VANET 환경에서의 익명성을 보장하는 요금 결제 프로토콜

준회원 나 진 한*, 종신회원 박 영 호**°, 문 상 재***

Anonymity Guaranteed Payment Protocol in Vehicular Ad Hoc Network Environments

JinHan Na* *Associate Member*, YoungHo Park**°, SangJae Moon*** *Lifelong Members*

요 약

VANET 환경에서 서비스가 안전하게 활용되기 위해서는 보안성 확보가 필수적이다. 본 논문에서는 VANET 환경에서 사용자의 익명성을 보장하는 요금 결제 프로토콜을 제안한다. 제안한 프로토콜은 후불 카드를 결제 수단으로 사용하도록 설계하고 사전 등록 과정과 갱신 과정, 요금 결제 과정으로 진행된다. 사전 등록 과정과 갱신 과정을 통해 사용자의 익명성을 제공하고 요금 결제 시 이동 차량에서의 연산 부하를 줄여 빠른 연산 처리가 제공된다.

Key Words : VANET, Payment Protocol, Anonymity, Encryption, Computational Load

ABSTRACT

Security is essential to make use of application service securely in VANET environments. This paper proposes payment protocol which supports user's anonymity. The proposed protocol is designed to use a charge card as a payment method and performs pre-registration, renewal and payment phase. The user's anonymity and disclosure of charge card information is protected through the pre-registration and renewal phase, and also fast computing operation is supported by minimizing the computational load on vehicles.

I. 서 론

전 세계 주요 선진 국가는 교통 물류 분야에서 교통 정보 수집 기술 및 응용한 서비스의 필요성이 제기되고 있다. 이러한 서비스가 가능하기 위해서는 인프라의 확충이 필수적이며 차량 통신에 관한 연구도 중요하며 VANET(vehicular ad hoc network)를 통해 차량 간 통신과 차량과 노변 장치간의 통신에 대한 연구가 활발하게 진행되고 있다.

국내에서는 VANET시스템 개발을 통해 기존 교통 정보 수집체계에서 사용하던 수동적인 방식인 CCTV, 루프 검지기 등을 통해서 수집한 데이터를 가공하여 교통 신호 제어 또는 통제하는 단순 정보 활용 방식에서 벗어나 이제는 교통 시설이 정보 통신의 대상이 되었고, 직접적으로 교통 자료를 제공하고 제공 받는 주체가 되는 인프라를 구축하는 것이라 할 수 있다. VANET은 모든 교통 대상 사물에 센서를 부착하고 센서를 부착한 노드 간 유·무선 통신 프로토콜을 통해 자동으로 네트워크를 구성하면서 상호 노드 간에 상태 정보와 위치 정보를

※ 본 연구는 국토해양부 교통체계효율화사업의 연구비 지원(06-교통핵심-A01-01)에 의해 수행되었습니다.
* 경북대학교 전자전기컴퓨터학부 (geneflag@gmail.com), ** 경북대학교 산업전자전기공학부(parkyh@knu.ac.kr)(° : 교신저자)
*** 경북대학교 전자공학부 (sjmoon@ee.knu.ac.kr)
논문번호 : KICS2010-03-141, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 5월 10일

주고받을 수 있는 최첨단의 네트워킹 기술로 지능형 차량에 무선 통신 기술을 지원하기 위하여 IEEE802.11p[1],[2] 기반의 기술을 사용하고 있다.[2]-[4]

VANET 환경에서 제공되는 서비스에 대한 요금 결제에 정보 보호 기술이 제공되지 않으면 요금 결제에 관련된 보안 위협이 발생할 수 있고 운전자의 프라이버시를 침해할 수 있으므로 보안성 확보가 필수적으로 해결되어야 한다. VANET은 전파를 통한 무선 환경으로 제한된 대역폭을 사용해야 하며 이동 단말기의 계산 능력의 한계, 이동성과 다양한 부가 서비스 기능의 제공 등 많은 제약 요인과 특수성이 고려되어야 한다. 또한 이동 차량과 노변 장치 간의 통신뿐만 아니라 가입자와 부가 서비스 제공자간의 통신도 고려해야 하므로 기존의 보안 프로토콜 및 알고리즘을 그대로 사용할 수 없다. 따라서 무선 환경 및 차량 단말기 처리 능력, 그리고 사용자와 부가 서비스 제공자간의 통신을 고려한 보안 프로토콜 개발이 이루어져야 한다.[4]-[6]

현재 관련 연구 내용으로는 국내 고속도로 요금 결제 체계인 하이패스 요금 결제 프로토콜[7], VANET 환경에서 사용자를 인증하고 요금 결제를 제공하는 KCM-VAN 방식[9] 등이 있다. 하이패스 요금 결재 프로토콜은 익명성이 제공되지 않으며 KCM-VAN 방식은 사전 등록 과정을 통해 임시 ID를 발급 받아 요금 결제에 사용하여 사용자의 익명성을 보장하고 있지만 임시 ID의 지속적인 사용으로 인해 운전자의 노출이 가능하다는 단점이 있다.

