ITS 무선통신기술의 현황과 전망

하동문, 김용득
(아주대학교 전자공학부)

I. 서론

지능형교통체계(ITS : Intelligent Transportation System)란 교통량, 차량번호 등을 감지할 수 있는 장치를 도로에 설치하여, 교통흐름을 컴퓨터로 처리하는 최적 신호 관리 체계와 도로변 또는 차량에 장착된 화면을 통하여 출발지에서 목적지까지의 최단거리, 소요시간, 주차상황 등 운전자가 필요로 하는 각종 교통정보를 신속, 정확하게 제공하는 서비스체계 및 차량에 고성능 센서(GPS, DMB등)와 제어장치를 부착하여 운전을 자동화하기 위한 차세대 차량을 의미한다.

이를 다시 기능별로 구성하면 차량통과 대수, 속도, 차종, 점유율, 대기행렬 등을 검지센서로부터 교통정보를 수집하여 이를 가공 처리한 후 운전자에게 이들 정보를 공급하는 체계로 그림〈1〉과 같이 표시할 수 있다. 교통정보 제공방식은 ARS, 인터넷 등에 의하여 출발 전 교통정보를 확인 후 최적 경로를 선택하는 여행 전 교통정보와 DMB, 셀폰, GSM, VMS와 같은 여행 중 교통정보를 제공받는 체계로 구성되며, 이들 각 블록은 유.무선 통신망으로 구성된다. 즉, 이들 ITS에 사용되는 통신망의 구성을 요약하면 그림〈1〉과 같으며, 특히 이동중인 차량과 ITS 인푸라와의 유망한 통신방식이 무선식별(RFID: Radio Frequency Identification)시스템이다.

이 RFID는 소형화, 지능화하는데 비해, 가격은 수 센트대로 저가화가 예상되어 ITS분야뿐 아니라 물류, 유통분야

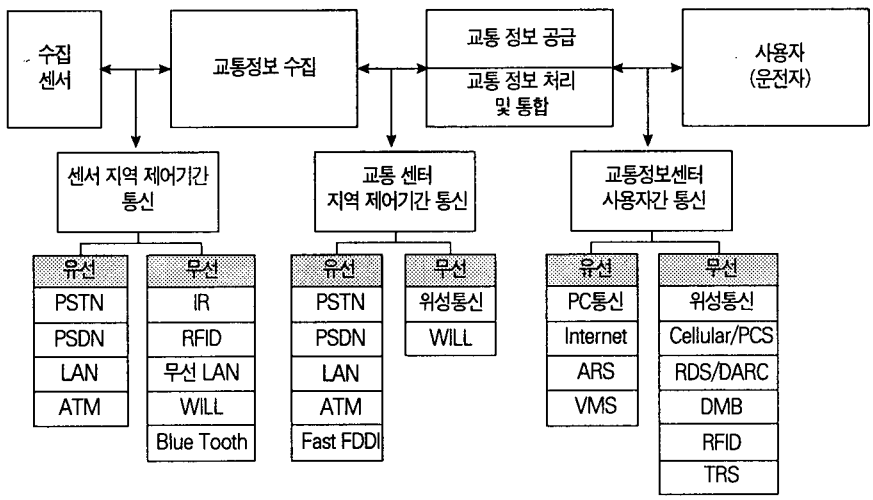

그림 1. ITS 통신망

에도 널리 사용되리라 기대된다. 즉, ITS 분야에서 무선식별기술은 단거리전용통신(DSRC : Dedicated Short Range Communication)으로 표준화가 추진되었고, 따라서 본 기고에서는 무선식별과 DSRC 기술에 대한 고찰을 통해 무선식별기술의 ITS 적용사례를 분석하고 향후 발전방향을 전망하고자 한다.

II. 무선식별 시스템 구성

RFID 시스템은 접촉식 식별 시스템과는 달리 트랜스폰더에 대한 전력공급과 리더와의 데이터 교환이 전기적 접촉없이 자계 또는 전자계 영역을 이용하여 이루어진다. 리더는 제어기능과 트랜스폰더와 연결 기능을 하는 무선주파수 모듈과 수신된 데이터를 다른 시스템으로 송신하기 위한 RS-232, RS-485 등 별도 인터페이스를 갖으며 RFID 시스템의 데이터 운반장치인 트랜스폰더는 결합장치와 마이크로칩으로 구성되며 표〈1〉에서처럼 동작방식, 데이터 량, 프로그램 가능성, 데이터 캐리어의 작동 원리, 전원 공급, 주파수 범위 등 다양한 특성을 갖는다.

