단거리 전용통신을 이용한 지능형 교통시스템에서의 안전한 전자 지불 시스템

A Secure Electronic Payment System in Intelligent Transportation Systems Using the Dedicated Short Range Communications

장청룡, 이용권
경동대학교 컴퓨터미디어공학부
Chung-Ryong Jang(crjang@k1.ac.kr), Yong-Kwon Lee(yklee@k1.ac.kr)

요약

교통체계의 구성요소에 다양한 첨단기술을 접목시켜 체계적이며 효율적인 교통제어를 위하여 차세대 지능형 교통시스템(ITS ; Intelligent Transportation Systems)을 구축, 운영하기 위하여 많은 연구와 개발이 이루어지고 있다. 이러한 ITS 응용서비스 중에서 요금의 자동결재가 요구되는 다양한 전자 지불 형태의 서비스에는 정당한 통신 실체들간에 인증이 반드시 요구되고 있다. 본 논문에서는 단거리 전용통신을 이용하여 고속도로에서의 톨 요금 자동 결재에 있어 인증 기능이 처리되는 차량 탑재 장치와 노변장치의 무선구간에서 차량의 이동 속도, 각 장치에서의 암호 기능 처리 또는 이를 관할하는 요금 정산 시스템 등에서의 제한된 처리 속도를 고려한 효율적인 인증 및 세션키 설정 프로토콜을 포함하는 암호 메커니즘과 이들을 이용한 전자지불시스템의 구현 방안을 제시한다. 특히, 국내에서 개발한 인증메커니즘인 EC-KCDSA와 암호화를 위한 SEED 암호 기법을 이용하여 무선망의 하나인 DSRC 환경의 ITS 서비스에 적용이 가능함을 확인할 수 있게 되었다.

■ 중심어 : | 차세대 지능형 교통시스템(ITS) | 단거리전용통신(DSRC) | 안전한 전자지불 | SEED | 인증 |

Abstract

Dedicated Short Range Communications(DSRC) as a prominent communications candidate for Intelligent Transportation Systems(ITS) have been developed to support ITS applications such as value-added information service, e-commerce, electronic toll payment, etc. These various applications associated with electronic payment through unsecure communication channel of DSRC suffer from security threats. To ensure secure payment, we have adopted appropriate cryptographic mechanisms including encipherment, authentication exchange and digital signature. The cryptographic mechanisms require to use cryptographic keys established between two communication entities.

In this paper, we propose a secure electronic payment system which is designed to have some functions for strong authentication, encryption, key agreement, etc. Especially, we adopt domestic developed cryptographic algorithms such as EC-KCDSA and SEED for digital signature and block cipher, respectively. We can show those mechanisms are appropriate for the secure electronic payment system for ITS services under the DSRC wireless environment in aspects of constrained computational resource use and processing speed.

■ keyword : | ITS | DSRC | Secure Payment | SEED | Authentication |

접수번호 : #040707-001
접수일자 : 2004년 7월 7일
심사완료일 : 2004년 10월 6일
교신저자 : 이용권, e-mail : yklee@k1.ac.kr

I. 서 론

지능형 교통시스템(ITS : Intelligent Transportation Systems)은 일반적인 교통시스템의 구성 요소인 도로, 차량 및 신호 체계에 전자, 제어, 정보, 통신 등의 첨단 기술을 융합시킨 차세대 교통시스템이다. ITS의 서비스 영역은 단순한 교차로의 신호제어로부터 위성을 통한 종합적인 차량 관련 정보 제공까지에 이르는 다양하고 방대한 서비스를 지원할 수 있으며 이에 대하여 구미, 일본 등의 선진국에서 많은 실용화 연구를 수행해 오고 있다[2,9,10].

이러한 ITS의 구축은 교통시스템 전체의 효율성과 안전성을 높이는 시도로 '80년대부터 선진국을 중심으로 국가의 정책사업으로 추진하여 왔으며 우리나라도 '90년대 중반부터 건설교통부의 주도하에 ITS 사업을 추진하고 있다[10,11,12].

ITS의 실용화를 위한 검토에서 표준화 그룹들 중 하나인 IEEE P1455와 국내에서는 통신 속도, 장치 가격 등을 고려하여 단거리 전용통신(DSRC : Dedicated Short Range Communications)을 채택하였다[2,12]. 이러한 통신 구조와 관련 표준에서 응용 서비스의 하나인 톨 요금 자동 정산을 위하여 차량 탑재 장치내의 사용자 ID, 장치 번호, 금융 계좌 정보 등 주요 정보들이 노변 장치로 전달되는 경우에 통신 실체들의 정당성을 확인하기 위한 인증 기능이 수행되어야 함을 규정하고 있다[2].

