VANET 기반의 긴급 차량 우선통과 서비스를 위한 인증 기법

준회원 윤 영 균*, 종신회원 정 수 환**°

An Authentication Scheme for Emergency Vehicle Priority Transit Service in VANET

Youngkyun Yoon* *Associate Member*, Souhwan Jung**° *Lifelong Member*

요 약

본 논문에서는 VANET (Vehicular Ad-hoc Networks) 기반의 첨단 교통관리 서비스에서 실시간 교통제어를 위해 필요한 긴급 차량 우선통과 시스템에서 요구되고 있는 인증 기법을 제안한다. 제안된 인증 기법은 교차로 상에서 긴급 차량에 신호 우선권을 부여하기 위한 대리 서명 기법을 적용하여 권한을 부여된 제어 권한을 인증하여 긴급차량들의 소통 상태 확보 및 다른 차량들의 안전성을 향상시킨다. 또한 인가된 제어 권한을 확인하기 위해 필요한 식별 절차에 필요한 ID를 제공하는 대리 서명 기법을 적용하므로 프라이버시를 보호하는 인증 기능을 제공 한다.

Key Words : VANET, Authentication, EVPT, Emergency Vehicle, ITS

ABSTRACT

In this paper, we propose an authentication scheme for EVPT (Emergency Vehicle Priority Transit) service in Vehiclar Ad-hoc Networks (VANET) enable a variety of vehicle comfort services, traffic management applications, and infotainment services. These are the basis for a new generation of preventive and active safety functions. By intelligently controlling signalling at intersections, providing additional information to the driver and warning the driver in critical situations. we therefore focus on vehicle-to-infrastructure communication for the authentication between emergency vehicles and traffic lights system. This authentication process should identify the vehicle, and provide privacy protection.

Ⅰ. 서 론

IT 기술은 우리의 생활 속에서 다양한 형태로 현실화되고 있다. 특히 차량의 경우, 국내외적으로 지능형 차량 및 지능형 교통 체계 (ITS: Intelligent Transportation System) 연구 개발을 통해 차량에 IT 기술을 접목하기 위한 기술 개발이 현재 진행되고 있다. DSRC는 이러한 지능형 교통 체계 서비스를 제공하기 위해 도입된 새로운 통신 수단으로써, 도로변에 위치하는 기지국 (RSU : Roadside Unit)과 차량단말 (OBU : On Board Unit)로 구성되는 통신 시스템으로 구성되어 있다. DSRC를 기반으로 하는 VANET (Vehicular Ad-hoc Networks) 통신에서는 차량들이 도로상에서 표지판이나 신호등과 같은 도로 주변의 RSU와 신속하고 정확한 통신을 지원하기 위해 차량의 고속 이동성, 네트워크 토폴로지와 노드

※ 이 논문은 2007년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원과(No.R01-2007-000-11504-0), 숭실대학교 교내 연구비 지원에 의해 수행되었음

* 숭실대학교 정보통신전자공학부 (yyk623@gmail.com), ** 숭실대학교 정보통신전자공학부 교수 (souhwanj@ssu.ac.kr) (° : 교신저자)

논문번호 : KICS2008-02-088, 접수일자 : 2008년 2월 15일, 최종논문접수일자 : 2008년 9월 26일

밀도의 급격한 변화 등 차량 환경에서 발생 할 수 있는 여러 가지 특수한 상황들을 고려해야 하기 때문에 각 서비스에 적합한 보안 프로토콜에 대한 연구가 필요하다.