〈표 1〉 RFID 시스템의 특징

특 징	세부분류		
동작방식	HDX/FDX	SEQ	
데이터 량	n-Bit	1-Bit EAS	
프로그램 가능성	가능	불가능	
트랜스폰더 동작 원리	IC	SAW	Physical
펌웨어 설계 방법	상태 처리기	마이크로프로세서	
전원공급	Battery	passive	
주파수 범위	LF	RF	Microwave
데이터 전송	Sub narmonics	Back-scatter	기타

RFID 시스템의 동작원리는 그림〈2〉와 같이 분류되며, 1-비트 트랜스폰더는 리더에 트랜스폰더가 전자계내에 '있다' 또는 '없다'의 두 가지 상태정보만을 제공하므로 전자도난 방지 기기 등에 사용한다. 이 시스템은 동작방식에 따라 무선 주파수 방식, 마이크로파 방식, 주파수 분배기, 전자기 방식, 및 음향자기 방식으로 구분한다. 무선 주파수 방식은 리더에서 발생되는 교류 자계에 의한 트랜스폰더내의 LC 공진회로의 공진에 따른 전압강하를 감지함으로써 트랜스더의 존재를 식별하고, 마이크로파 방식은 리더에서 전송한 마이크로파에 대한 2차 고조파를 생성하는 비선형 특성 선로(예, 다이오드) 소자를 갖는 트랜스폰더를 사용하며, 주파수 분배기는 자가-유도성 코일을 사용하여 리더가 전송한 신호의 주파수를 반으로 분할하는 방식을 사용한다. 전자기 방식은 강 자계를 사용하여 리더의 기본 주파수에 대한 고조파를 발생시키는 방식을 사용하며 음향자기 방식에서는 트랜스폰더 코일의 공진에 의한 교류 자계를 리더가 감지하여 트랜스폰더를 인식한다.

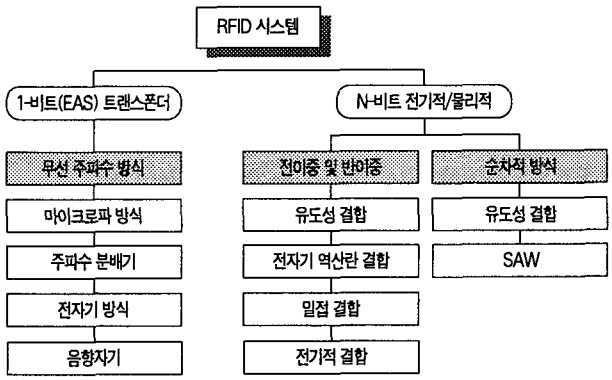

그림 2. RFID 시스템 동작원리별 분류

반면에 n-비트 메모리 트랜스폰더 시스템은 수 킬로바이트까지의 데이터 저장 용량을 갖으며, 데이터의 읽기와 쓰기를 위해 트랜스폰더와 리더간의 데이터 송수신이 가능해야 한다. n-비트 메모리 RFID 시스템은 데이터 전송 방식에 따라 전이중 및 반이중 방식과 순차적 방식으로 구분된다. 즉, 시간에 따른 전이중, 반이중, 순차적 시스템에서의 에너지와 데이터 전송은 그림〈3〉과 같은 방식으로 수행된다.

반이중 및 전이중 방식에서는 리더로부터 트랜스폰더로의 에너지 전송은 데이터의 전송 방향과 무관하게 항상 연속적인 반면 순차적 시스템에서는 리더로부터 트랜스폰더로의 데이터와 에너지 송신이 트랜스폰더로부터 리더로의

데이터 전송과 교대로 발생한다. RFID시스템은 결합 방식에 따라 유도성 결합, 전자기 역산란 결합, 밀접 결합, 전기적 결합으로 분류되고 순차적 시스템의 경우에는 유도성 결합과 표면 음향파 트랜스폰더로 구분된다.