외국의 경우 일본 마츠시다 통신공업주식회사에서는 1997년경 톨 요금 자동 정산 서비스를 위하여 사용자의 강한 인증과 암호화에 RSA와 DES를 각각 이용하여 DSRC 환경에서 실용화하였다[9].

ITS의 여러 서비스 중에서 전자식 지불 방식을 이용하는 톨 요금 정산, 주차 요금 정산, 첨단 교통정보 사용 요금 정산, 전자거래 등에 요구되는 개인의 프라이버시 정보와 노출시 민감한 정보의 상호 교환에 요구되는 인증 처리와 암호통신에 관련된 메커니즘 및 이의 구현을 위한 시스템의 설계에 대하여 논의하고자 한다.

이에 따라 본 논문에서는 DSRC 환경에서 톨 요금 자동 정산 서비스의 구현을 위한 설계로서 국내에서 개발한 인증 메커니즘인 EC-KCDSA(Elliptic Curve - Korean Certificate based Digital Signature Algorithm)을 인증 처리를 위하여 적용하였고 암호화를 위하여 SEED 알고리즘을 적용하였다.

본 논문의 II 장에서는 자동 요금 징수에 따른 전자 지불 시스템의 위험 분석과 대책, III 장에서는 DSRC 운용환경에서의 전자 지불 시스템 구현을 위한 강한 인증과 암호화 메커니즘의 선정과 구현에 대한 국내 개발 보안 알고리즘 활용의 타당성 평가를 하여 DSRC 통신 환경에서 요구되는 차량 속도 80km/h에서의 보안 처리에 소요되는 시간이 설계 기준인 130msec내에 처리할 수 있음을 검증한다.

II. 자동 요금 징수와 전자 지불

기존의 고속도로 주행을 위한 통행 차량은 일단 출발지의 톨게이트를 진입하여 원하는 목적지의 톨게이트를 통과하게 된다. 이러한 경우, 수동식 또는 요금 징수원에 의한 처리시 교통 체증을 유발시켜 민원의 대상 및 에너지의 과소비를 조장하게 된다. 이를 해소하기 위한 대안 중의 하나가 자동 요금 징수이다. 이의 초기 형태에서는 차량 번호판의 인식에 의한 처리 방법이 사용되었으나 최근 무선통신 기술, 암호 기술 및 IC 기술의 발달로 전자 지불의 한 패턴으로 자리 잡고 있다. 또한, 최근 무선 인터넷 기술의 발달로 다양한 형태의 첨단 교통정보의 제공과 전자거래가 가능하여 지고 이에 대한 유료화, 폐쇄 사용자 그룹의 운영 등에 따른 사용 요금의 지불시에 사용자 정보의 접근에 대한 처리가 요구되고 있다. 이와 같은 사용자 정보는 차량 소유자에 대한 것으로 이를 악의의 제 3자에게 노출되어 오용될 경우 많은 악 영향을 줄 것이 자명하다.

그림 1에서와 같이 톨 요금 정산을 위한 전자결재에 참여하는 통신실체는 차량 탑재 장치(OBE: On-Board Equipment)와 노변 장치(RSE: Road Side Equipment)이며 이들은 보안이 취약한 DSRC 무선 구간에서 관련 정보를 송수신 한다. 먼저 사용자의 정보를 접근하여 처리하여야 하는 경우에 대하여 이를 처리하

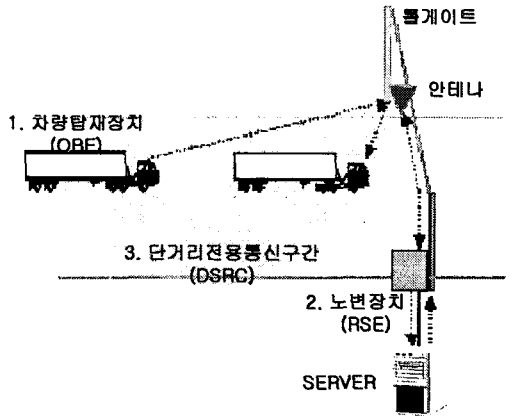


그림 1. DSRC 운용 환경에서 톨 요금 전자 결재 통신 구성도

표 1. DSRC 전자 지불에서의 보안 취약성

구성 요소	위협	취약점			
		인증성	비밀성	무결성	가용성
노변장치	-정당한 장치로의 위장	불법 노변장치를 이용한 차량 탑재 장치 내의 관련 정보 획득	민감한 정보의 노출 및 변조	전달 정보의 훼손	장치 훼손
차량 탑재장치(스마트 카드 이용시 카드 리더 및 카드)	-차량탑재장치의 도난 및 복제 -스마트카드의 분실	-정당한 장치로의 위장 -정당한 사용자로의 위장	민감한 정보의 노출 및 변조	전달 정보의 훼손	장치 훼손
노변장치와 차량 탑재장치간의 무선 구간	-무선 구간에서의 민감한 정보의 획득 또는 변조	노변 장치와 탑재 장치 자체 문제	민감한 정보의 노출 및 변조	전달 정보의 훼손	해당 없음