본 논문에서는 긴급 구호 차량을 위한 교차로 신호 우선권 부여, 교차로 충돌 회피, 그리고 긴급 출동 차량 접근 경보 등의 교차로 신호등을 제어하는 안전에 연관된 응용 서비스들이 신호등과 연계되어 긴급차량의 신속한 이동을 위해 수행할 수 있는 적절한 인증 방식을 제안한다. 긴급차량의 교차로 신호 우선권부여는 구급차, 소방차, 경찰차 등의 긴급차량들을 위한 보안 응용 서비스로서, 긴급 차량들이 비상시에 목적지까지 신속히 이동하여야 함을 기본으로 두고 있다. 기존의 제안된 보안 프로토콜은 프라이버시를 위해 ID 식별을 제한하거나 반대로 ID 식별을 위해 정확한 식별자를 노출하게 된다. 프라이버시를 위해 ID 식별을 제한하게 되면 ID 식별 검증의 어려움이 있으며 단순한 검증만으로 신호를 변경하는 것은 위협 요소가 많다. 이를 위해 VANET 환경에서 기존의 연구된 인증 기법은 대칭키, 그룹키 또는 디지털 서명을 사용하는 기법으로 메시지의 무결성을 보장한다. 그러나 메시지의 무결성이 보장되는 것만으로 신호등의 제어를 서비스하는 것에 대하여는 여전히 다양한 공격의 가능성이 존재하므로 차량의 적절한 권한을 검증하는 절차가 필요하다. 따라서 교차로 상에서 긴급 구호 차량 신호 우선권 부여를 위한 교차로 신호등 제어 프로토콜을 실제적으로 적용하고자 정당한 권한을 차량에 부여하여 VANET에서 발생 가능한 공격에 안전하고 인가된 권한을 제공하는 기관을 구분하여 인증할 수 있는 대리서명 기법을 적용하여 정당한 차량에 대해서 신호 우선권 부여가 가능한 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 VANET에서의 기존 관련연구기술을 정리하고 Ⅲ장에서는 긴급 차량의 권한 인증을 실제적으로 적용하기 위해 제안된 보안 프로토콜을 설명한다. Ⅳ장에서는 제안 프로토콜의 특징 및 안전성을 분석하며 Ⅴ장에서 결론을 맺고자 한다.

Ⅱ. 기존 연구

2.1 Pair-wise Key를 사용한 인증 기법[12]

Pair-wise Key를 사용한 인증 기법은 대칭키 인증 기법으로 인증 기법의 속도 측면만을 보면 가장 빠르고 효율적이다. Pairwise Key는 네트워크상에서 두 노드가 안전하게 통신하기 위해 공유하고 있는 세션키이다. 이러한 세션키를 사용하는 대칭키 암호화 기법은 오버헤드와 시간의 측면으로 볼 때 공개키 암호화 기법보다 매우 효과적이다.

1. A → B : $\{B|K|T\}_{PuKB}$, $Sig_{PrKA}[B|K|T]$
2. A → B : Mc, $HMAC_K$

그림 1. 세션키를 사용하는 인증 기법

세션키를 사용하는 인증 기법은 상호간의 세션키 K를 공유하고 그 키를 사용하므로 빠르고 안전한 인증을 제공하지만 여기에는 여러 가지 문제점이 존재한다. VANET에서는 동적으로 세션키를 할당하게 되면 키를 관리하는 것이 어렵기 때문에 이를 위한 새로운 키 관리 매커니즘이 필요하고 또한, 이 기법을 적용하기 위해 매 신호등마다 세션키를 교환해야 한다면 이것은 VANET 노드들에게 상당한 오버헤드를 수반하게 된다.

2.2 디지털 서명을 사용한 인증 기법[13]

디지털 서명을 사용한 메시지 인증 기법은 VANET에서 가장 적절한 인증 방식으로 제시되고 있다. 디지털 서명은 통신 개체간의 특별한 관계 또는 연관성 없이 CA에서 발급된 인증서를 통해 메시지 인증, 부인방지와 무결성을 보장하기 때문에 네트워크의 휘발성이 큰 VANET에서는 가장 적합한 인증 기법으로 알려져 있다. VANET은 내부와 외부의 공격자로부터 보호하기 위해 메시지의 정당성은 반드시 검증되어야만 한다. 그러나 대부분의 안전 메시지들은 특별하게 민감한 정보들을 포함하고 있지 않으므로 기밀성은 요구되지 않는다. 결과적으로 VANET에서는 메시지에서는 인증이 필요하며 암호화는 요구되지 않는다. 최근 VANET에서 보다 효율적이며 안전하게 보호하기 위해 다양한 인증 프로토콜이 연구 되고 있으나 아직 연구 초기 상태이며 메시지 인증을 위해 탁월한 디지털 서명기법을 적용하고 있다. 각각의 차량에 공개키/개인키 쌍을 할당하는 방법은 보안을 위해 가장 간단하고도 효율적인 방법이다. 이러한 공개키들은 반드시 신뢰된 기관에 의해서 할당되고 발행되어야 하며 PKI (Public Key Infrastructure)의 사용을 통해 지원한다. PKI 솔루션을 기반으로 차량은 메시지를 전송하며 그 메시지는