본 논문에서는 VANET 환경에서 익명성을 보장하는 요금 결제 프로토콜을 제안한다. 제안한 프로토콜은 사전 등록 과정, 갱신 과정, 요금 결제 과정으로 구분되며 사전 등록 과정과 갱신 과정을 통해 사용자 익명 ID와 카드 인증 값 생성 및 주기적인 갱신을 진행한다. 그리고 요금 결제 과정에서 진/출입 노변 장치 정보를 통해 결제 요금을 확인하고 센터에서 요금에 대한 선 결제가 이루어지고 차후 사용자의 금융 기관에 선 결제된 요금에 대해 사용자의 카드 인증 값을 통해 후 결제 되게 된다. 본 프로토콜은 후불 카드 형태로 설계하여 사용이 편리하며 결제 시 사용자의 익명성과 후불 카드 정보의 유출을 방지하며 이동 차량에서의 연산 부하를 최소로 하여 빠른 이동이 제공되도록 제안한다.

Ⅱ. 기존 연구

요금 결제 프로토콜은 VANET 환경에서 제공하는 서비스들에 대한 합법적인 사용자가 서비스 이용에 따른 요금 결제를 원활하게 진행하도록 하는 것을 목적으로 한다. 먼저 VANET 응용 서비스에 대해 알아보면 차량 안전 주행 관련 서비스, 효율적인 교통 체계 구축을 위한 서비스, 사용자 편의 서비스로 구분할 수 있다. 차량 안전에 관련된 서비스는 차량 충돌 경보나 도로 노면상태 제공, 차량 간 협력 운전 등의 서비스를 통해 차량 운전 시 운전자의 안전을 향상시키게 된다. 효율적인 교통 체계 구축을 위한 서비스로는 실시간 교통 정보를 운전자에 제공, 능동적인 교차로 신호체계 구축 등을 통해 도로 지·정체 해소를 통해 효율적인 교통 체계를 구축 할 수 있을 것이다. 마지막 사용자 편의 서비스는 차량 내에서 인터넷 서비스 제공이나 주차 요금, 통행료 징수와 같은 요금 결제를 지원하여 운전자에 대한 편의 서비스를 제공되게 된다.

이러한 VANET 응용 서비스 환경에서 요금 결제에 대한 정보 보호 기술이 제공되지 않으면 불법적인 사용자에 의한 보안 위협이 발생할 수 있으며 이에 관련된 연구가 국내외적으로 활발하게 진행되고 있다.

2.1 하이패스 결제 프로토콜

하이패스 결제 프로토콜은 톨게이트 지/정체 및 요금 지불 수단의 다양화를 통해 사용자의 편의성과 효율적인 통행료 관리 체계를 구축하기 위한 요금 결제 프로토콜[7]이다. 사용자의 결제카드(IEP), 구매 단말기(PDA), 고속 도로 톨게이트 상에 설치된 서비스 제공자 보안모듈(PSAM)간의 통신을 통해 사용자의 도로 이용요금을 카드에서 서비스 제공자 보안 모듈로 전자적 가치를 결제하게 된다.

PDA에서 초기화 명령을 받은 IEP는 거래금액 초기화와 난수(R_{IEP}) 생성, 이전 거래 일련번호(NT_{IEP})를 증가는 등의 준비 과정을 마치고 세션 키 생성을 통해 PSAM와 동기화에 필요한 내용을 전송해 주게 된다. PSAM에서는 IEP로부터 받은 내용을 확인하고 먼저 로드키를 생성한다. 생성된 로드키를 통해 IEP와 동일한 세션 키를 생성[8]하고 서명을 검증하여 동일한 세션 키가 생성되었는지 확인하고 응답을 IEP로 보내면 IEP에서는 요금 결제를 위해 금액 조건을 확인하고 결제 금액에 대한 지불 정보를 작성하고 그 내용을 세션 키로 서명하여 다시 PSAM으로 전송한다. PSAM은 전송받은 지불 정보를 통해 사용자의 전자적 가치를 도로공사 쪽으로 이전하게 되고 지불 완료 정보를 기록한다.

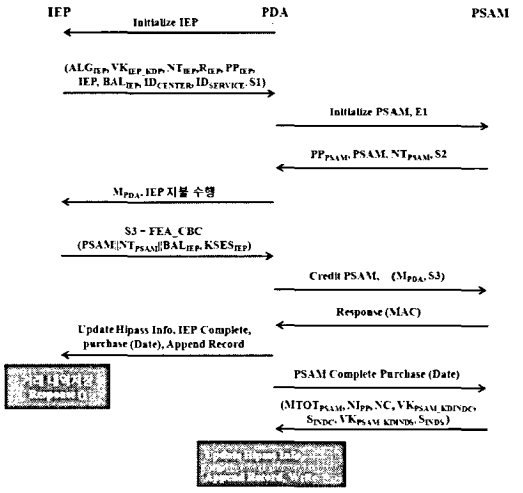


그림 1. 하이패스 결제 프로토콜

PDA로부터 결제 완료 명령을 받으면 IEP에서는 결제가 이루어지 내용에 대해 데이터를 생성하고 응답을 보내게 되면 PDA에서 PSAM으로 결제 완료 명령을 보내고 PSAM은 결제 내역에 대한 서명을 생성한다. 이 과정이 완료되면 PDA에서는 hipass 정보를 기록하여 과정을 마무리 되며 과정은 그림 1과 같다.