는 실체인 차량 탑재장치(OBE)와 노변 장치(RSE)간에 사용자 인증이 요구된다. 더욱이, 이러한 통신 실체들은 무선통신이라는 환경 하에서 악의의 공격자로부터 다양한 공격에 노출되어 있어 민감한 정보의 전달시 암호통신도 필요하게 된다.

1. 전자 지불에서의 위험 분석

이러한 무선 통신 환경에서 신뢰적인 통신 실체들간의 안전한 통신을 확보하기 위하여 먼저 안전성이 취약한 기존의 DSRC 방식을 이용하는 탑재장치(OBE)와 노변 장치(RSE)간의 보안 취약점들을 보안 서비스의 관점에서 살펴본다. 여기서, 차량 탑재 장치에는 인증 토큰으로 이용되는 스마트카드와 카드리더 기능을 갖춘 차량 탑재 장치이거나 혹은 이러한 기능을 통합한 차량 탑재 장치, 그리고 이들과 교신하는 노변장치들에 대한 보안 위협과 취약점들을 보안관리 지침에 의거하여 표 1에 정리하였다[1].

먼저 노변 장치의 위협으로는 정당한 관리 기관이 아닌 임의의 자에 의해 설치된 노변 장치를 이용하여 탑재장치로부터 오는 민감한 정보를 갈취하여 오용할 수가 있다는 취약점이 있다. 차량탑재 장치의 경우는 도난 및 복제에 의하여 정당한 사용자로 가장하는 위협에 대한 선의의 사용자 피해가 우려된다. 그리고 안전하지 못한 무선 통신 구간에서는 민감한 정보의 획득 및 변조로 인한 민감한 사용자 정보의 노출에 따른 취약점이 대두된다. 이들 위협과 취약점들을 분석하여 DSRC 전자지불 처리 과정에서 노출될 수 있는 가능성에 대처할 보안 대책을 기술적인 관점에서 암호기법을 적용하여 그 메커니즘들을 실용화하기 위한 방안을 다음 절에서 모색하기로 한다.

2. 보안 대책

DSRC 통신 실체들간의 안전하고 신뢰적인 통신 링크를 통하여 차량 탑재 장치 및 스마트 카드내의 사용자 ID, 장치 고유번호, 다기능 카드의 경우에는 지불 연계 은행계좌번호 등과 같은 공개시 민감한 전자 지불 관련 정보들이 정상적으로 교환될 수 있도록 하여야 한다. 이를 위한 기술적 대안으로 무선 통신 구간 및 통신 실체들간에 암호 기술이 적용됨으로써 이를 해결할 수 있다.

이러한 암호 기법으로 통신 실체들의 정당성을 확인하는 인증 수단으로 약한 인증의 경우는 단순한 패스워드, 강한 인증일 경우는 디지털 서명이 이용될 수 있다. 더욱이, 인증 토큰을 사용하는 경우에는 암호기술을 적용한 스마트카드를 이용할 수 있다. 또한, DSRC를 이용하는 무선 구간에서의 암호 통신을 위하여 먼저 세션키의 설정을 위하여 Diffie-Hellman의 키 교환 메커니즘을 이용하여 공유 세션키를 얻어 대칭키 암호알고리

즘을 적용함으로써 이를 처리할 수 있을 것이다.

III. DSRC 전자 지불 시스템 설계

1. 운용 환경과 설계 요구조건

유료도로를 주행하는 차량이 자신의 전용 차선을 진입하여 톨게이트를 통과하는 과정에서도 거의 60~80km/h의 속력을 유지한다. 이러한 속력에서 통신 실체들 간의 인증과 암호 통신을 하기 위하여 처리 시간에 대한 제약이 있다. 이러한 제약은 DSRC 시스템과 톨 요금 정산 처리 시스템에 있어서의 처리 지연과 차량의 이동 거리에 기인한다. 이와 같은 최대 속력에서 RF 커버리지 유효 거리가 3m일 경우 소요 처리 시간은 0.13sec 이내 이어야 한다[9].

