

등이 등장하면서 신용카드 및 각종 지급 결제 서비스 분야 등에 적용되고 있다. 그러나 RFID 칩의 가격이 고가이고 다른 전파의간섭이 기술적인 문제가 될 수 있다는 점이 상용화가 되는 걸림돌이 되고 있으며, 2차원 바코드 역시 규격화를 이루고 있는 리더기와 소프트웨어 등 대부분 비싼 로열티를 지급하고 들여와야 하는 것이 문제이다.

본 논문은 유비쿼터스 환경에서 2차원 바코드와 RFID를 이용한 사례 및 적용 분야에 대한 최근 기술의 특성을 비교, 분석하여 이에 따른 문제점을 파악하고 활성화 할 수 있는 방안을 고찰하였다.

또한 의류, 제화, 생산품 등의 상품에 태그를 부착하여 상품의 기본적인 정보를 입출력 처리하여 신속, 정확, 안전하고 통합적인 물류관리 시스템으로 물류비용의 최소화와 고객 서비스를 획기적으로 향상 시킬 수 있는 시스템을 개발하고자 RFID 리더기와 태그를 갖춘 임베디드 시스템 환경에서 인식 할 수 있는 소프트웨어를 설계 및 구현한다. RFID 태그와 GPS 위치정보를 파싱하는 모듈, 서버측의 데이터베이스의 구축을 통한 물류 관리 시스템으로 자동 검수의 신속, 정확한 재고 조사와 제품의 위치 파악, 정보 갱신, 입고 및 출고 확인, 도난 방지 등의 기능에 활용될 수 있다.

또한, 휴대용 PDA를 사용함으로써 기존의 고정식 인식 시스템이 할 수 없는 영역까지 응용의 범위를 넓힐 수 있었고, 저비용의 시스템구축을 통한 경제성을 실현할 수 있었다.

향후 연구 계획으로는 이러한 문제점들을 해결하고자 제시되는 새로운 대안책으로 임베디드 보드를 설계하여 PDA를 대체하고, RFID 리더기와 GPS 수신기의 모듈을 장착하여 휴대하기 편리한 구조의 일체형 시스템을 개발하고자 한다.

25. PKI 기반의 암호화 통신 컴포넌트 설계 및 구현

전자통신공학과 조원희
지도교수 임재홍

PKI(Public Key Infrastructure)는 우리 실생활 전반에 걸쳐 폭 넓게 자리 잡아가고 있다. 우리가 인터넷을 통하는 한 순간에도 PKI 기반의 시스템들은 복잡한 인증체계를 구동시키며 안전하고 신뢰성있는 네트워크 환경에 일조하고 있다. 그러나 이렇게 널리 유용하게 사용하는 기존의 체계에도 개선되고 있기는 하나 속도, 비용, 범용성 등의 주요한 문제가 발생해왔었다.

본 논문에서는 이러한 점들을 극복해보고자 PKI를 기반으로 하는 개인키와 공개키, 그리고 세션키를 통한 개인 사용자에게 대한 독립적인 인증이 가능하며 기본적인 암호화 기능을

제공하는 통신 컴포넌트를 설계 및 구현하였다. 또한 세션키의 재사용성을 증가하여 대기 시간과 전체 시스템의 속도향상을 할 수 있도록 하였으며 컴포넌트에 자체적으로 탑재 가능한 인증기관 역할을 하는 데이터베이스를 통해 데이터베이스가 주로 접근 대상이 되는 가상 환경에서 사용자 인증과정에 포함되는 권한 인증기능을 포함시키도록 하였다. 그리하여 기존의 고비용과 고성능의 인프라가 필요하지 않은 소규모 네트워크 또는 짧은 메시지 통신이 주를 이루는 환경에서 신뢰성있게 동작할 수 있는 통신용 컴포넌트를 통해 적합하게 사용할 수 있도록 하고자 하였다.

이러한 결과 기존의 PKI기반의 TLS같은 응용 솔루션에 비해 속도면에서 우세할 수 있게 되어 처리율의 증가, 대기시간에 대한 회피가 가능해졌다. 또한 탄력적인 키 길이를 이용해 적절한 수준의 보안강도를 유지할 수 있으며 인증서의 부피를 줄이고 이를 통한 권한 부여가 가능하도록 하여 클라이언트에서 보다 간편한 절차에 의해 PKI기반의 암호화 통신을 통해 서버 또는 주 시스템에 접근이 가능하도록 설계해 보았다.

키 길이의 탄력적인 운영은 통신환경이 허용하는 보안성을 저해하지 않는 만큼 안에서 이루어져야 할 것이며 인증기관의 운영 또한 일부 접근 가능한 권한으로부터 안전하게 보호되어야만 한다.

26. 최적화된 큐 기반의 NMEA 멀티플렉서 설계 및 구현

전자통신공학과 최 정 훈
지도교수 임 재 홍

해상전자장치들 간에 통신을 하기 위한 표준 통신 프로토콜이 필요하며, 이러한 해상전자장치들 간의 표준통신 프로토콜을 정하는 목적으로 미국해상전자통신협회(NMEA : National Marine Electronics Association)라는 위원회가 발족하였다. NMEA는 해양 전자산업의 발달 및 교육, 판매 시장에 공헌하는 위원회 이며, 해상전자장치 사이에 통신을 위하여 전기적 신호에 관한 인터페이스와 데이터 프로토콜로 정의할 수 있다.

NMEA 프로토콜을 사용하는 장치로부터 출력되는 신호를 처리하기 위해서, 장치의 기본 포트를 이용하면서 부족할 경우 멀티포트를 사용하여 처리하고 있다. 그러나 수많은 출력신호에 대한 부가 적인 멀티포트의 적용과 전용장치로서 출력에 대한 제약사항의 문제점이 발생 하므로, 이를 해결하기 위하여 NMEA 관련 신호들을 다중화(Multiplexing) 할 수 있는 모듈인 멀티플렉서가 필요하다.

현재 국내에서는 NMEA 멀티플렉서를 개발한 사례와 제품이 없어, 외국의 고가 장비를