CAN 통신과 Smart Device를 이용한 차량 도난 방지 System

김재경* · 황만태** · 김영길***

Car Theft Protection System using CAN Communication and Smart Devicenment

Jae-Kyung Kim* · Man-Tae Hwang** · Young-Kil Kim***

요 약

현재 도난방지를 위해 사용되는 방법은 Key를 이용한 방법, 원격 도어락과 차량 경보를 이용한 방법 등이 있다. 이 방법들은 차량의 Key를 분실할 경우 차량의 도난을 방지함에 있어 어려움이 있다. 그래서 본 논문에서는 Smart Device 와 CAN 통신을 이용한 차량 도난 방지 시스템에 대하여 제안한다. CAN의 차량 식별자 고유ID를 Head Unit에 보내고, Smart Phone을 통해 수신된 식별자 ID를 비교하여 동일한 ID 일 때 차량의 ACC(Accessory)를 on/off 하여 차량의 시동을 걸 수 있다.

ABSTRACT

Smart Device Communications using the development of anti-theft system for vehicles have been investigated. because Progress of Smart Device If someone get the Key for Vehicle theft , he can be easily stolen vehicle. We thought about the concept of dual security devices. Using vehicle's identifier ID of CAN, when Comparing Smat phone identifier ID value and identifier ID received from the Can in the Head, If the same ID is compared. At this point after the activity of the vehicle's ACC On/Off the system allows the vehicle's ignition

키워드

Smart Device, CAN 통신, 도난방지 시스템

Key word

Smart Devicee, CAN Communication, Theft Protection System

* 정회원 : 아주대학교 의용공학과 박사 과정
** 준회원 : 아주대학교 전자공학과 석사 과정
*** 종신회원 : 아주대학교 전자공학과 교수 (교신저자, ykkim@ajou.ac.kr)

접수일자 : 2011. 06. 07
심사완료일자 : 2011. 07. 13

Ⅰ. 서 론

현대와 미래의 전자 산업은 'Ubiquitous'라는 말로 대별할 수 있듯이, 언제나 어디서나 User가 사용하고자 원하는 모든 것을 마음대로 사용할 수 있는 시대가 도래 할 것이다. 이들의 중심에 서있는 대표적인 전자 산업 분야 중 하나로 Car infortainment(information + entertainment) 산업 분야를 예로 들 수 있다. 또한 Smart Phone 사용의 증가로 애플리케이션을 이용한 차량 연동 서비스들이 늘어나고 있는 추세이다.

자동차 부품산업은 지난 5년간 8.3%에 달하는 연강성장률을 보였으며, 전자 부품 산업 분야에서 강력한 성장 동력으로 급부상 하고 있다. 과거 20년 전에는 자동차에 탑재되는 전자장치는 일반적으로 Car Audio/Radio가 전부였다. 이후 전자점화, ECU(Electronic Control Unit), 장금장치 등이 기본 탑재 되면서 자동차는 전자업계의 새로운 '기회의 땅'으로 급부상 하고 있다. 현재 자동차에 탑재되는 전자 장치는 자동차 전체 제조의 22% 이상을 차지하기에 이르렀다. 이와 함께 자동차 내부의 통신 네트워크에 대한 첨단 제어 시스템의 수요가 증가 하고 있다.

차량 통신 네트워크를 검토해 보면 오래전부터 자동차의 배기량, 실시간 동작 및 가격 등 다양한 요구조건으로 인한 설계문제를 해결하기 위해서 여러 가지 새로운 통신 네트워크가 개발되거나 개선돼 있다. 한 대의 자동차에는 요구조건이 다른 여러 가지 동작 분야와 관련된 상응하는 통신 네트워크가 존재한다. 이러한 통신 네트워크는 자동차의 전자장치 간에 필요한 통신을 하는데 가교역할을 한다. 차량용 통신 네트워크의 종류는 다음과 같다.

1) MOST(Media Oriented Systems Transport)

MOST Bus는 오디오, 비디오, 내비게이션 통신 시스템 등 모든 종류의 자동차 멀티미디어 애플리케이션을 위해 BMW와 다임러크라이슬러의 주도 하에 1998년에 개발된 규격이다.