국내 고속도로 요금 결제 체계인 하이패스의 경우 결제 과정에서 사용자 ID가 노출되어 사용자의 프라이버시를 보장 할 수 없고 결제 카드 정보의 유출 가능성이 있는 문제점을 가지고 있다.

2.2 KCM-VAN (kiosk centric payment protocol for VANETs)

VANET 환경에서 고객이 인증을 목적으로 직접적으로 고객의 거래 은행과의 통신 할 수 없는 시나리오로 진행되는 결제 프로토콜(KCM-VAN)[9]을 제안하고 있다.

KCM-VAN 방식은 각 개체 간의 메시지 교환 과정에 별도의 암/복호화 과정이 진행하기 위하여 제안한 암호화 방식[10]을 사용하며 시스템 초기화 및 사용자 등록 과정과 결제 과정으로 진행된다. 시스템 초기화 및 사용자 등록 과정은 공개키 연산[10],[11]을 통해하고 레지스터에 저장/클라이언트의 금융기관에 알리면 운전자의 임시ID를 발급하게 된다.

운전자는 서비스 제공자에게 거래 요청 메시지를 보내면 응답 메시지를 암호화[10]하여 전송한다. 운전자는 거래 요청에 대한 요금을 지불하기 위해 서비스 제공자에게 전송하는 암호화된 요금 결제 메시

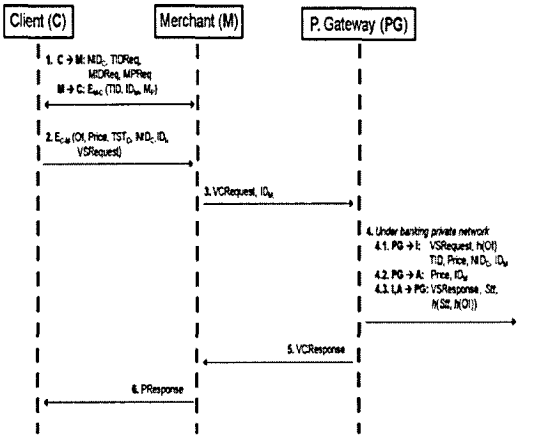


그림 2. KCM-VAN 방식

지내에 운전자의 거래 은행에 전송할 결제 요청 메시지로 암호화(VSRequest)하여 서비스 제공자에게 전송한다. 서비스 제공자는 운전자로부터 전송받은 요금 결제 메시지를 복호화하여 내용을 확인하고 결제 정보, 타임스탬프 정보를 확인하고 서비스 제공자 생성 타임스탬프로 교체하여 메시지를 암호화(VCRequest)하여 지불 대행 기관으로 요청 메시지를 전송한다.

지불 대행 기관에서는 서비스 제공자로부터 받은 요청메시지를 복호화하여 운전자의 거래 은행과 서비스 제공자의 거래 은행사이의 거래를 중계하게 된다. 복호화된 메시지내의 운전자의 거래 요청 메시지(VSRequest)를 거래 은행으로 전송하면 운전자의 거래 은행은 거래 요청 메시지를 복호화하여 요청 금액만큼을 지불 대행기관으로 보내주면 지불 대행 기관은 서비스 제공자 거래 은행으로 요청 금액을 이체시켜 요금 지불이 이루어지게 하고 결제 내역 암호화하여 운전자에게 전송하는데 전송 과정에서 지불 대행 기관과 서비스 제공자의 결제 내역 확인이 이루어지면 최종적으로 운전자에게 결제 내역이 전송되고 결제가 종료되게 된다.

KCM-VAN 방식의 경우 사전 등록 과정을 통해 임시 ID를 발급 받아 요금 결제에 사용하여 사용자의 익명성을 보장하고 있지만 임시 ID의 지속적인 사용으로 인해 운전자의 노출이 가능해지므로 익명성 보장이 힘들어지는 문제점을 가지게 된다.

Ⅲ. 요금 결제 프로토콜

제안하는 요금 결제 프로토콜은 사전 등록 과정,

갱신 과정, 요금 결재 과정을 통해 VANET 환경에서 차량에 대한 요금 결제 서비스를 제공하게 된다. 먼저 사전 등록 과정은 사용자가 은행으로부터 발급 받은 후불 카드를 센터에 사전 등록하는 과정을 통해 차량 운전자의 익명 ID와 카드 인증 값을 생성하고 요금 결제 단계에 사용한다. 그리고 갱신 과정을 통해 사전 등록 과정에서 생성된 사용자의 익명 ID와 카드 인증 값의 갱신이 이루어지는데 사용자의 요청이나 일정 기간마다 익명 ID와 카드 인증 값을 갱신하여 요금 결제 과정에서의 사용자의 익명성과 프라이버시를 보장하게 된다. 마지막으로 요금 결제 과정은 도로상에서 주행 중인 차량이 도로에 설치된 노변 장치, 센터와 통신을 통해 도로 요금을 산정하고 사용자의 결제 요청에 따라 요금에 대한 선 결제가 이루어진다. 센터는 사용자의 거래 금융 기관과 통신 과정에서 결제 요금의 후 지불을 요청하면 카드 인증 값을 통해 후불 카드를 확인하고 요청 금액에 만큼 결제하여 요금 결제 과정을 마치게 된다.