유도성 결합 시스템이란 리더의 일차 코일과 트랜스폰더의 이차 코일간의 트랜스포머 형태 결합에 기반을 두고 있으므로 수동형으로 동작하고 코일간의 거리가 0.16λ를 초과하지 않는 경우에만 적용된다. 전자기 역산란 결합은 전자기파의 반사 특성을 이용하는 방식으로 리더와 트랜스폰더 사이의 간격이 1m 이상인 장거리 시스템에 주로 사용되고 15m 이상의 인식범위가 요구되는 경우에는 트랜스폰더에 전력 공급을 위한 배터리를 사용해야한다. 밀접 결합 시스템은 0.1cm에서 최대 1cm의 인식 범위로 설계되므로 트랜스폰더는 리더안에 삽입되거나 표시된 면위에 놓아서 동작시키는 방식을 채택한다. 밀접 결합 시스템은 유도성 결합과 같이 코일간의 트랜스포머 형태 결합에 기반을 두고 있으나 리더와 트랜스폰더가 밀접 결합되기 때문에 유도성 결합 또는 마이크로파 시스템에 비해서 에너지 전송 효율이 매우 양호하므로 고전력을 소모하는 칩의 동작에 매우 적합하다.

RFID 리더의 주된 기능은 트랜스폰더를 활성화시키고

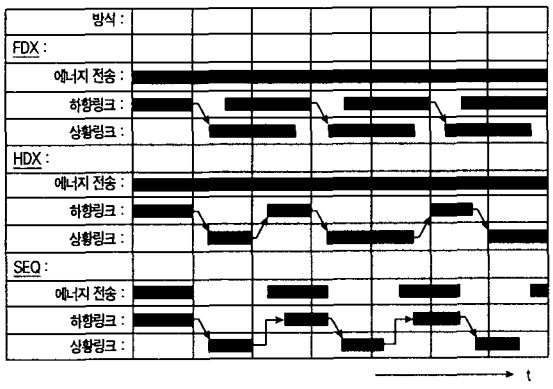

그림 3. RFID 시스템 전송 방식

통신 시퀀스를 구성하며 응용 소프트웨어와 트랜스폰더간에 데이터를 전달하는 것으로 통신 주체간의 연결과 충돌방지 및 인증 과정의 수행 등은 리더에 의해서 관리된다. 리더는 그림(4)에서처럼 제어 시스템과 고주파(HF) 인터페이스라는 두 가지의 기본적인 기능 블록으로 구성된다.

여기서 HF 인터페이스는 송신기와 수신기로 구성되며

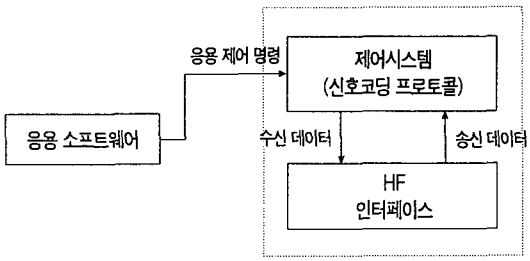

그림 4. RFID 시스템 리더 구성도

RS-232 인터페이스를 통해서 응용 소프트웨어와 데이터 교환을 수행한다. 리더의 HF 인터페이스는 트랜스폰더를 활성화시키기 위한 고주파 전송 전력의 발생과 트랜스폰더로의 전원 공급, 트랜스폰더로의 데이터 전송을 위한 전송 신호의 변조, 트랜스폰더로부터 전송된 HF 신호의 수신과 복조 기능을 수행한다. 리더의 구성요소인 제어 시스템은 응용 소프트웨어와의 통신과 이의 명령 실행, 트랜스폰더와의 통신 제어, 신호의 코딩과 디코딩을 수행하며 보다 복잡한 시스템에서는 충돌 방지 알고리즘의 실행, 트랜스폰더와 리더간에 전달될 데이터의 암호화와 암호 해독, 트랜스폰더와 리더간의 인증 수행과 같은 부가적인 기능을 담당한다.