2) FlexRay

FlexRay는 높은 데이터 전송 속도와 함께 매우 우수한 에러 관리가 요구되는 steer-by-wire 시스템이나 break-by-wire 처럼 새로운 X-by-wire 시스템을 위해 1999년 BMW와 다임러크라이슬러의 주도하에 특별히 개발되었다.

3) LIN(Local Interconnect Network)

LIN은 저렴하면서도 복잡하지 않고 더욱 정교한 애플리케이션 요구를 지원하기 위해 개발되었다. LIN규격은 초기 멤버인 BMW, 다임러크라이슬러, 아우디, 볼보, 모토로라, VW, 볼 자동차용 등의 컨소시엄이 정의했다.[1]

4) CAN(Controller Area Network)

CAN은 자동차 내의 각종 계측제어 장비들 간에 디지털시리얼 통신을 제공하기 위하여 1988년 보쉬와 인텔에서 개발한 차량용 네트워크 시스템으로, CAN은 마스터/슬레이브, 다중 마스터(Multiple master), 피어 투 피어(peer to peer)등을 지원하는 매우 유연성이 있는 네트워크이며 공장의 열악한 환경이나 고온, 충격이나 진동, 노이즈가 많은 환경에서도 높은 신뢰성을 제공한다. 이러한 특징을 이용해 차량 도난 방지 시스템을 제안한다.[1],[2],[3]

Ⅱ. 도난 방지 시스템의 연구

도난 사고에 대한 대비를 위해 가장 많이 사용된 방법은 자물쇠와 Key를 사용하는 것이었다. 이 방법은 집, 자동차, 오토바이크 등의 대형 품목부터 가방 등의 소형 제품에 이르기까지 광범위하게 사용 되었으며 발전해 왔다. 전자공학의 발전은 이와 같은 기존의 기계식 잠금-해제 장치들을 전자식 장치로 변환 시키고 있다.

현관문 전자 잠금 장치인 '게이트웨이', 자동차 'RF 리모콘'등이 그 대표적인 예라고 할 수 있다. 이러한 기계적인 잠금-해제 장치 제어 외에 또 다른 도난 방지의 대책으로는, 제품에 대한 사용을 규제제함으로써 도난에 대한 욕구를 억제시키는 방법이 있다. 그 예로 제품에 비밀 번호를 입력해야만 사용가능 하게 하는 방법이 있으며, 컴퓨터 로그인 시 패스워드 입력, 휴대폰 잠금 기능 등이 있다.

이외에도 지문 인식, 동공 인식, 음성 인식, RFID, 감시용 자동차용카메라, 위치추적기 등이 도난 방지용으로 사용되고 있다.

1) 차량(내) 도난 방지

자동차는 그 특성상 가전제품과 같이 고정된 장소에 놓여 있지 않음으로 인해 도난에 쉽게 노출되어 있다. 또한 차량의 Key를 분실 하게 되면 차량의 도난 위험이 더 커진다. 또한 다른 도난 형태로 차량에 대해 전문 지식이 부족한 범죄자들에 대해서는 차량 내의 귀중품 또는 차량 내 고가의 부품들을 도난 하는 것이 가장 일반적인 도난의 형태이다. 이러한 이유로 시장에 판매되는 모든 자동차들은 기본적으로 도난을 보호할 수 있는 장치를 갖추고 있으며 다음과 같은 것들이 있다.

1-1) 차량 잠금장치

가장 오래되고 일반적인 방법으로 Key를 사용하여 차 문을 잠그고 열 수 있는 장치이다. 차량 동작 또한 Key가 있지 않으면 동작 할 수 없는 구조로 설계되어 있다. 그러나 잠금장치 기능은 강력하게 범행을 실행하고자 하는 의지를 갖고 있는 범죄자에게는 큰 장애가 되지 못하는 단점이 있다.

1-2) 차량 경보 기능

일반적으로 차량 경보기는 원격 시동과 원격 도어락 기능을 지원하는 리모콘과 함께 사용된다. 리모콘을 사용하여 문을 잠근 이후에 일반 자동차 열쇠를 사용하여 차량의 문을 열거나 열고자 시도하면 경보기가 울리게 된다. 또는 차량의 충격 여부를 감지하여 경보음이 울리게 함으로써 도난 범죄에 대해 보다 신속히 대처할 수 있도록 돕는다.