차량의 개인키로 서명된다. 그리고 CA의 인증서를 포함하여 메시지를 전송하며 그 절차는 다음과 같다.

$$V \rightarrow I : Mc, Sig_{PrKV}[Mc|T], Cert_V$$

그림 2. 디지털 서명을 사용하는 인증 기법

여기서 V는 긴급 차량이며 I는 신호등 시스템을 의미한다. Mc는 제어 메시지이고 T는 타임스탬프로 메시지의 신규성을 제공하여 재전송 공격을 방지한다. 메시지를 받은 신호등 시스템에서는 V의 공개키를 사용하여 메시지를 검증하여 메시지의 정당성을 확인하여 신호등을 제어한다. 공개키 기반의 디지털 서명 기법을 사용한 기법은 메시지의 인증 기능을 훌륭하게 지원하지만 인가된 제어 권한을 확인하기는 어렵다. 인가된 제어 권한을 주기 위한 인증서를 별도로 발행한다면 인증서 관리를 위한 추가적인 오버헤드가 존재하며 익명 인증서 즉 ID를 사용하지 않는 인증서를 발행하여 프라이버시 지원한다면 프라이버시와 ID 식별의 trade-off 관계를 가지는 문제가 존재한다. 또한 VANET에서는 인증서의 위조 및 불법적인 사용을 방지하기 위해 인증서의 발급을 제한하고 있으며, 불법적인 변경 및 보안 관리를 위해 차량내의 Trusted Component (TC)에 인증서를 저장해야 하므로 이에 따르는 문제가 발생 할 수 있다.

2.3 DH 키와 디지털 서명을 사용한 인증 기법[16]

DH 키와 디지털 서명을 사용한 메시지 인증 기법은 차량과 신호등 사이의 통신을 위해 DH 키를 서로 교환한 후 생성된 세션 키로 디지털 서명을 암호화 하여 전송하여 안전한 통신을 지원한다. 여기서 모든 긴급 차량은 차량을 식별할 수 있는 태그와 신호등을 제어할 수 있는 크리덴셜을 포함하고 있으며 크리덴셜은 제어 메시지를 보내는 차량의 인가를 제공한다. 제어메시지를 보내는 동안에 신호등과 긴급 차량은 Diffie Hellman 프로토콜을 사용하여 세션키를 공유하고 모든 정보에 연관된 것들을 세션키로 암호화하여 제공하므로 긴급 차량에 대한 프라이버시를 제공한다. 다음의 그림은 DH 키와 디지털 서명을 사용한 메시지 인증 기법의 전체 프로토콜을 나타낸다.

DH 키와 디지털 서명을 사용한 메시지 인증 기법은 DH 키 교환을 통해 상호 인증을 제공하고, 디지털 서명을 통해 메시지 무결성을 보장한다. 그러나

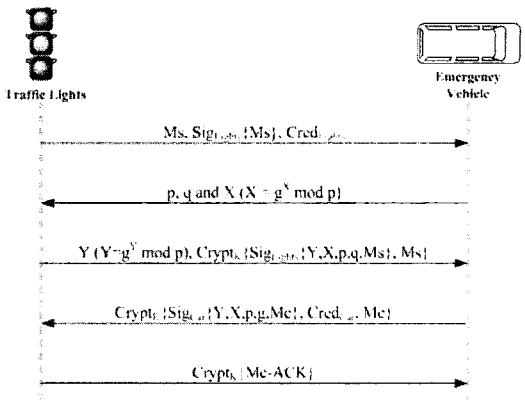


그림 3. DH과 디지털 서명을 통한 신호등 제어 프로토콜

Ms:	주기적인 상태 메시지
SigCar{X}:	"Car"에 의해 생성된 "X"의 서명
CredLights:	Light의 크리덴셜
X,Y,p,q:	공개된 Diffie-Hellman 키 파라미터
x,y:	비밀 Diffie-Hellman 키 파라미터
CrptK{X}:	키 X를 사용한 X의 암호화
Mc:	제어 메시지
Mc-ACK:	제어메시지 Mc를 위한 확인

그림 4. 신호등 제어 프로토콜 용어

DH의 취약점으로 인해 중간자 공격에 취약할 수 있으며, 긴급 차량이 지나는 경로상의 모든 신호등 시스템과 항상 DH 과정을 수행해야 하므로 많은 신호등을 통과할수록 오버헤드가 가중된다.