III. RFID 통신 프로토콜

RFID 시스템에서 수행되는 통신은 응용 소프트웨어와 리더 그리고 리더와 트랜스폰더간의 통신으로 구분된다. 이러한 두 가지 통신은 모두 마스터-슬레이브 방식으로 이루어진다. 즉, 응용 소프트웨어는 마스터에 해당하고 리더는 슬레이브로서 응용 소프트웨어로부터 쓰기/읽기 명령을 수신하였을 때만 동작하게 된다. 또한 리더는 응용 소프트웨어로부터의 명령을 수행하기 위하여 트랜스폰더와 통신을 수행할 때 마스터로 동작한다.

〈표 2〉 RFID 시스템 통신 프로토콜 예제

애플리케이션↔리더	리더↔트랜스폰더	설 명
→Blockread_address[00]	→Request	트랜스폰더 메모리 읽기 [어그레스]
	←ATR_SNR[4712]	트랜스폰더가 판독 영역에 있는가?
	→GET_Random	일련 번호를 갖는 트랜스폰더가 동작인증 개시
	←Random [081514]	
	→SEND_Token1	인증 성공적 완료
	←GET_Token2	읽기 명령 [어드레스]
	→Read_@ [00]	트랜스폰더로부터 데이터
	←Data [9876543210]	애플리케이션으로의 데이터
←Data [9876543210]		

따라서, 트랜스폰더는 리더로부터의 명령에만 응답하고 독립적으로 동작하지는 못한다. RFID 시스템에서 수행되는 통신 프로토콜의 예를 표〈2〉에 보여준다. 즉, 읽기 명령은 트랜스폰더를 활성화시키고 인증절차를 시작하며 최종적으로 요청한 데이터를 전송한다.

RFID 시스템에서 데이터 전송은 코딩된 후 변조장치를 통해서 고주파 신호로 변환되어 전송되고 수신측에서 복조와 디코딩 과정을 통해서 원래의 데이터로 복원된다. 이들 데이터 코딩 방법에는 그림〈5〉와 같이 NRZ 코드, 맨체스터 코드, 단극 RZ 코드, DBP 코드, 밀러 코드, 변형된 밀러 코드, 차분 코드, 펄스-휴지 코드 등이 사용된다. NRZ 코드는 대체로 ASK, FSK, 및 PSK 변조방식과 함께 사용되고 맨체스터 코드는 트랜스폰더에서 리더로의 데이터 전송에 부반송파를 사용하는 부하변조로 사용되기도 하며 변형된 밀러 코드와 펄스-휴지 코드는 유도성 결합 RFID 시스템에서 하향링크에 주로 적용된다.

또한 RFID 시스템에서는 신뢰성 있는 데이터의 전송을 위해서 오류제어와 충돌방지방법이 사용된다.

즉, RFID 시스템에서 오류검출방법은 패리티 검사, LRC(Longitudinal Redundancy Check), 및CRC(Cyclic Redundancy Check) 등이 사용된다. 또한, RFID 시스템에서는 다수의 트랜스폰더가 하나의 리더의 전송영역내에 동시에 존재하는 다중접속 상황이 발생하게 되는데 이를 해결하기 위해서 사용되는 것이 충돌방지방법이다. 충돌방지방법에는 공간분할다중접속(SDMA), 주파수분할다중접속(FDMA), 시간분할다중접속(TDMA), 및 부호분할다중접속(CDMA)이 사용된다.

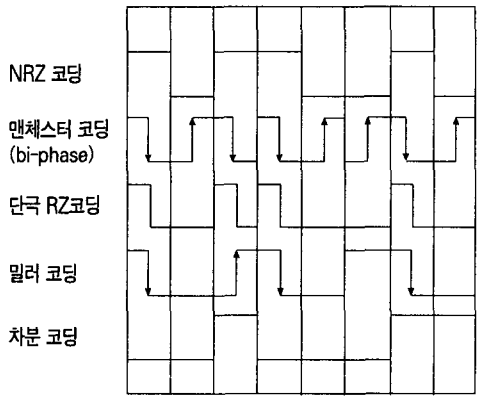

그림 5. 기저대역 신호 코딩

IV. 보안 체계

RFID 시스템의 응용은 출입 시스템과 지불 및 티켓 발행 등 점차 고도의 보안이 요구되며, 고의적으로 시도되는 공격으로부터 데이터를 보호하기 위한 보안 수단이 필수적이다. 따라서 높은 보안성을 갖는 RFID 시스템은 데이터를