1-3) 위치 추적 기능

위치추적기란 일종의 단말기이며 현재까지는 GPS를 이용한 위치 추적기가 가장 많이 사용되고 있다. 최근 들어 지상파를 이용한 단말기 들이 출현하고 있으며, 위치추적 서비스를 통해 실시간으로 현재의 위치를 파악할 수 있다.

Ⅲ. CAN 통신 및 Smart Device를 이용한 자동차 도난 방지 기법 및 알고리즘

오늘 날 도난 방지 시스템을 보면 경고음 위주의 구식 방식부터 Smart Card방식까지 발전 해왔다. 이 방식들은 실제 도난의 목적이 있다면 차량을 도난 해 갈 수 있는 기회를 쉽게 제공하게 된다. 실제 Smart Card나 다른 모든 경우에는 Key를 습득하면 차량을 도난 할 수 있는 기회가 있다. 이에 본 논문에서는 CAN 통신과 Smart Device의 표준이라 할 수 있는 iPhone을 이용하여 차량 도난 방지에 대해 설명하고자 한다.

그림 1은 차량 통신 네트워크 시스템을 통해 고유 식별 ID를 받아서 Head Unit에게 전송한다. 그리고 iPhone 보안 애플리케이션을 이용해 사용자가 기억하고 있는 보안 ID를 입력한다. 이때 Head Unit은 입력 받은 보안 ID와 ECU가 전달한 고유 식별 ID를 비교한다. 서로 일치 한다면 ACC Locking을 Unlock으로 설정 변경하여 시동을 걸 수 있게 한다. 이에 사용자가 Key가 있다 하더라도 인증 절차가 없으면 ACC ON을 할 수 없게 된다.

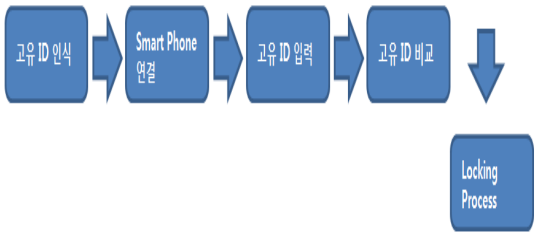

그림 1. 도난 방지 시스템 흐름도
Fig. 1 Flowchart of Antitheft System

3.1 CAN 통신 및 Smart Device

3.1.1 CAN 통신

CAN 네트워크 통신은 차량의 제너레이터 또는 배터리로부터 각각의 ECU들에게 전원이 공급되는 한 항상 통신이 이루어지며, 네트워크상에 브로드케스팅 방식으로 메시지가 전달되어 수신측의 ECU에서 선택적으로 메시지를 받아들인다. 본 논문에서는 CAN을 통해 수신한 고유 식별 ID를 통해 차량 도난 방지 시스템에 적용한다.

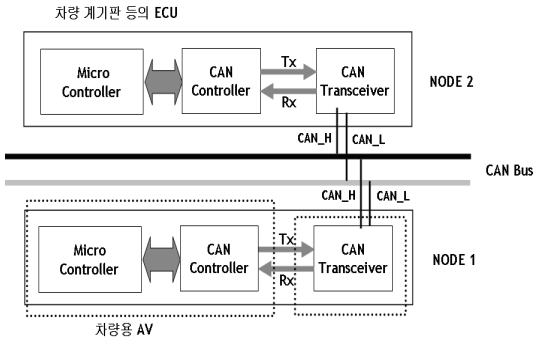

그림 2. CAN 네트워크 버스 블록다이어그램
Fig. 2 Block Diagram of CAN Network Bus

그림 2에서 볼 수 있듯이 ECU장치들은 고유의 번호를 갖는다. 생산되는 제품의 외관에 바코드 등을 사용하여 제품의 시리얼넘버를 기입하는 것이 일반적이었으나 현대 전자 산업에서는 제품 내부 메모리에 시리얼 넘버 및 제품의 정보 등을 기입한다. 이는 양산 이후 문제 발생 시 신속히 대처할 수 있도록 하기 위함이다. 특히 차량의 경우 전자 제치장치에 문제 발생 시 인명 피해에 직접적으로 영향을 미칠 수 있으므로 제품 정보에 대한 관리가 보다 철저하며, 문제 발생 시 생산되었던 차량들을 리콜하여 조치하는 제도를 취하고 있다.