이와 같은 DSRC 시스템의 처리 시간에 대한 제약 조건은 강한 인증시 디지털 서명을 이용하는 경우에 그 처리 시간에 제약을 준다. 이를 해결하기 위하여 노변 장치와 탑재 장치에는 강한 인증을 적용하기 위하여 이산대수문제에 기반을 하는 디지털 서명을 이용하는 경우에 타원곡선 암호 알고리즘을 채택함으로써 안전성과 처리 속도의 개선을 제고할 수 있게 되었다. 이를 위한 대안으로 고려할 수 있는 것으로는 먼저, 강한 인증 메커니즘으로 현재 국내 표준화를 완료하고 국제 표준화가 진행중인 타원곡선 암호(ECC ; Elliptic Curve Cryptography) 버전의 디지털 서명인 EC-KCDSA가 이용 가능하다. 또한, 암호 통신을 위하여 국내 단체 표준화가 완료되고 최근 국제 표준화중인 블록암호인 SEED의 이용이 가능하다[5,6,7,8].

2. 암호 메커니즘의 설계

2.1. 스칼라 곱셈을 이용한 강한 인증

강한 인증을 처리하기 위하여 안전성과 처리 속도의 제약을 개선하기 위하여 타원 곡선 암호를 이용한 구현 방법을 고려해 보기로 한다. 최근, 이에 대한 연구 결과로 S/W 구현일 경우와 H/W 구현일 경우 처리 단위 프레임 당 각각 수십 msec와 수 msec가 걸리는 수준이다[14]. 특히, 처리 속도, 차량 탑재 장치의 H/W 자원, 그리고 스마트카드에서 H/W 자원 등에 대한 제약조건이 있는 경우 H/W의 구현이 필연적이다. 이를 위하여 타원 곡선 암호 처리를 위한 스칼라 곱셈 연산이 요구되며 이의 효율적 구현이 바람직하다.

스칼라 곱셈은 타원 곡선 상의 점들의 합 연산에 의하여 얻어지게 되므로 정수 연산과는 달리 유한체 상에서의 연산에 의거하여 처리된다. 본 논문에서는 스칼라 곱셈의 구현을 위하여 RSA의 1024 비트와 동일한 안전도를 갖는 GF(2^m)상에서 정의된 m=163 비트의 타원곡선 상에 있는 점들에 대하여 적용한다.

표 2. 스칼라 곱셈기의 하드웨어 리소스와 클럭수

소요 클럭수	Double point : $2m^2 + 4m + 5$ Sum of two points : $2m^2 + 4m + 7$ 전체시간(nP) : $(4m^2 + 8m + 12)(m-1)$		
하드웨어 리소스	구성요소	수량	각 Processing Element당 gate수
	Inverter	1	0.8
	Mux(2:1)	2	5
	Flip_flop	10	43
	XOR	1	3.8
	AND	3	3.9

이러한 구현을 위하여 표 2에서 보여진 바와 같이 스칼라 곱셈기를 구성하는 각 processing element의 H/W 자원과 클럭 속도를 결정하는 최장 지연 패스(critical path)에 영향을 주는 MUX, AND 게이트, XOR 게이트에 대하여 곱셈 연산에 소요되는 시간을 고려하여 삼성 STD85 0.5㎛ high density CMOS standard cell library를 이용하여 측정한 결과 9 msec을 얻을 수 있었다[14]. 이와 같은 처리 속도의 ECC 스칼라 곱셈기는 현재 스마트카드에 적용하면 저가의 embedded-micom에 적합한 보안 제품의 운용에 적합한 보안용 ECC 코프로세서로의 활용이 가능하다.

이와 같은, ECC 코프로세서를 이용하여 강한 인증 기법 중 하나인 국내 개발 EC-KCDSA에 적용함에 있어 표 3의 서명 처리의 경우, 서명 생성 과정과 검증 과정에서 각각 1회(서명 생성의 단계 2에서, $K \times G = (x_1, y_1)$ 계산, 여기서 G는 위수 Q를 갖고 순환군(cyclic group)을 생성하는 타원곡선 $E(F(q))$의 한 점)와 2회