Ⅲ. 제안 프로토콜

신호등 시스템 제어 서비스는 경찰차, 구급차, 소방차와 같은 긴급 출동 차량들이 교차로를 원활하게 통과하기 위해 DSRC를 이용하는 응용 서비스 중의 하나이다. 여기에서 긴급 차량은 제어 채널을 통해 접근 경보 메시지를 전송하여 타 차량의 주의를 요구하며, 동시에 공공 안전-교차로 채널 (ch.184)을 통해 교차로 우선 통과 요청 메시지를 전송한다. 제어 채널을 통해 긴급차량 접근 경보 메시지를 수신한 일반 차량들은 교차로 우선 통과 메시지를 수신한 교차로 상의 RSU는 긴급차량이 교차로를 우선 통과할 수 있도록 신호등을 작동시키며 인근 도로상의 타 차량들은 신호등의 동작과 긴급 차량 접근 경보에 따라 긴급차량에게 길을 비켜줄 수 있게 된다. 이와 같은 서비스를 위해 다음과 같은 보안 기능들을 정의한다.

• 신호등의 상태 메시지 전송

신호등이 자신의 상태정보를 전송하고 이 메시지들은 필수적으로 무결성이 보장 되어야 하고 발신자를 인증할 수 있어야 한다.

• 긴급 차량에 의한 신호등 제어

긴급차량은 제어 메시지를 신호등에게 전송한다. 이를 위해서 제어 메시지의 인증과 인가된 권한을 반드시 점검해야 하며 발신자가 검증되어야 한다. 또한 재전송 공격을 방지하기 위해서 제어 메시지의 신규성이 항상 검증되어야 한다.

이번 장에서는 VANET 환경에서 차량과 신호등 간에 발생 가능한 다양한 공격으로부터 안전한 통신을 위해 적용하기 적합한 보안 기법으로 대리서명을 소개하고 이를 VANET에 적용하여 프라이버시를 지원하는 보안 기법을 제안한다.

3.1 대리인 보호형 보증 부분 위임 대리 서명 방식[9]

대리 서명방식이란 대리 서명자로 하여금 원서명자를 대신하여 서명을 할 수 있는 서명 시스템을 말한다. 대리 서명방식의 조건은 원서명자로부터 지정받은 사람만 대리 서명을 생성할 수 있어야 하며, 대리 서명자로 지정 받지 못한 제 삼자는 대리 서명을 생성 할 수 없어야 한다. 또한 대리 서명을 검증하는 사람은 대리 서명으로부터 원서명자가 대리서명자에게 대리 서명을 위임한 사실을 확인 할 수 있어야 한다. 지금까지 제안된 대리 서명방식의 종류는 완전 위임, 부분 위임, 그리고 보증 위임 등의 세 가지 방식으로 구분할 수 있으며 M.Mambo와 E. Okamoto는 이산대수 문제를 이용하여 부분 위임에 의한 대리 서명방식을 제안하였다[10]. 본 논문에서는 이를 발전시킨 보증 부분 위임 방식을 사용한 서명방식을 사용하고[9] 안전성이 검증된 Nyberg-Rueppel 방식의 디지털 서명 방법을 적용하여 메시지를 서명한다[11]. 대리인 보호형 대리 서명방식[9]은 원서명자의 부정행위 및 공격을 방지하기 위해 대리서명자의 비밀키를 사용한다. 일반적인 대리 서명방식은 원서명자의 신뢰성을 전제로 하는 방식이다. 그러나 원서명자의 정직하지 못한 행동 즉, 원서명자가 대리서명자를 가장한 서명은 대리서명자를 곤란하게 만들 수 있다. 다음과 같은 절차에 의해서 원서명자의 부정행위를 방지한다.