이러한 시리얼 넘버 또는 별도의 고유 번호를 CAN통신을 통해 공유하고 전원이 단락 되어도 데이터가 사라지지 않는 EEPROM과 같은 비활성 메모리에 저장함으로써 위와 같은 시스템을 구성 할 수 있다. 아래 그림 3은 CAN 통신을 통한 차량 정보인식 프로세스 CAN 메시지 및 Head Unit의 동작을 설명한다.

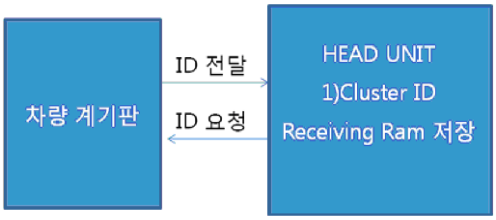

그림 3. 초기 장착 시 차량 정보 인식
Fig. 3 Car Information Recognition at Beginning Installation

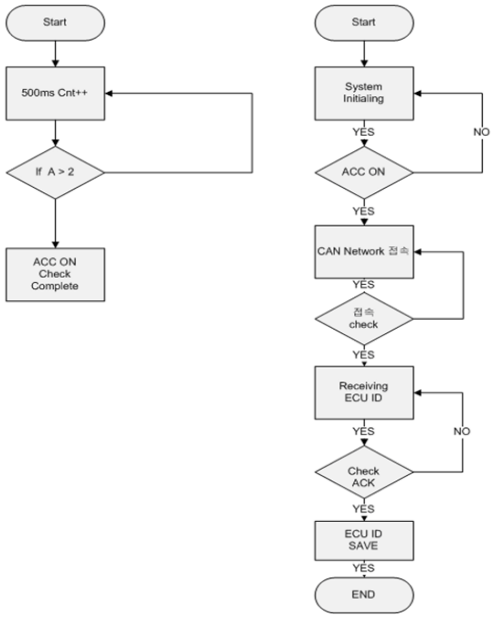

그림 4. 도난 방지 시스템 알고리즘
Fig. 4 Algorithm of Antitheft System

그림 4는 도난 방지 시스템에 관한 알고리즘 순서도를 보여준다.

3.1.2. Smart Device 연결

전달된 고유 ID를 수신 받아 본격적인 도난 방지 시스템으로 진입 할 수 있다. 1항에서 인지된 값을 통해 도난 방지 시스템의 첫 단계로 들어간다. 실제 요즘 사용자의 수가 늘어나고 있는 Smart Phone의 애플리케이션을 통해 확인을 위한 ID값을 입력 받는 시스템을 고안하였다. 대상 Device 는 현 개발에 사용 하고 있는 iPhone 4G를 사용 하였다. iPhone 4G는 IOS를 통해 양방향 통신으로 사용 할 수 있다. 이때 Device와 CAR Head Unit에 널리 사용되는 BT를 이용한다. 그림 5와 같이 Head Unit과 iPhone의 연결을 위해 BT의 RFCOMM을 이용하여 SPP Profile에 접속을 한다. SPP의 전송 Channel이 되는 무선 Protocol로 SPP Profile을 사용 할 수 있다. 이를 통해 무선 연결을 구현한다.

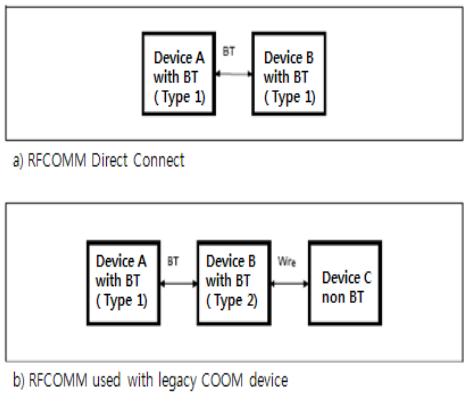

그림 5. SPP Profile 처리
Fig. 5 SPP Profile Processing

그림 6은 인증 iPohne CP Authentication을 실행 하는 단계를 나타낸다. 현 실험에서 Smart Device 를 iPhone 으로 선정하였기 때문에 다음 인증 단계가 필요하다. CP 인증이란 Apple에서 자사 Smart Device를 사용 시 Head Unit 내부에 Apple에서 지정한 Chip을 사용 하여 iPhone과 통신을 위해 Process하는 과정이다.