표 3. EC-KCDSA를 이용한 서명 처리 과정

서명생성단계	1단계	난수값 K를 {1,2,...,Q-1}에서 생성
	2단계	타원곡선의 점 $K \times G = (x_1, y_1)$를 계산
	3단계	서명의 첫 부분인 해쉬코드 $R = h(x_1)$를 계산
	4단계	메시지의 해쉬코드 $H = h(Z_A \| M)$을 계산
	5단계	중간값 $E = R \oplus H$를 계산하고, 만약 $E \geq Q$이면, $E = E - Q$를 계산
	6단계	서명의 두 번째 부분 $S = X_A \cdot (K - E) \bmod Q$를 계산한다. 만약, S = 0이면 단계 1에서부터 다시 수행한다.
전송단계		메시지 $\{M \| S\}$
서명검증단계	1단계	수신된 서명이 $0 < S' < Q$와 $\|R'\| \leq \|H\|$를 만족하는지 확인
	2단계	메시지의 해쉬코드 H는 $h(Z_A \| M')$을 계산
	3단계	중간값 $E' = R' \oplus H'$를 계산하고, 만약 $E' \geq Q$이면, $E' = E' - Q$를 계산
	4단계	서명자의 공개 검증키 Y_A를 이용하여 타원곡선의 점 $S' \times Y_A + E' \times G = (x_2, y_2)$를 계산
	5단계	$h(x_2) = R'$ 임을 확인하여 검증

(서명 검증의 단계 4에서, 타원곡선의 점 $S' \times Y_A + E' \times G = (x_2, y_2)$ 계산. 여기서, Y_A는 $X_A^* \times G$로 계산되는 서명자 A의 공개 검증키. X_A^*는 $X_A \cdot X_A^* = 1 \bmod Q$와 $0 < X_A^* < Q$를 만족하는 수이며 X_A는 $0 < X_A < Q$를 만족하는 정수로서 랜덤하게 선택된 서명자 A의 개인 서명키)의 스칼라 곱셈 연산이 요구된다[5]. 따라서, 서명 생성 과정에서는 9msec와 검증 과정에서는 18msec가 소요된다. 여기서, 서명 생성과 검증 과정에서 처리되는 연산중 난수 발생과 해쉬 기능을 포함한 여러 계산 과정은 스칼라 곱셈 연산에 비해 연산 처리 속도가 상대적으로 낮으므로 무시한다.

2.2. 암호화

암호통신 및 민감한 저장 데이터의 보호를 위하여 암호 처리가 요구되며 이를 위하여 DES에 비하여 안전하며 처리 속도가 우수한 국내 개발 128비트 키의 블록암호인 SEED를 활용할 수 있겠다. 이것도 역시 H/W 구현이 바람직하며 표 4와 같이 국제표준화가 최종 단계에 있는 128비트 블록 암호인 SEED, AES와 camellia에 대하여 H/W 자원과 최장 지연 시간을 고려한 iterative architecture로 구현하고 128비트의 입력 데이터 블록과 키를 사용하며 1라운드에 1클럭이 소요되도록 한다. 또한, 암호화 처리만을 하도록 하여 ECC 스칼라 곱셈기 구현에 적용한 것과 동일한 삼성 STD85 0.5㎛ high density CMOS standard cell library를 이용하여 약 0.44μsec를 얻을 수 있다[7].

표 4. SEED 하드웨어 복잡도 및 블록당 처리 속도 비교 (Samsung STD85 0.5㎛ high density CMOS standard cell library : 암호화만 적용)

항목 \ 블록 암호	SEED (대한민국)	AES(RIJNDAEL) (미국)	camellia (일본)
Hardware Resource (1 round 당 gates)	3636	5312	3648
Clock Period – critical path(nsec)	27.2	9.7	8.1
전체수행시간(nsec)	435.2	97	145.8
Speed(Mbps)	294.1	1319.6	877.9

2.3. 세션키 설정

암호통신을 위하여 인증된 통신 상대들은 세션키가 요구된다. 운용 환경이 무선 구간이며 처리 시스템들의 자원의 이용과 인터렉션은 최소화되어야 한다는 점에서 검토 대상 키 관리 메커니즘으로는 ISO/IEC 11770-3의 Diffie-Hellman 키 교환 방식중 가장 간단한 키 합의 메커니즘 1을 고려하도록 한다. 이 메커니즘은 각 통신실체의 키 구성 알고리즘을 이용하여 세션 비밀키를 공유하는 메커니즘으로 통신실체들간의 인터렉션이 없어 자원이 한정된 무선통신 구간에서의 트랜잭션 처리 부하를 경감시킬 수 있다는 장점을 갖는다[3].

암호통신을 위하여 비밀 세션키의 설정이 필요한 경우 두 통신 실체간에 인증을 한 후 Diffie-Hellman 키 교환을 다음과 같은 절차에 따라 할 수 있으며 각 통신 실체들이 먼저 자신의 공개키를 사전처리 과정에서 설정(이 경우도 각각 1회의 ECC 스칼라 곱셈 연산이 소요)하여 처리하는 경우는 1회(세션키 설정 단계 c)의 ECC 스칼라 곱셈 연산이 소요되어 9msec가 소요된다.