대리인 보호형 보증 부분 위임 대리 서명 방식은 개인키가 대리인에 의해서만 표현되어질 수 있기 때문에 대리인 보호형 대리서명 기법이다. 이 기법은 대리서명 내에 원서명자와 위임자의 역할이 동일하다는 단점이 있다. 따라서 권한에 대한 내용이 아주 명백하게 표시 되어 있어야 하며 그렇지 않은 경우에는 이들의 역할이 바뀔 수 있기 때문에 검증자는 대리 서명의 권한에 표시된 내용과 일치하는지에 대해서 점검해야 한다.

3.2 대리 서명을 통한 인가된 제어 권한 검증 기법

다음의 그림 5는 긴급 출동 차량이 교차로를 원활히 통과하기 위해 DSRC를 이용하는 시나리오를 나타내는 그림이다. 여기에서 긴급 출동 차량은 RSU 제어를 위해 교차로 우선 통과 요청 메시지를 전송하고 주변 차량에 긴급 차량 접근 경보 메시지를 전송하여 타 차량에게 긴급차량의 접근을 알리고 주의할 것을 요청한다. 이러한 교차로 우선 통과 메시지를 수신한 교차로 상의 RSU는 긴급 차량이 교차로를 우선 통과할 수 있도록 신호등의 신호를 변경시키며 인근 도로상의 타 차량들이 신호등의 동작과 긴급 차량 접근 경보에 따라 긴급 차량에게 길을 비켜줄 수 있게 된다.

긴급 차량 교차로 우선 통과 서비스는 경찰, 소방서와 같이 공공의 안전을 위한 목적을 수행하는 차량에게만 제공되어야 한다. 이러한 서비스를 위해 적절한 인증 기능이 수행되지 않는다면 가장 공격과 거짓 정보를 전달하게 하는 공격에 취약하게 된다. 또한 긴급 상황 발생 시에 긴급 차량들은 빠른 이동 속도가 확보 되어야 하므로 긴급차량이 빠른 속도로 이동할 때 교차로에서는 다른 방향 차선의 차량들과 심각한 사고를 유발할 가능성도 존재한다. 따라서 긴급차량은 주변의 모든 차량에 경고 메시지를 전달하고 사전에 발생할 사고를 방지하기 위해 신호를 제어함으로써 이동 속도를 확보하고 발생 가능한 사고들을 예방한다. 긴급차량은 서비스를 제공하는 기관