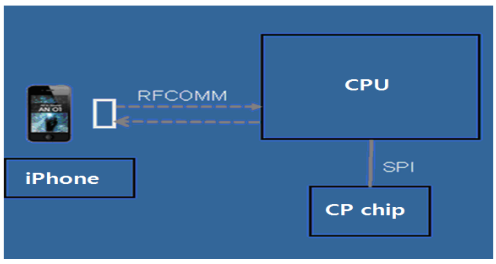

그림 6. CP 인증
Fig. 6 CP Authentication

3.1.3 Communication

그림 6은 iPhone과 통신을 위해 사용하는 단계를 나타낸다. 앞에서 설명 했듯이 BT Paring 후 RFCOMM SPP Profile을 통해 CP 인증 까지 완료를 하면 Smart Phone의 BT를 사용 하여 Head Unit과 통신을 할 수 있다.

3.2. 고유 ID 입력 및 Locking 동작 Process

인증을 완료 하면 Start Ready 상태가 되고, 이때 애플리케이션이 실행되어 있지 않으면, POP UP을 사용하여 Smart Phone Press the Security 애플리케이션을 띄운다. 이때 사용자는 애플리케이션을 실행하여 고유 ID를 입력한다. 실제 Smart Phone의 경우 사용 범위가 넓어서 선택하기 쉽다. 동작 과정은 다음과 같다.

- 실행된 어플리케이션에 고유 식별 ID을 입력
- ID Head Unit으로 전송
- 고유 ID Compraring
- ID가 일치 하는 경우 ACC Locking을 해제하고 Stand by 상태로 진입한다.
- ID가 일치 하지 않는 경우 수신된 고유 ID와 입력된 고유 ID의 비교 시스템이 동작한다.
- Error 발생 시 차량 ACC를 Locking 시켜 Start Mode 진입을 하지 않는다.

그림 7. 정보 입력 및 확인
Fig. 7 Information Input and Confirmation

Ⅳ. 실험 및 평가

4.1. 실험 환경

본 실험을 위해서는 그림 8 과 같이 전원 공급 장치와, CAN통신이 지원되는 차량 계기판(Cluster)과 차량용 Head Unit이 필요 하며, 장비 및 소프트웨어 툴에 대한 상세 내역음 아래와 같다.

[실험 장비 및 소프트웨어 툴]
- 인터페이스
  CANcardXL (Vector)
- 네트워크 인터페이스 드라이버
  CAN Driver (Vector)
- 개발 Tool
  CANoe V5.0.44 (Vector)

- 데이터베이스 Tool
  CANdb++ (CANoe 포함)
- Panel 생성 Tool
  Panel Editor (CANoe 포함)
- 개발 언어
  CAPL (CANoe CAPL Browser)
- Head Unit
  IPHONE 4G
- 전원 공급 장치
  Votage Drop Test Tower System

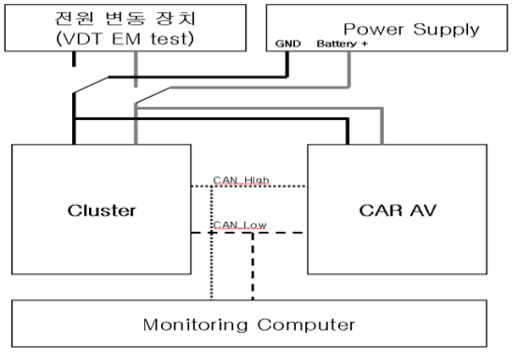

그림 8. 실험환경 Set-up
Fig. 8 Experimental Conditions Set-up

4.2. 실험 및 결과

본 논문은 Head Unit을 통한 기기의 도난방지 기법에 대한 노의 이므로, 기본적으로 Head Unit은 CAN 통신이 지원되는 시료로 실험을 진행한다. 첫째, ACC On/Off에 따라 Mode 진입 여부 확인. 둘째, 고유 ID확인 후 전원 변동 시험에 따라 Mode 해제 여부 확인을 한다. 판정기준은 아래와 같다.