복사하거나 변경하기 위한 데이터 반송파의 불법적 해독, 건물의 불법 출입이나 요금을 지불하지 않고 서비스를 받을 목적으로 리더의 판독 영역 내에 이종의 데이터 반송파를 위치시키는 것, 순수한 데이터 반송파를 모방하기 위한 무선 통신의 도청과 데이터 재생과 같은 각각의 공격으로부터 방어 능력을 가져야 한다. 즉, 사용자 인증과 데이터 암호화를 통해서 위와 같은 공격으로부터 시스템을 방어할 수 있어야한다. 인증(Authentication)이란 리더와 트랜스폰더간 통신의 합법성 여부를 판단함으로써 위에서 언급한 것과 같은 보안 공격을 차단한다. RFID 시스템에서의 리더와 트랜스폰더간의 상호인증은 ISO 7898-2에서 규정하고 있는 3단계 통신 상호 인증 원리에 기초하며, 여기에는 상호 대칭 인증과 계산하여 구한 키를 사용하는 인증이 있다.

① 상호 대칭 인증

상호 대칭 인증 방법에서는 RFID 응용 서비스를 구성하는 모든 트랜스폰더와 리더들이 동일한 비밀 암호키를 사용하며 상호 인증 과정은 리더가 GET_CHALLENGE 명령을 트랜스폰더로 전송하면서 시작된다. 명령을 수신한 트랜스폰더는 난수(RA)를 생성하여 리더로 전송하고 이를 수신한 리더는 공통의 비밀 키와 공통적인 키 알고리즘을 사용하여 데이터 블록(TOKEN 1)을 계산한다. 여기에는 리더가 생성한 난수(RB)와 부가적인 데이터가 포함되고 이 데이터 블록을 트랜스폰더로 전송하면, 트랜스폰더는 수신된 TOKEN 1에 포함된 난수와 자신이 이전에 송신한 값을 비교하여 공통 키의 일치여부를 판단한다. 만약 일치한다면 트랜스폰더는 새로운 난수를 생성하고 TOKEN 1을 통해 수신된 리더가 생성한 난수와 제어 데이터를 포함하는 TOKEN 2를 계산하여 전송함으로써 공통 키의 일치 여부를 확인한다. 이러한 일련의 과정을 통해서 리더와 트랜스폰더는 자신들이 동일한 시스템에 속해 있고 양자간의 통신이 합법적이라는 것을 확신할 수 있다.

② 계산하여 구한 키를 사용하는 인증

상호 대칭 인증은 해당 응용 서비스에 속한 모든 트랜스폰더들이 동일한 암호키를 사용하기 때문에 대중 교통망에서의 티켓팅 시스템과 같이 다수의 트랜스폰더를 사용하는 경우에는 공통 키 노출의 잠재적인 취약성을 내포하고 있다. 이러한 문제점을 해결하기 위하여 모든 트랜스폰더가 서로 다른 암호키를 사용하는 "계산하여 구한 키를 사용하는 인증" 방법이 도입되었다. 이 방법에서 트랜스폰더는 제조과정에서 자신의 고유한 일련번호와 마스터 키를 사용하여 생성된 암호키를 사용한다. 리더는 그림〈6〉에서처럼 GET_ID 명령을 통해서 수신된 트랜스폰더의 일련번호와 마스터 키 를 이용하여 해당 트랜스폰더의 암호 키를 특수 안전 모듈인 SAM(Security Authentication Module)에서 생성하여 인증과정에 사용한다.