제안된 요금 결제 프로토콜의 수행 환경은 다음과 같다.

- 사용자는 은행에서 후불 카드를 발급
- 은행과 사용자간에 대칭키 공유
- 결제 금액 확인을 위한 노변 장치 정보는 각 노변 장치의 공개키로 암호화하여 전송
- 사용자와 센터 간 요금 결제를 위한 세션 키는 금융 IC 표준 내용을 따름

제안 프로토콜에서 사용되는 표기는 표 1과 같다.

표 1. 표기와 그 의미

표 기	의 미
ID_A	A의 identity
VID_A	A의 차량 identity
PID_A	A의 익명 identity
CI_A	A의 후불카드 정보
K_A	A의 비밀 키
K_{AB}	user와 bank사이에 공유된 대칭 키
KDP_A	A의 카드 로드 키
K_S	요금 결제 세션 키
$K_{\hat{S}}$	통신 세션 키
t_A	A의 타임스탬프
R_A	A의 난수
NT_A	A의 거래 일련 번호
Stt	거래 상태
$AUTH_A$	A의 카드 인증 값
GI, EI	진입/진출 노변 장치 정보 $GI=[PID_A, RSU_i\|\|t_i]_{RSU_i}$ $EI=[PID_A, RSU_j\|\|t_j]_{RSU_j}$
OI	결제 정보

3.1 요금 결제 시나리오

요금 결제 과정은 VANET 환경에서 정상 등록된 차량이 도로 주행 시 노변 장치, 센터, 금융 기관과의 통신을 통해 요금이 결제되는 시나리오로 그림 3과 같다. 제안하는 요금 결제 프로토콜은 사전 등록 과정, 갱신 과정, 요금 결제 과정을 진행된다.

사전 등록 과정과 갱신 과정을 통해 사용자의 익명 ID와 후불 카드에 대한 카드 인증 값의 생성 및 갱신이 이루어지며 요금 결제 과정에서 차량에 대한 요금 결제는 Step1. 차량 진입, Step2. 요금 결제을 통해 차량 결제 요금 산정 및 결제 요청에 따라 산정 요금의 선 결제가 진행된다. 그리고 Step3. 금융기관 결제 에서는 선 결제한 사용자의 요금에 대해 사용자의 금융기관에 요청하여 요금에 대한 후 지불하고 요금 결제를 종료하게 된다.

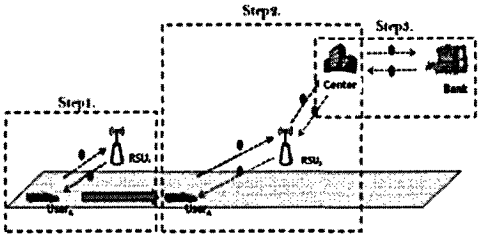


그림 3. VANET 환경에서의 요금 결제 시나리오

3.2 사전 등록 과정

본 논문에서의 후불 카드에 대한 사전 등록 과정으로 요금 결제 과정 이전 사용자가 은행으로부터 발급 받은 후불 카드를 센터에 등록하여 요금 결제 과정에서 사용되는 사용자의 익명 ID와 후불카드 등록에 대한 카드 인증 값을 발급받아 실제 결제 거래에서 사용자의 익명성 및 프라이버시 보장과 안전한 요금 결제를 지원한다. 사전 등록 과정은 그림 4와 같다.

사용자 A는 후불 카드 발급 은행을 방문하여 후불 카드를 센터에 등록한다.

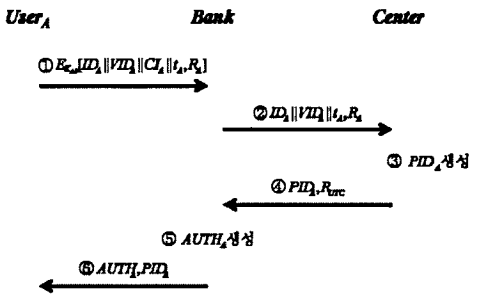


그림 4. 사전 등록 과정

① 사용자 ID, 차량 ID, 후불 카드 정보, 등록 시간, 사용자 난수를 카드 발급 시 공유된 대칭키로 암호화하여 전송한다.

② 은행은 전송 받은 데이터에서 사용자의 ID와 발급된 후불 카드 정보가 일치하는지 확인하고 카드 정보를 저장하고, 센터 간에 형성된 secure channel을 통해 후불 카드 정보를 제외한 나머지 데이터들을 전송한다.

