 차량에 사용되 시동키는 transponder 라고 부르는 ASIC module이 키의 손잡이 부위에 삽입되어 있는 특수하게 제작된 키이다. 키의 손잡이에 삽입된 transponder 라고 하는 ASIC module이 비밀 코드를 가지고 있으며 이 코드를 자동차에 장착된 컴퓨터에 전송하여 삽입된 키가 정당한 키인지 아닌지를 판단하고, 이에 따라 엔진 시동이 가능하게 할 것인가 아닌가를 결정하게 된다. 이 키와 자동차간에는 무선으로 통신이 이루어져야 하므로 키와 통신을 하기 위한 원형의 소형 안테나가 시동키를 삽입하는 부위에 장착되게 된다. 그리고 이 신호는 RF 신호이므로 이 신호를 변환하여 마이크로 컴퓨터에 전송하기 위한 변환 반도체 칩이 있게되고 마이크로 컴퓨터는 이 칩과 통신을 하여 데이타 처리를 하게된다. 그림 1 과 그림 2 는 이 시스템의 개념도와 구성도를 보여준다.

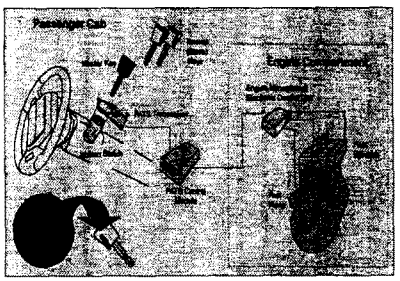

그림 1. Immobilizer system의 개념도

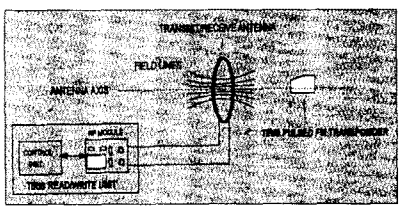

그림 2. Immobilizer system의 구성도

우선, immobilizer의 기본 구성 장치들에 대해 간략 살펴보기로 한다. 이 시스템에 있어서 가장 중요하다고 할 수 있는 장치로는 immobilizer control unit(ICU 있다. 이것의 역할은 transponder와 engine con unit(ECU)과의 통신을 중재하는 것뿐만 아니라, 기타 치들과의 통신을 제어하는 기능을 가지고 있다. transmitter는 RF통신으로 도어를 lock 또는 unlock시는 신호를 보내고 engine control unit(ECU)은 시동는 시동금지를 실행하며 그 외에 ETACS는 transmitt 로부터 받은 신호에 의해 도어를 기계적으로 lock

unlock을 시켜준다. 즉, 키에 삽입된 transponder로부터 받은 신호를 해독하여 engine을 동작시키는 기능과 transmitter로부터 전달된 신호에 의해 도어를 (un)lock시키는 기능을 주동작으로 한다. 여기서, tester는 ICU와 ECU의 상태를 살펴보고 제어할 수 있는 장치로 키를 등록하거나 현재 등록된 키의 상황 등을 모니터링할 수 있고 engine의 상태를 체크하여 시스템 전반적인 조정을 가능하게 한다. code save device(CODE SAV.)는 transmitter을 등록시키는 장치이다. 아래 그림3은 시스템의 간략한 블록도를 나타낸 것이다. 화살표가 단방향인 것은 한 쪽으로만 통신이 가능함을 의미하고 양방향 화살표는 상호간의 통신이 이루어짐을 가리킨다.

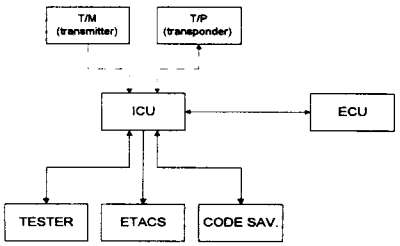

그림 3. 시스템 블록도

현재, 위에서 살펴본 개개의 장치들은 이미 사용하던 기존 제품을 그대로 이용하며 단지, transponder의 기이 기존의 것과는 다른 encryption 기능이 있기에 소프트웨어 상에서 encryption을 해독하는 알고리즘이 추가되었다. 기존 transponder는 단순한 데이터를 송신하 저장하고 비교하는 수준에 그친 반면, encryption 기능을 가진 transponder는 transponder내에 암호코드를 입력 수 있으며 잠금 기능까지 내장되어 있다. 일단 잠금 기능이 이루어진 transponder는 암호코드를 소프트웨어나 하드웨어적으로 변경이 불가능하게 된다. 또한 암호코드가 40비트로 이루어져 있으므로 암호코드를 찾아낸다는 것 자체가 힘든데다가 암호화되어 있으므로 매번 통신 때마다 숫자가 random하게 발생하므로 코드를 해독하기는 불가능하다. 물론, 통신상으로 읽어보는 것 또한 불가능하므로 높은 보안성을 유지한다고 할 수 있겠다. 시동키로서 모두 5개까지 등록 가능하다. ID키는 암호코드를 생성하는 키로서 나머지 4개의 키를 등록시킬 수 있다. 사용자가 4개의 키 중에서 하나를 분실하였을 경우, 서비스센터에서 분실하지 않은 3개의 키와 새로운 키를 ID키나 tester를 이용하여 재등록이 가능하다. 그렇게 되면, 분실된 키로는 더 이상 시동이 불가능하게 된다. 분실에 따른 도난의 방지와 분실하지 않은 키들의 재사용 측면에서 효과적인 방식이다.