· 단계 a : n ($nG = O$인 대단히 큰 소수. 여기서, O는 타원곡선상의 무한대점)보다 작은 PRU를 선택하여 사용자측 통신 실체(OBE)의 개인키

로 정한다. 그리고 나서, OBE는 공개키에 해당하는 타원곡선 $Ep(x, y)$상의 점을 계산하여 놓는다: $Y_U = PR_U \times G$

- 단계 b : 통신 실체 CA(RSE를 경유한 CA)도 동일한 방법으로 개인키 PR_{CA}와 이에 상응하는 공개키 $Y_{CA} = PR_{CA} \times G$를 만들어 놓는다.
- 단계 c : 사용자측에서는 비밀 공유키인 $Ks = PR_U \times Y_{CA}$ (= $PR_U \times (PR_{CA} \times G)$)를 만들고 반면에CA는 비밀 공유키인 $Ks = PR_{CA} \times Y_U$ (= $PR_{CA} \times (PR_U \times G)$)를 생성한다.

앞서 설명한 ECC 스칼라 곱셈기와 같은 코프로세서와 SEED의 H/W 구현 기술을 이용하여 그림 2와 같이 설계된 인증 토큰인 스마트카드를 DSRC 환경의 ITS 자동 요금 정산에 적용할 수 있을 것이다. 이러한 경우, 차량 탑재 장치에서 인증 및 암호통신을 처리하는 기능 일체형 장치를 구비하거나 혹은 인증 토큰으로 스마트

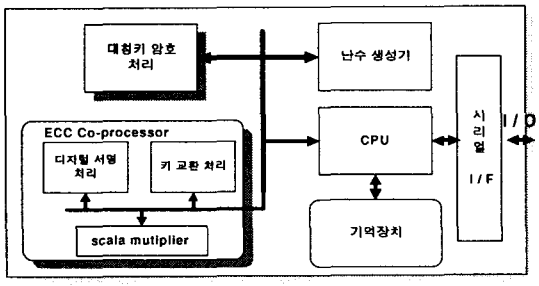


그림 9. ECC Co-processor를 내장한 스마트카드의 구조

카드를 이용한 암호처리 방법을 채택할 수 있을 것이다. 한편, 노변 장치의 경우도 자체에서 암호 처리를 할 것인가 아니면 암호 처리는 요금 자동 정산 시스템에서 하고 단순히 무선 중계용만의 기능을 수행하도록 설계할 수 있다. 이와 같은 장치의 설계는 DSRC 시스템의 전체 처리 시간 제약 조건 등을 고려하여 시행하여야 할 것이다.

3. 제안 전자 지불 시스템의 적용 타당성 평가

본 절에서는 앞에서 설계한 ECC 코프로세서를 내장한 스마트카드를 이용하여 차량탑재 장치(OBE)와 노변장치(RSE)간에 요금 자동 지불을 위한 시스템을 실제 운용환경에서의 적합 여부를 검토하여 보기로 한다. 이에 대한 운용환경은 5.8GHz DSRC 통신으로 1.048Mbps의 전송속도를 유지하며 하나의 전송 프레임은 1kbyte로 한다. 따라서, 1개 프레임의 전송 속도는 7.6msec가 소요된다[13].

먼저, 첫 번째 사례로 단순 인증에 의한 OBE 측에 있는 요금 정산정보를 RSE 측으로 보내는 경우이다. 이러한 정산 정보는 노출시 문제를 일으키지 않으므로 암호화 처리를 하지 않고 단순 인증과 정산정보의 전달을 위하여 OBE 측과 RSE 측간의 커맨드를 처리하는데 소요되는 시간이다. 즉, 단순 인증시 1회 그리고 정산정보의 전달시 정산정보 요구(Get Request), 이의 응신(Get Response), 정산정보의 처리의 수정 요구(Set Request), 이의 처리 결과 응신(Set Response)에 대한 4회의 전송이 요구되어 총 5회의 전송에 38msec가 소요된다.

여기서, OBE 측과 RSE 측에서의 관련 커맨드의 처리는 전송에 걸리는 시간에 비하여 상대적으로 작으므로 무시하기로 한다. 따라서, 요금 자동 정산에 요구되는 처리 소요 시간인 130msec내에 충분히 처리할 수 있다[9].