㉠ 차량 탑승 후 ACC ON 시 Security Mode로의 진입
[판정기준] (ACC ON)
'Security Mode'로의 진입 OK
'Security Mode 로의 미 진입 NG
㉡ 차량 탑승 후 ACC OFF 시 Security Mode로 미 진입
[판정기준] (ACC OFF)
'Security Mode'로의 진입 NG
'Security Mode 로의 미 진입 OK

그림 9 전원변동에 따른 도난 방지기 동작 확인을 위한 그림이다.

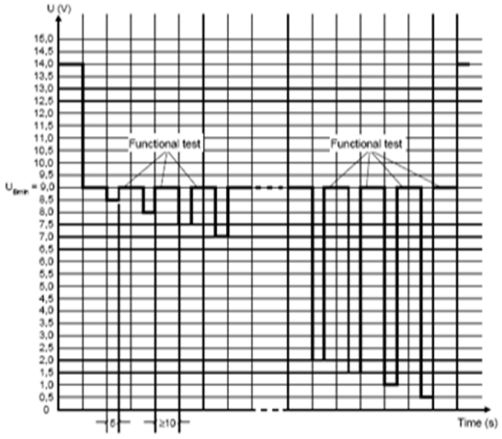

그림 9. 전원변동에 따른 도난 방지기 동작 확인
Fig. 9 Experimental Conditions Set-up

[판정 기준]
'Security Mode'로의 미진 입 OK
'Security Mode'로의 진입 NG

V. 결론 및 향후 연구 방안

차량에서 검증된 통신 네트워크인 CAN 통신을 이용하여 본 도난 방지 시스템을 구축함으로써, 보다 안정적이고 강력한 도난 방지 기능 구현이 가능하다. 실제 차량의 시동을 강제로 걸 시에 ACC On/Off시 해당 모드에 추가 진입하여 확인 절차를 거쳐야 하기 때문에 강제로 시동을 걸 수 있는 방법은 없다. 또한 본 논문에서 제안하는 시스템에 추가적으로 CAN 동신을 이용한 차량 애플리케이션을 확대 하면 더 많은 차량과 관련된 보안 및 정보 전달에 이용 될 수 있다. 사용 User가 많아지기 때문에 부가 기능으로 적용하여 사용하게 되면 더 많은 기능을 적용할 수 있어 차량의 제품 경쟁력에 도움을 줄 수 있다.

참고문헌

[1] 최신 시리얼 버스의 구조 : CAN의 기초지식(월간 전자기술)

[2] "Road Vehicles Interchange of Digital Information Controller Area Network(CAN) for High Speed Communication", *ISO DIS 11898* (February 1992)

[3] "Controller Area Network Basics, Protocols, Chips and Applications", Konrad Etschberge

저자소개

김재경(Jae-kyung Kim)

1988. 2 아주 대학교 전자공학과 학사
1990. 2 아주대학교 전자공학과 석사

1989.12 ~ 2011.2 메디슨 연구소
2010. 8 ~ 아주대학교 의용공학과 박사 과정
2011. 4 ~ 현재 : 지멘스 (SLS) 초음파 상무이사
※관심분야 : 의료기기(초음파진단기), 신호처리

황만태(Man-tae hwang

2005. 1 광운대학교 전파공학 학사
2011. 9 아주대학교 전자공학과 석사
2005.1 ~ 2011.9 LG전자
※관심분야 : 신호처리, 임베디드 System

김영길(Young-kil Kim)

1978 고려대학교 전자공학과 학사
1980 한국과학기술원 석사
1984 ENST(프랑스) 박사
1984-현재 아주대 전자공학과 교수
※관심분야: RFID Platform, Embedded System, 초음파 의료기기, Mobile 의료정보 시스템