③ 요금 결제에 사용할 사용자의 익명 ID는 식 1과 같이 사용자 ID, 차량 ID, 타임스탬프, 사용자 난수와 센터 난수를 X-OR하여 생성하게 된다.

$$PID_A = [ID_A \| VID_A \| t_A \| R_A] \oplus R_{UTC} \quad (1)$$

④ 생성된 익명 ID와 센터 생성 난수를 은행으로 전송한다.

⑤ 은행에서는 센터에서 생성한 익명 ID와 난수, 후불 카드 정보로 요금 결제에 사용할 은행과 사용자가 공유하고 있는 대칭키로 암호화한 카드 인증 값을 생성하고 식 2와 같다.

$$AUTH_A = E_{K_{AB}}[H[CI_A \| R_{UTC}] \oplus PID_A, R_{UTC}] \quad (2)$$

⑥ 은행은 사용자의 익명 ID와 카드 인증 값을 사용자에게 전송하고 사용자는 카드 인증 값의 복호화를 통해 익명 ID와의 일치하고 사전 등록 과정을 마치게 된다. 위와 같이 결제 카드에 대한 사전 등록 과정을 통해 요금 결제에서의 사용자의 익명성과 프라이버시를 보장하게 된다.

3.3 갱신 과정

갱신 과정은 사전 등록 과정에서 발급된 익명 ID와 카드 인증 값에 대해 사용자의 요청이나 일정 주기마다 갱신한다.

시간 경과에 따라 사용자의 익명 ID의 노출되는 문제점을 해결하여 지속적인 익명성을 제공하며 카드 인증 값 갱신하게 되며 그 과정은 그림 5와 같다.

① 사용자의 갱신 요청 시 기존 익명 ID와 갱신에 필요한 난수, 타임스탬프, 기존 카드 인증 값을 통신 세션 키로 암호화하여 센터로 전송한다.

② 센터는 전송받은 데이터를 세션 키로 복호화하여 기존 익명 ID를 통해 사용자ID, 차량ID를 확인한다. 그리고 식 1의 난수와 타임스탬프를 제거하고 사용자로 부터 전송받은 난수, 타임스탬프와 센터에서 새로운 난수를 생성하여 식 3과 같이 익명 ID를 갱신한다.

$$PID'_A = [ID_A \| VID_A \| t'_A \| R'_A] \oplus R'_{UTC} \quad (3)$$

③ 센터는 익명 ID 갱신에 따른 카드 인증 값 갱신을 위해 센터와 사용자의 ID, 갱신된 익명 ID, 센터에서 생성한 난수, 기존 카드 인증 값을 은행의 공개키로 암호화하여 전송한다.

④ 은행은 센터로부터 전송 받은 데이터를 은행의 비밀 키로 복호화 하여 사용자ID에 해당하는 대칭 키로 카드 인증 값이 복호화 되는지 확인한다. 이 과정이 확인되면 카드 인증 값의 기존 익명 ID, 난수를 제거하고 센터에서 전송한 갱신된 익명 ID와 난수로 식 4와 같은 갱신된 카드 인증 값을 생성한다.

$$AUTH'_A = E_{K_{AB}}[H[CI_A \| R'_A] \oplus PID'_A, R'_{UTC}] \quad (4)$$

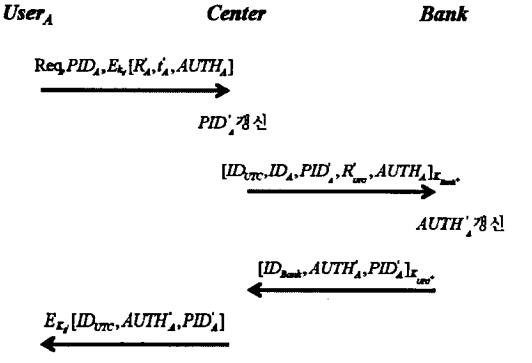


그림 5. 갱신 과정

⑤ 은행은 갱신된 익명 ID와 카드 인증 값을 은행ID와 함께 센터의 공개키로 암호화하여 전송한다.

⑥ 센터는 은행 전송 데이터를 센터의 비밀 키로 복호화 하고 사용자와의 통신 세션 키로 암호화하여 사용자에게 전송한다. 사용자는 센터에서 전송된 데이터를 복호화 하여 갱신된 익명 ID와 카드 인증 값에 대한 검증과정을 거쳐 갱신된 익명 ID와 카드 인증 값의 이상 유무를 확인하고 갱신 과정을 마친다.

위와 같이 결제 카드에 대한 갱신 과정을 사용자의 요청이나 일정 기간마다 온라인상으로 갱신하여 요금 결제에서의 사용자의 익명성 보장 및 후불 카드 정보의 유출을 방지하여 사용자의 프라이버시를 보장하게 된다.