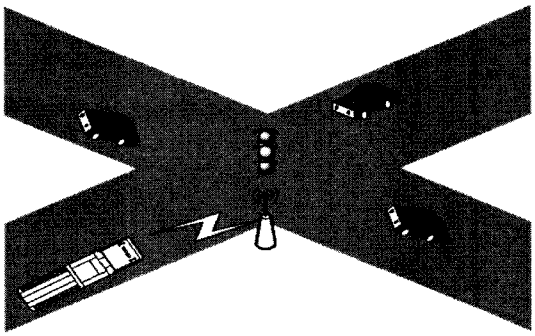


그림 5. 긴급 출동 차량의 교차로 우선 통과 서비스

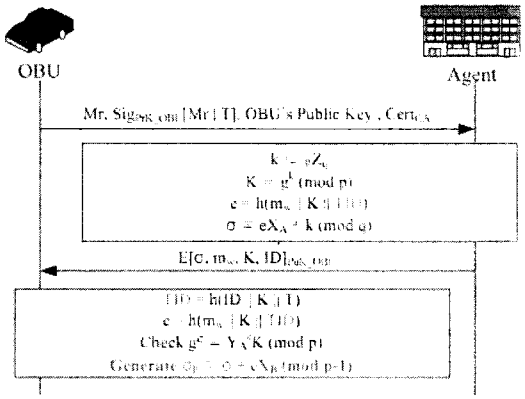


그림 6. 긴급 차량과 기관의 통신 프로토콜

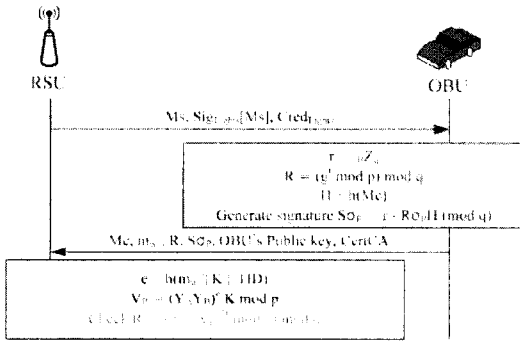


그림 7. 신호등 시스템과 긴급차량과의 통신 프로토콜

에서 사용하는 차량으로 신호등을 제어 할 수 있는 적절한 권한을 가져야 한다.

본 논문에서는 대리인 보호형 보증 부분위임 대리서명 기법을 적용하여 차량이 위임정보를 기반으로 서명한 메시지를 통해 서명 수행자를 구별하고 서명 수행자가 기관으로 제어 권한을 위임 받은 차량임을 확인할 수 있다. 차량에게 경찰의 권한을 위임하는 일인 만큼 이후 공격에 사용되는 것을 방지하기 위해 사용 후 권한을 반납해야 하며, 폐기 시간을 두어 정해진 시간 내에서만 사용할 수 있도록 한다.

Mr : 권한 요청 메시지
Ms : 신호등 시스템의 주기적인 상태 메시지
Mc : 신호등 제어 메시지
T : 타임 스탬프
TID : 임시 ID로 차량의 식별정보와 K값을 포함하고 재전송 공격을 방지하기 위한 시간 정보 T를 함께 해시하여 생성
X_A : 기관의 비밀 서명정보
X_B : 긴급차량의 비밀 서명정보
σ : 대리 서명 생성용 비밀 서명정보
σP : 재생성한 대리 서명용 서명 비밀정보
p : 큰 소수
g : 원시원소

- 동작절차

① 긴급차량은 권한 요청 메시지 Mr와 시간 정보 T를 자신의 개인키로 서명하여 기관에 인가된 제어 권한을 요청한다.

② 기관은 차량의 프라이버시 및 인증 권한 부여를 검증하기 위한 TID를 생성한다. TID는 차량의 식별정보와 K값을 포함하고 재전송 공격을 방지하기 위한 시간 정보 T를 함께 해시하여 생성하여 제어 권한 위임에 대한 정보를 구별하기 위한 정보로 사용하고 대리 서명을 생성할 수 있는 비밀 서명정보 σ에 유효기간과 대리 서명자의 관계 등이 언급된 보증서를 해쉬 함수를 이용하여 포함시킨다.

③ 비밀 서명정보를 비밀리에 전달받은 긴급 차량은 받은 대리 서명 생성용 비밀 서명정보 σ의 정당성을 기관의 공개 검증정보 YA를 이용하여 확인한다. 여기서 위임 정보의 정당성을 확인하여 기관으로 가장하는 공격자들에게서 차량을 보호한다. 받은 비밀 서명정보가 확인되면 긴급 차량은 자신이 비밀리에 보관하고 있는 일반 서명 비밀정보 XB를 포함시킨다. 변환된 대리 서명용 비밀정보 σP를 생성할 수 있는 노드는 긴급 차량 뿐이므로 차량을 보호 할 수 있다.

④ 인가된 권한을 받은 차량이 신호등으로부터 주기적으로 전달되는 메시지를 받게 되면 신호등 시스템이 전송하는 Ms를 서명한 정보를 검증한다.

⑤ 긴급 차량은 자신이 재생성한 대리 서명용 서명 비밀정보 σP를 이용하여 일반적인 디지털 서명방식을 이용하여 신호 변경 요청 메시지 Mc의 대리 서명을 생성한다.

⑥ 신호등 시스템에서는 긴급 차량의 공개 검증정보를 계산하고 VP를 계산하여 확인한다. 대리 서명의 검증 순서는 일반 디지털 서명의 검증 순서에 따라 검증한다. 검증을 위한 계산과정에서 YA와 YB가 포함되므로 기관과 긴급차량의 신원을 확인 할 수 있으며 특히, XB가 포함되므로 긴급차량에 의해서 전달된 것을 확인할 수 있다.