또한 데이터 암호화 기법은 수동적이고 능동적인 모든 공격으로부터 보호하기 위하여 사용된다. 암호화와 복호화에 사용된 키가 동일하거나 서로 직접적인 연관이 있는 암호화 방식을 대칭 키 암호화 알고리즘이라 하고 반대로 키가 복호화 과정과 관련이 없는 경우에는 비대칭 키 암호화 알고리즘이라고 하며, RFID 시스템에서는 대칭 키 방식이 사용되는데, 이는 또 블록 암호화와 스트림 암호화 방식으로 구분된다. 블록 암호화의 경우 계산량이 매우 많으므로 RFID 시스템에서는 비트 또는 문자 단위로 암호화를 수행하는 스트림 암호화 방식을 사용한다. 스트림 암호화란 모든 평문에 동일한 암호화 함수가 적용되는 블록 암호화와는 달리 평문의 비트 또는 문자가 암호화되어짐에 따라 상이한 암호화 함수가 적용된다. 이 방식에서 암호화는 비밀키와 평

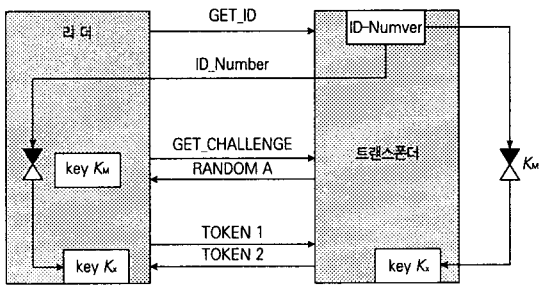

그림 6. 계산하여 구한 키를 사용하는 인증

문 그리고 현재의 스트림 암호시스템 상태와 연동하여 작동된다. 즉, 비밀키와 현재의 상태변수로부터 도출되는 키 수열이 평문과 결합되어져 암호문이 생성된다. 암호문은 일반적으로 평문과 스트림 암호시스템의 상태의 함수 값을 비트 단위로 XOR하여 생성된다. 스트림 암호화는 암호시스템의 다음 상태가 결정되는 방식에 따라서 동기식 스트림 암호화와 자기 동기식 또는 비동기식 스트림 암호화로 분류된다.

V. 표준화 방안(DSRC)

ITS 분야에서는 기존의 공중 무선통신망과는 달리 도로에서 주행중인 차량을 대상으로 하여 도로변에 노변장치(RSU : Road Side Unit)라는 비교적 간단한 기지국을 설치하고 차량에는 RFID 트랜스폰더의 일종인 차량 단말기(OBU : On Board Unit)라는 저가의 통신 단말기를 탑재하여 고속으로 무선 패킷 통신을 행한다. 이러한 무선기기는 용도상 통상 100m 이내의 무선 링크를 통신범위로 하므로 단거리 전용통신(DSRC)이라는 새로운 개념의 통신방식이 정립되고 있다. DSRC의 특징은 100m 이하의 통신범위에서 능동방식과 수동방식이 가능한 다양한 ITS 서비스를 제공하며, 값싸고 단순한 변조 기술을 사용하여 ITS 무선 패킷 데이터 통신 시스템을 구성하는 데에 있다. DSRC 통신 프로토콜은 고속으로 주행하는 차량과 통신이 가능한 시간이 수초에서 수십 밀리초에 불과하므로 단순하고 빠른 통신절차를 채용한다. 따라서 프로토콜의 구조가 OSI 계층의 물리계층, 데이터 링크계층 및 응용계층의 3계층만으로 구성되어 있고 네트워크 계층 등 필요한 기능은 계층 7에 통합되어 있다. DSRC의 표준화 추진은 국제기구인 ISO에서 TICS가 주관하고 있으며, ISOTC-204 WG 15에서 DSRC 시스템의 표준에 관한 연구활동이 계속되어 1994년부터 ITS 표준화도 함께 추진하고 있다.