3.4 요금 결제 과정

3.4.1 차량 진입

차량 진입 과정은 그림 3의 Step1에 해당하는 과정으로 차량이 VANET 환경의 도로상의 진입 지점의 노변 장치와 통신 과정으로 그림 6과 같이 진행된다.

사용자의 익명 ID와 진입 노변장치 정보 요청 메시지를 전송하면 노변장치에서는 식 5와 같은 진입 노변 장치 정보 응답 메시지를 사용자에게 전송한다.

$$GI = [PID_A, RSU_i \| t_i]_{RSU_i} \quad (5)$$

사용자는 진입 노변장치 정보를 저장하고 요금 결제 과정에 요금 결제 요청과 함께 전송한다.

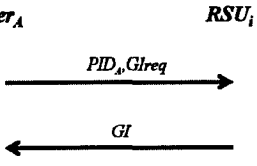


그림 6. 차량 진입 과정

3.4.2 요금 결제

요금 결제과정은 그림 3의 Step2.에 해당하며 VANET 환경에 진출하는 차량이 노변장치와 센터와 통신하여 요금을 결제하는 과정으로 그림 7과 같다.

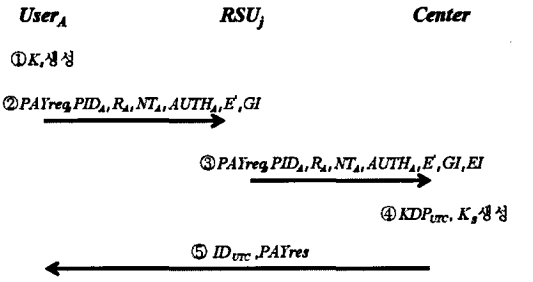


그림 7. 요금 결제 과정

① 사용자가 요금 결제를 위해 세션 키를 생성하는 과정으로 난수, 거래일련 번호를 생성한다. 금융IC표준 세션 키 생성 방법을 사용하며 식 6과 같다.

$$K_S = FEA\_CBC[NT_A \| R_A, KDP_A] \quad (6)$$

② 사용자가 요금 결제를 위해 요금 결제 요청 메시지와 사용자의 익명 ID, 난수, 거래 일련 번호, 카드 인증 값을 전송하게 되는데 세션 키로 앞의 전송 데이터에 대한 해쉬 값을 생성하여 출구 노변장치로 전송한다. 이때 해쉬 값은 식 7과 같다.

$$E' = H_{K_S}[PID_A, R_A, NT_A, AUTH_A, GI] \quad (7)$$

③ 출구 노변장치는 사용자 전송 데이터에 출구 노변장치 정보를 포함하여 센터로 전송하게 된다.

④ 결제 요청을 받은 센터는 사용자와 동일한 세션 키를 생성하기 위한 센터 로드키를 생성하는데 센터ID와 전송 받은 익명 ID, 센터 마스터키를 사용하여 식 8과 같이 센터 로드키[7],[8]를 생성한다.

$$KDP_{UTC} = 3DES\_CBC[ID_{UTC} \| PID_A, KMP_{UTC}] \quad (8)$$

생성된 센터 로드키를 이용하여 세션 키를 생성하는데 사용자로부터 전송받은 난수와 거래 일련번호, 센터 로드키를 사용하여 식9의 세션 키를 생성한다.

$$K_S = FEA\_CBC[NT_A \| R_A, KDP_{UTC}] \quad (9)$$

이때 생성된 세션 키를 통해 해쉬 값을 검증하여 통신상의 데이터의 무결성을 확인한다. 일치 여부가 확인되면 전송된 진입 노변장치 정보와 출구 노변장치 정보를 통해 사용자의 결제 요금을 산정하고 선 결제하게 된다.

⑤ 센터는 산정된 요금에 대해 세션 키로 암호화한 식 10의 선 결제 내역을 사용자에게 전송하여 결제를 종료한다.

$$PAYres = E_{K_S}[PID_A, ID_{UTC}, price] \quad (10)$$

3.4.3 금융기관 결제

금융기관 결제 과정은 그림 3의 Step3.에 해당하는 과정으로 차량 요금 결제를 승인한 센터와 사용자의 거래 은행과의 통신 과정이다.

결제 요청에 대해 선 결제된 내역에 대해 카드 인증 값을 통해 결제 요금을 거래은행에서 센터로 요금을 지불하는 과정으로 그림 8과 같이 진행된다.

센터는 사용자의 거래 은행으로 센터ID, 사용자 익명 ID, 요금, 거래 일련번호, 카드 인증 값를 공개키 방식으로 암호화하여 전송한다. 거래 은행은 사용자와 공유된 대칭키로 암호화된 카드 인증 값을 복호화하고 센터가 결제 요청한 사용자 익명 ID와 일치하는지 확인한다. 확인이 이루어지면 요금에 대한 후 지불이 이루어지고 사용자의 지불 카드 내역으로 저장하게 된다. 후 지불이 정상적으로 이루어지면 은행은 은행ID, 결제요청 사용자의 익명 ID,

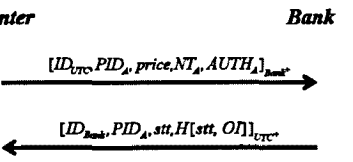


그림 8. 금융기관 결제 과정

거래 상태와 결제 정보와 거래 상태를 해쉬한 값을 은행의 공개키로 암호화하여 전송한다. 센터에서는 최종적으로 사용자의 결제내역을 확인하고 거래를 종료한다.