제안하는 기법은 대리 서명 기법을 통해 긴급 차량에게 주어지는 인가된 제어 권한 확인이 가능하도

록 돕는다. 또한 시간 정보 T와 인가 권한의 유효 기간을 포함하는 mw를 통해 재전송 공격을 방지하고, 진행 경로 상의 모든 신호등과 특별하게 세션을 맺지 않아도 인가된 권한에 대한 인증이 가능하다. 대리서명의 단점을 보완하기 위해 TID를 사용하여 차량이 독자적으로 역할을 바꾸지 못하도록 방지하며 인가된 권한의 유효기간 설정을 통해 제어 권한의 영구적 사용을 방지한다.

Ⅳ. 제안 기법의 특징 및 안전성 분석

VANET에서는 긴급차량에게 교차로에서 우선 통과할 수 있는 권한을 부여하여 안전하고 효율적인 환경을 제공하고자 한다. 긴급차량의 교차로 우선 통과 서비스는 DSRC에서 사용되는 무선 채널(ch.184)을 통해 구성되며 차량에서 OBU로 전송한 교차로 우선통과 메시지를 통해 동작한다. 이러한 제어 채널을 통해 들어온 정보에 대해 신호등과 같은 제어 장비들이 동작하도록 하는 방식은 단순한 액세스 인증과 같은 기본적인 인증만을 수행하기 때문에 인가된 제어 권한을 검증하고 차량 인증 기능을 보안 기술에 포함하지 않는 다면 거짓 정보를 발생하여 우선권을 부여 받는 차량에 대해 취약하다 또한 긴급차량의 정보를 스니핑하여 가장 공격을 수행할 수 있기 때문에 차량 안전에 심각한 혼란을 발생시킬 수 있다.

본 논문에서 제안하는 기법이 적용되면 다음과 같은 2가지 주요한 장점이 존재한다. 첫 번째 장점은 긴급차량이 TID를 사용하여 메시지를 전송하도록 하므로 긴급 차량의 원본 ID를 보호할 수 있도록 하였다. 즉 프라이버시 기능을 강화하였다. 두 번째 장점은 기관으로부터 차량이 인가된 권한을 받아 신호등을 제어하기 위해 긴급차량과 신호등 시스템간의 상호 인증을 지원하기 위한 절차가 따로 필요하지만 대리 서명기법을 사용하여 신호등 시스템과 긴급차량간의 특별한 세션을 맺지 않아도 상호간에 인증이 가능하도록 하였다.

4.1 제안 기법의 특징

4.1.1 TID를 통한 원본 ID 보호

VANET에서는 프라이버시 기능이 가장 중요한 기능으로 대두되고 있다. 이에 따라 Long-term Identification을 갖는 인증서와 Short-term Identification을 갖는 인증서로 구분하고 있으며, 공장, 정비소와 같은 안전한 공간에서 설치가 되는 Long-term Identification을 갖는 인증서와 이러한 인증서를 이용하여 발급 받아 저장할 수 있는 Short-term Identification을 갖는 인증서로 구분할 수 있다. 본 논문에서는 이러한 Short-term Identification을 TID로 대체할 수 있으며 인증 절차에 포함 시키므로 다수의 Short-term Identification을 포함하고 있는 인증서를 발급받지 않아도 원본 ID를 보호할 수 있다.

4.1.2 프라이버시 보호와 인증 기능 동시 수행

긴급 차량의 경우에 신호등 시스템이 긴급 차량의 인증서를 얻게 된다면 보안 문제는 고려하지 않게 된다. 신호등과 긴급차량의 통신 단계에서 긴급차량이 자신의 인증서를 신호등 시스템에 전송하게 되면 자신의 인증서가 공개되고 실제의 ID가 공개될 수 있다. 또한 ID를 사용하지 않은 인증서를 사용하게 된다면 ID 식별에 문제가 발생하기도 한다. ID를 식별하는 것과 프라이버시 기능을 제공하는 것은 이와 같이 Trade-off 관계에 있기 때문에 상황에 따른 조절이 필요하다. 그러나 신호등 제어 서비스의 경우에는 ID를 확인하는 것이 중요하기 때문에 ID 식별이 반드시 요구된다. 따라서 본 논문에서는 긴급 차량이 TID를 발급받도록 하여 긴급차량과 신호등과의 통신에서 실제적인 긴급차량의 ID를 공개하지 않고 긴급차량의 증명을 익명으로 실시하더라도 권한을 부여한 기관을 인증하게 되므로 보안을 약화시키지 않고도 익명성을 제공하는 것이 가능하다.