VI. ITS 적용 사례

DSRC를 중심으로 한 무선식별기술의 ITS 분야 적용 사례로는 자동 통행요금 징수 시스템(ETCS : Electronic Toll Collection System), 교통 정보수집 및 제공 서비스, 주차관리시스템, 그리고 첨단 안전 차량 등이 있다. ETCS는 전자지불 기능을 하는 스마트카드와 OBU를 이용하여 DSRC에 기반한 무선통신을 통해 고속도로, 유료도로 요금소에서 무정차 주행중에 통행료를 징수하는 시스템으로서, 요금소에서 정체완화를 통한 물류비 절감 및 환경오염 개선, 요금징수 전산화를 통한 운영 유지비 절감 및 이용자에게의 서비스를 개선하는 효과를 갖는다. 국내에서는 한국도로공사에서 Hi-Pass라는 이름으로 DSRC 고속 수동방식을 이용하여 시범사업으로 운영 중에 있다. 교통정보수집 및 제공 서비스는 교차로나 도로상의 주요지점에 설치된 노변장치와 ETCS를 위해서 차량에 장착된 ETCS 차량단말기간의 통신을 통해서 차량 통과 대수, 차량 점유률, 대기행렬, 그리고 차량속도와 같은 다양한 교통정보를 추출하는 것이다.

DSRC를 이용하면 교통정보의 수집뿐만 아니라 교통센터에 집결된 다양한 실시간 교통정보를 운전자에게 전달할 수 있고, 여기에 GPS 위치정보와 GIS 지도정보를 추가하면 차량주행안내 시스템의 구현도 가능하다. 주차관리시스템은 앞에서 기술한 ETCS 기술을 빌딩, 아파트, 유료주차장 등의 주차관리에 응용한 경우라고 할 수 있다. 이러한 주차관리시스템은 출입이 허가된 차량에 RFID 트랜스폰더를 부착하여 차량의 데이터를 사전에 서버에 등록한 후 입·출입시 리더기와의 순간적인 통신을 통하여 출입가능여부를 판단하여 무정차로 출입을 통제할 수 있도록 한 것이다. 첨단 안전 차량은 교통 신호 제어기의 신호변경 정보를 DSRC를 통해 실시간으로 차량내 단말기에 전달하여 운전자로 하여금 위험지구에서 의사결정을 안전하게 내릴 수 있도록 유도하는 차내경고시스템이다. 첨단 안전 차량은 녹색신호등의 잔여시간 정보를 유선을 통해 RSU로 전송하는 교통신호제어기, 수신한 정보를 DSRC를 통해 무선으로 차내단말기로 송신하는 RSU, 그리고 RSU로부터 수신한 정보와 속도를 분석하여 경고음과 LCD에 경고 메시지를 출력하는 차내장치 등으로 구성된다.

VII. 결론

본 기고에서는 유비쿼터스 네트워크에서 센서 기능을 담당하는 RFID에 대해 동작원리와 통신 프로토콜 및 데이터 보안등의 관점에서 논하였고, RFID 응용분야 중 ITS 분야 적용사례, 즉 ETCS, 교통정보수집 및 제공, 주차관리시스템, 첨단 안전 차량과 같은 응용분야에 대해서 DSRC 표준안을 중심으로 기술하였다. RFID 시스템은 향후에는 주변 환경 인지 기능, 개체 간 통신 기능, 상황 인지 정보처리 능력과 같은 유비쿼터스 센서로서의 역할이 강화되고 트랜스폰더의 소형화 및 지능화가 이루어질 것으로 예측된다. 특히 ITS 분야에서는 운전자 안전성, 운전효율, 그리고 운전자 편리성 제공을 위한 다양한 응용분야들이 창출될 것으로 전망된다. 이러한 응용분야들은 우리의 실생활과 밀접한 고부가가치 창출이 가능한 핵심 전략분야이므로 정부와 학계의 지속적인 관심과 기술투자가 절실하다고 하겠다.

참고문헌

[1] Klaus Finkenzeller, RFID handbook 2nd edition : fundamentals and applications in contactless smart cards and identification, 2003

[2] Kazimierz Siwiak, Ultra-Wide Bnad Radio : Introducing a New Technology, VTC2001 Spring, 2001

[3] Muhlberger, High speed public encryption on contactless smart cards, 2001

[4] ISO 9798 : Information technology-Security techniques-Entity authentication

[5] Japan ISO TC204 WG15 Committee, "DSRC-5.8GHz Full Duflex Active DSRC", Ver.0.65, 1998

[6] CEN TC 278 WG 9 SGL 7, "DSRC Application Layer Architecture and Definition of Services", Working Document

[7] www.rfidjournal.com

[8] www.autoid.org

[9] www.itskorea.or.kr