Ⅳ. 분 석

4.1 연산량 분석

제안하는 프로토콜은 사전 등록 과정, 요금 결제 과정으로 진행되고 연산량은 표 2와 같다. 사전 등록 과정은 요금 결제 과정에서 사용자의 익명을 위한 익명 ID생성과 후불 카드 인증 값을 생성하기 위해 사용자는 필요한 정보를 전송하고 확인하기 위해 암/복호화와 해쉬, X-OR 연산이 진행된다. 요금 결제 과정은 차량 진입, 요금 결제, 금융기관 결제로 구분되는데 사용자는 센터와 세션 키 설정을 위한 FEA_CBC 연산과 전송 데이터의 무결성을 보장하기 위한 해쉬 연산, 선 결 제 내역 확인을 위한 복호화가 진행된다.

요금결제 시 제안한 프로토콜과 하이패스 요금결재 프로토콜은 대칭키 방식을 사용하며 KCM-VAN은 공개키 방식을 사용하고 있다. 또한, 요금결제 시 하이패스 요금결재 프로토콜은 그림 1과 같이

표 2. 연산량 분석

		Pass 수	*User*	$RSU_{i,j}$	*Center*	*Bank*
사전 등록 과정		4회	암/복호화1회 해쉬 연산 1회 X-OR 1회		암/복호화1회 X-OR 1회	암/복호화2회 해쉬 연산 1회 X-OR 1회
갱신 과정		4회	암호화1회 복호화2회 해쉬 연산 1회 X-OR 2회		암/복호화1회 X-OR 2회	암/복호화2회 해쉬 연산 1회 X-OR 1회
요금 결제 과정	차량 진입	2회		서명 생성 1회		
	요금 결제	3회	FEA_CBC 1회 복호화 1회 해쉬 연산 1회	서명 생성 1회	서명 검증 1회 3DES_CBC 1회 암호화 1회	
	금융기관 결제	2회			암/복호화 1회 해쉬 연산 2회	암/복호화 1회 해쉬 연산 2회

복잡한(11번) 데이터 전송 과정이 필요한 반면 제안한 프로토콜은 그림 7과 같이 간단한(3번) 데이터 전송과정으로 이루어져 있다. 제안한 프로토콜은 표 2와 같이 차량에서의 연산량이 소요되며 고속 이동 환경인 VANET 환경에서 요금결제가 실시간 처리 가능하도록 하였다.

4.2 안전성 분석

제안하는 요금 결제 프로토콜에서 안전성 분석은 다음과 같다.

4.2.1 내부자 공격

제안하는 요금 결제 프로토콜은 내부자에 의한 위장 공격이나 메시지 변조 공격에 대처할 수 있다. 위장 공격의 경우 공격자가 노출된 익명 ID를 사용하여 요금 결제를 시도하는 경우 요금 결제를 위한 세션 키를 생성하지 못하므로 공격이 되지 않으며 노출된 카드 인증 값과 타인의 익명 ID를 통해 요금 결제를 시도 하여도 금융기관 결제 단계에서 카드 인증 값의 익명 ID와 일치하지 않게 되므로 공격자의 공격에 대처할 수 있다. 그리고 메시지 변조 공격에 대해서는 RSU 정보는 각 RSU의 비밀키로 서명되어 센터에서 확인하고 결제 요금을 산정하기 때문에 공격자의 변조 공격을 막을 수 있고 갱신 과정에서 VANET 환경에서 센터에서 ECIES(elliptic curve integrated encryption scheme)통해 생성, 분배한 통신 세션 키를 통해 필요한 데이터를 전송하고 결제 요청 메시지에 대해서는 요금 결제 단계에서 생성한 세션 키로 해쉬 연산하여 전송되므로 메시지에 대한 무결성을 보장하고 공격자의 변조 공격을 막을 수 있게 된다.

4.2.2 재전송 공격

재전송 공격은 가장 가능성이 높은 공격 중 하나이며 제안한 프로토콜에서는 재전송 공격을 방지하기 위하여 시간과 난수를 사용하였다. 결제 내용을 재전송하여 결제 시도할 경우 거래 일련번호와 난수를 통해 재전송된 메시지를 확인할 수 있기 때문에 공격자의 재전송 공격을 방지 할 수 있게 된다.

4.2.3 사용자 프라이버시 보장

제안한 프로토콜은 사전 등록 과정에서 익명 ID를 생성하여 요금 결제 과정에서 사용자의 익명성을 보장하고 카드 인증 값 생성을 통해 사용자의 후불 카드 정보의 유출을 차단한다. 이를 통해 사용자의 노출을 방지함으로서 프라이버시를 보장하게 된다. 만약 만일의 사고 발생의 경우 상위 기관에서 익명 ID의 확인을 통해 책임 유무를 판단하게 된다. 하지만 한번 생성된 익명 ID를 계속 사용하게 되면 사용자의 익명성 보장이 힘들어지게 되므로 주기적인 갱신을 통해 운전자의 익명성을 보장하도록 한다.