한편, 두 번째 사례는 스마트카드를 다목적 통합 카드의 기능으로 수행하는 경우 정산정보에 정산 연계 은행 계좌번호 등 민감한 정보가 포함되어 있어 강한 인증을 요구하고 동시에 정산정보의 전송시 암호 통신을 하는 경우를 고려하여 보기로 한다.

그림 3에서 보여주는 강한 인증 및 암호통신에 소요되는 암호 메커니즘으로는 앞 절에서 논의한 EC-KCDSA 디지털 서명, EC Diffie-Hellman 키 교환 및 SEED 암호화 기법이 이용될 수 있다. 이들의 처리 소요시간은 표 5에 보여진다.

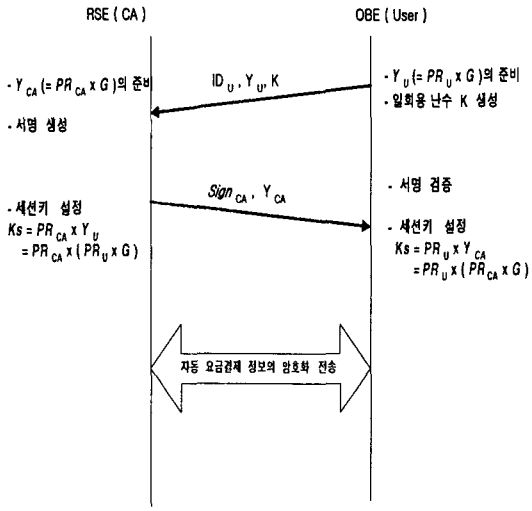


그림 3. DSRC 자동 요금 정산 시스템에서의 강한 인증 및 암호통신의 주요 트랜젝션

표 5. DSRC의 강한 인증 및 암호통신에서의 소요 연산

항목		암호 연산 회수(회)		전송 회수 (회)	비 고
		스칼라 곱셈	암. 복호화		
강한 인증	서명 생성	1		2	
	서명 검증	2			
키 교환		2			인증 과정의 전송에서 각각의 공개키 전달
암호 통신			2x2*	4	* RSE에서 OBE에 내장된 정산정보 요청에 대한 응신(Get Response)과 이의 처리에 대한 정산 결과의 수정 요구(Set Request)시의 2회 전송에 대한 암복호화 처리

즉, 키 교환을 인증 과정에서 처리할 경우에 전송 회수는 인증과정 2회와 정산 정보처리를 위한 통신에 필요한 4회로 총 6회의 전송에 45.6msec가 소요된다.

아울러, 암호기법을 적용하는 연산에서는 5회의 스칼라 곱셈 연산과 4회의 암복호화(1kbyte 프레임 처리) 처리에 각각 45msec와 0.014msec(=4x(0.00044 x1024/128))로 총 45.014 msec가 소요됨을 알 수 있다. 따라서, 강한 인증과 암호 통신에 소요되는 전체 처리시간은 90.614msec가 걸리게 되므로 설계 기준인 130msec 내의 처리가 가능함을 알 수 있다.

IV. 결 론

DSRC의 무선 통신을 이용한 자동 요금 정산을 위한 전자 지불에 있어 사용자의 프라이버시 정보와 민감한 지불 관련 정보들을 차량 탑재 장치 측으로부터 노변 장치를 경유하여 정산처리 시스템으로 가져오게 된다. 이러한 경우, 차량 탑재 장치와 노변 장치간은 무선 통신 구간으로 안전성이 취약하고 이 구간에는 민감한 정보가 교환되고 있어 이를 안전하게 처리하여야 한다.

본 논문에서는 DSRC의 운용 환경의 차량 탑재 장치가 80km/h의 속력으로 진행하는 경우 130msec 이내로 정산에 요구되는 모든 처리를 완료해야 한다는 시간적 제약을 해결하기 위한 방안을 제시하였다. 즉, 기존 외국에서 실용화에 적용된 인증과 암호화를 위한 보안 메커니즘으로 RSA와 DES 대신에 국내에서 개발한 메커니즘인 EC-KCDSA와 SEED를 적용시켜 설계하여 이의 실용화 가능성을 평가한 결과 약 91msec의 처리 시간이 소요됨을 확인함으로써 이를 톨 요금 자동정산을 위한 전자결재에 적용할 수 있음을 보여 주었다.

더욱이, 이들의 구현을 하드웨어로 할 경우 embedded-micom인 스마트카드를 인증 토큰 및 암호 알고리즘 처리 기능을 지원할 수 있도록 타원곡선 암호 처리의 스칼라 곱셈기를 채택함으로써 자동 요금 정산을 위한 인증 기능과 민감한 정보의 암호통신을 위한 트랜잭션 처리에서 시간적 제약 요건에 대한 설계 요구 조건을 만족시킬 수 있음을 확인할 수 있었다.