2.2 프로그램 주요 알고리즘

2.2.1 Encryption 알고리즘

디지털 시그너쳐 트랜스판더(DST)는 인증 코드(authentication code)나 challenge-reponse 시퀀스 동 트랜스판더에 의해 되돌려진 디지털 신호(digita signature)를 사용하는 보안성을 가지고 있다. 24비트 response를 생성하기 위해 40비트의 challenge와 40비의 key를 사용한다. 여기서 response는 이번 시스템에서의 signature key에 해당하고, challenge는 chall key, key는 encryption key에 해당한다.

*세부적인 내용은 TIRIS 스펙을 참조한다.자세한 내용은 보안상 생략한다.

2.2.2 BCC 알고리즘

트랜스판더와 ICU간의 통신에서 전송오류를 감지하는 기능을 가진 알고리즘으로서 데이터 전송시 BCC를 발생시켜서 identification 코드의 뒷부분에 연결하여 전하게 된다. 따라서 ICU는 이 데이터를 전송 받은 후 BCC를 검토하여 통신상의 오류가 발생하였는지를 체크한다. 실제 시스템에서 많이 사용되는 generato polynomial 로는 CRC-16, CRC-CCITT, CRC-32 있는데, 본 시스템에서는 CRC-CCITT를 사용하고 있다 그림 4 는 BCC 점검 흐름도를 보여준다.

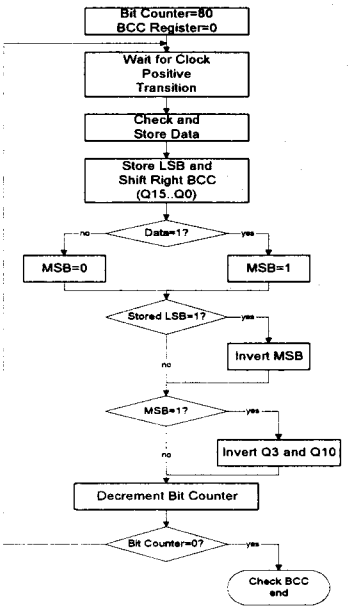

그림 4. BCC 점검 흐름도

Encryption 알고리즘과 같이 이미 안정성과 신뢰성을 인정받은 알고리즘이므로, 스펙에 나온대로 구성을 하여 사용하였다. 역시 자세한 내용은 DST 스펙을 참조한다. 물론, BCC가 오류가 있음에도 0이 되는 경우가 있지만 극히 드물고 오류가 나더라도 등록된 숫자와 맞지 않으면 결국에는 동작을 하지 않으므로, 크게 우려되는 사항은 아니다.

3. 결 론

본 프로젝트로 개발된 자동차용 immobilizer syste 소프트웨어는 유럽 수출차종에 부착될 immobilizer에 들어갈 것으로 98년 상반기에 양산될 전망이다. 수출차에 포함되어 그 신뢰성과 안정성을 인정받는다면, 장래 국내용 차량에도 immobilizer가 의무화되는 때에는 국내용 차량에 부착하는데 크게 문제가 되지 않을 것임에 틀림없다. 그리고, 앞으로 지속적인 기술개발이 따라 준다면 외국기술과 능히 대등하게 나아갈 수 있으리라본다.

key에 관련된 일반제품들에 적용하기에는 경제성이 현재로서는 별로 없어보이지만, 특수용도로는 얼마든지 그 분야가 넓고, 이와 비슷한 형태로 충분히 쓸 수 있다. key가 아닌 card를 이용한 잠금장치가 많은 요즘, RF통신을 이용한 비접촉식 card도 나오고 있다. 이 또한 그

형태가 key가 아닐 뿐이지 RF통신을 이용한다는 점에서는 같은 맥락에서 발전하고 상품화될 것으로 본다.

[참 고 문 헌]

[1] F. Halsall, Data Communications, Computer Networks, Addison Wesley, 1992
[2] 업체기술표준 Immobilizer & Keyless System Spec.
[3] Texas Instruments TIRIS Spec. --DST Algorithm and Software Requirements.
[4] Texas Instruments TIRIS Spec. --Sequence Control Spec. For DST/TMS3791B.
[5] Mitsubishi Microcomputers 7477/7478 Group Spec. & 740 Family Instruction.