V. 결 론

VANET 환경에서 제공되는 서비스가 안전하고 신뢰성 있게 제공되기 위해서는 보안성 확보가 필수적으로 해결되어야 한다. 본 논문에서는 VANET 환경에서 익명성을 보장하는 요금 결제 프로토콜을 제안하였다. 제안한 요금결제 프로토콜은 후불 카드를 결제 수단으로 사용하도록 설계하였다. 사전 등록 과정과 갱신 과정을 통해 요금 결제 과정에서 사용되는 사용자의 익명 ID와 카드 인증 값의 생성 및 갱신을 통해 사용자에 대한 익명성 제공하고 사용자와 은행사이에 공유된 대칭키로 암호화된 카드 인증 값을 요금 결제 과정에 사용하여 후불 카드 정보의 유출을 방지한다. 그리고 갱신 과정과 요금 결제 과정을 VANET 환경의 도로상에서 온라인으로 진행하여 사용자의 편의성을 보장하고 요금 결제 과정에서 사용자의 연산 부하를 최소화함으로서 빠른 이동성과 자원의 제약을 갖는 VANET 환경에 적합하도록 이동 차량에서 최소의 연산 부하를 갖도록 설계하였다. 추후 연구 방향으로 사용자의 편의성 및 안전성을 고려한 갱신 과정의 갱신 주기 및 방법에 대한 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] IEEE1609.2, Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE standards, 2006.

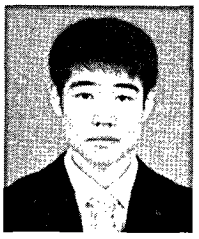
[2] IEEE802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[3] Hannes Hartenstein and Kenneth P. Laberteaux "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communication Magazine, pp.164-171, June, 2008.

[4] Maxim Raya, Panos P., and Jean-Pierre Hubaux "Secureing Vehicular Communications," IEEE Wireless Comm. Vol.13, No.5, pp.8-15, 2006.

[5] Maxim Raya and Jene-Pierre Hubaux "Security Aspect of Inter-Vehicle Communication," Swiss Transport Research Conference, pp.1-14, March, 2005.
[6] 나진한, 박영호, 문상재, "U-TSN에서의 지불 인증 프로토콜 개발,"한국통신학회 추계종합학술발표회 논문초록집, pp.107, 2009년 11월
[7] 한국도로공사, 후불전자카드 규격 제정 및 공개, 2008
[8] 금융결제원, 금융 IC 카드 표준 개정(안), 2003
[9] J.T.Isaac, J.S.Camara, S.Zeadally, and J.T.Marquez, "A Secure Vehicle-to- Roadside Communication Payment Protocol in Vehicular Ad Hoc Network," Computer Communications, Vol.31, pp.2478-2484, 2008.
[10] J. Zhang, W. Zou, D. Chen, Y. Wang, On the security of a digital signature with message recovery using self-certified public key, Informatica (Slovenia) Vol. 29, No.3, pp.343-346, 2005.
[11] Y. Tseng, J. Jan, H. Chien, Digital signature with message recovery using selfcertified public keys and its variants, Applied Mathematics and Computation, Vol.136, No.2-3, pp.203-214, 2003.

나 진 한(JinHan Na) 준회원

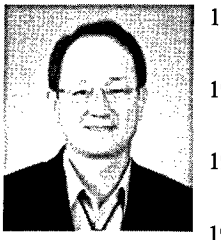


2008년 2월 상주대학교 전자전기공학부(공학사)
2008년 3월~현재 경북대학교 전자전기컴퓨터학부 석사과정
<관심분야> 정보보안

박 영 호(YoungHo Park) 종신회원

1989년 2월 경북대학교 전자공학과(공학사)
1991년 2월 경북대학교 전자공학과(공학석사)
1995년 8월 경북대학교 전자공학과(공학박사)
1996년 3월~2008년 2월 상주대학교 전자전기공학부 교수
2003년 8월~2004년 7월 Oregon State University 방문 교수
2008년 3월~현재 경북대학교 이공대학 산업전자전기공학부 교수
<관심분야> 네트워크 보안, 융합 보안 등

문 상 재(SangJae Moon) 종신회원



1972년 2월 서울대학교 공과대학(공학사-전자공학)
1974년 2월 서울대학교(공학석사-전자공학)
1984년 6월 미국 U.C.L.A.(공학박사-통신공학)
1984년 7월~1985월 6월 미국 OMNET 회사 컨설턴트
1984년 7월~1985년 6월 미국 U.C.L.A 포스트닥터
2001년 2월~2002년 2월 한국정보보호학회 회장
1974년 12월~현재 경북대학교 전자공학부 교수
<관심분야> 암호학, 네트워크 보안 등