앞으로, 본 논문에서 간과한 인증과정에서의 해쉬 처리와 난수 생성 그리고 자동 요금정산 처리에 소요되는 관련 커맨드의 처리까지를 고려하여 이들 처리 장치들에서 소요되는 처리 지연 및 이의 처리를 톨플라자의 로컬 서버에서 처리하여야 하는가 혹은 중앙 서버에서 처리를 하여야 하는 것이 효율적인가에 대한 보다 심층적인 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] ISO/IEC JTC1, "Guidelines for Management of Information Technology Security, Part 1, 2

and 3", ISO/IEC TR 13335-1, 2 and 3, 1997.
[2] IEEE, Standard for Message Sets for *Vehicular/ Roadside Communications*, pp. 14 -17, IEEE Std 1455, 1999.
[3] ISO/IEC JTC1/SC27, "Information Technology-Security Techniques-Key Management-Part 3 : Mechanisms using Asymmetric Techniques," ISO/IEC 11770-3, 1999.
[4] ISO/IEC JTC1/SC27, "Information Technology -Security Techniques-Cryptographic techniques based on elliptic curves-Part 3 : Key establishment," ISO/IEC JTC 1/SC 27 N2445, 1999.
[5] ISO/IEC JTC1/SC27, "Information Technology -Security Techniques-Cryptographic Techniques Based on Elliptic Curves-Part 2 : Digital Signatures," ISO/IEC JTC1/SC27 N2443, 1999.
[6] ISO/IEC JTC1/SC27, "National Body Contributions on NP 18033 "Encryption Algorithms" in Response to SC27 N2477," ISO/IEC JTC1/SC27 N2530, 2000.
[7] Korean Experts, "Hardware Implementation Evaluation for ISO/IEC 18033-3," ISO/IEC JTC1/SC27 Quebec meeting contribution, 2003.
[8] ISO/IEC JTC1/SC27, "Information Technology -Security Techniques-Encryption Algorithms -Part 3: Block Ciphers," ISO/IEC JTC1/SC27 N3937, 2004.
[9] http://www.mci.pa nasonic.co.jp/its/english /res_art0.html (to res_art5.html)
[10] 김종혁, "첨단 교통관리 시스템", 정보과학회지, 제16권, 제6호, pp. 5-13, 1998.
[11] 박순철, 이상범, "지능형 및 자동형 고속도로 시스템", 정보과학회지, 제16권, 제6호, pp. 36-42, 1998.
[12] 정성원, "지능형 교통시스템(ITS) 표준화 연구", 정보과학회지, 제16권, 제6호, pp. 43-50, 1998.
[13] 임춘식 외, "ITS 고속 무선패킷통신시스템 개발에 관한 연구, 제 4장 DSRC 응용서비스", 정보통신부, 1999.
[14] 김종만, 정용진, "타원곡선 암호(ECC) 처리를 위한 스칼라 곱셈기", 한국통신학회 하계 종합학술발표회, 한국통신학회, 2000.
[15] http://www.kisa.or.kr/technology/sub1/current _okcs.htm

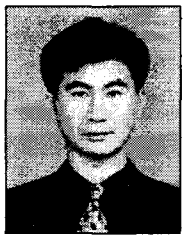
저 자 소 개

장 청 룡(Chung-Ryong Jang) 정회원

- 1980년 : 성균관대학교 전자공학과 졸업(공학사)
- 1986년 : 연세대학교 전자공학과 졸업(공학석사)
- 1994년 : 성균관대학교 정보공학과 졸업(공학박사)
- 1979년~1983년 : ERTI 연구원
- 1984년~1997년 : 한국통신 연구개발본부 선임연구원
- 1997년~현재 : 경동대학교 컴퓨터미디어학부 부교수

<관심분야> : 통신망보호, 블록암호, 보안제품 시험

이 용 권(Yong-Kwon Lee) 정회원



- 1984년 : 강원대학교 통계학과 졸업(이학사)
- 1999년 : 강원대학교 전자계산학과 졸업(이학석사)
- 2003년 : 강원대학교 전자계산학과 박사수료
- 1984년~1989년 : KCC S/W 개발팀장
- 1989년~1997년 : Postech S/W 개발팀장
- 1997년~2001년 : 동우대학 전자계산학과 조교수
- 2001년~현재 : 경동대학교 컴퓨터미디어학부 조교수

<관심분야> : 정보보호, 데이터베이스