4.2 안전성 분석

VANET에서의 몇 가지 공격들은 일반적인 네트워크상에서의 공격과 유사하다. 본 논문에서 설명하고 있는 프로토콜은 이러한 공격을 방지한다.

4.2.1 Replay Attack

재전송 공격은 가장 가능성이 높은 공격이다. 여기서는 일반적으로 재전송 공격을 방지하기 위한 2가지 가능성 있는 방법이 존재한다. 첫 번째 방법은 모든 노드가 동기화된 시간을 설정하는 것이고 또 다른 방법은 Nonce를 사용하는 것이다. 일반적으로 Nonce는 큰 숫자를 사용하도록 한다. 본 논문의 프로토콜에서는 랜덤값 K가 충분히 큰 수로 선택이 되며, mw가 포함하고 있는 폐기 시간을 통해서 재전송 공격을 예방한다. 예를 들면 공격자가 마지막 메시지를 다른 신호등 시스템에 재전송한다면 mw의 인가된 권한 폐기 시간을 확인하여 인증이 실패되었음을 알린다.

4.2.2 Man-in-the-middle Attack

공격자는 신호등과 긴급차량 사이에서 권한을 얻기 위한 개입을 시도할 수 있다. 본 논문의 프로토콜에서는 공개키를 기반으로 디지털 서명을 제공하므로 중간에서 메시지를 변조하는 것이 불가능하며 기관과 긴급차량, 긴급차량과 신호등 시스템은 인증서를 통해 상호인증을 지원하고 있기 때문에 중간에서 메시지를 변경하는 것이 어렵다. 예를 들면 공격자가 인가된 권한을 얻기 위해 차량과 기관 사이에서 공격을 시도한다면 긴급 차량은 자신의 인증서를 기반으로 자신의 ID와 시간 정보 T값을 함께 서명하여 자신이 등록된 기관으로 전송하게 하고 기관으로부터 받은 위임 정보를 긴급 차량이 검증하기 때문에 중간자 공격이 어렵다. 또한 신호등 시스템과 긴급 차량 사이에서 공격을 시도해도 대리 서명 비밀정보로 서명된 메시지를 변조할 수 없기 때문에 메시지의 변조 공격이 불가능하다.

4.3 기존 프로토콜과의 비교

VANET에서의 보안을 위해 지금까지 소개되었던 비밀키를 사용하여 인증하는 방법과 공개키를 사용하여 인증 하는 방법 등의 인증 기능 및 보안 서비스 제공 여부 등을 비교하여 표 1로 정리하였다.

먼저 IEEE 802.11i는 사용자 인증 및 상호인증 등의 기본적인 네트워크 보안 서비스를 지원하지만 매 신호등에서마다 과정을 수행해야 하고 인가된 제어권한을 부여하고 확인하는 과정이 존재하지 않는다. pairwise key를 기반으로 하는 방법은 사전에 서로 공유된 키를 기반으로 인증 및 보안 기능을 제공한다. 그러나 신호등 시스템 환경에서는 공개키를 기반으로 하여 비밀키를 교환하며 그 비밀키를 기반으로 HMAC을 생성하여 메시지의 무결성을 지원한다. 메시지 전송 후 확인 측면만 보면 적은 계산량을 가지지만, 상호인증을 지원하지 않고 매 신호등 시스템마다 공개키를 사용하여 비밀키를 교환해야하는 단점이 있다. 공개키 기반의 인증 기법은 인증서와 디지털 서명을 사용하여 메시지 무결성을 제공하나 상호인증을 지원하지 않고 ID가 포함된 인증서를 제공하므로 ID 노출의 위험성이 존재한다. 또한 초기 인증서를 발급받은 상황에서 인증서를 재발급 받는 절차가 복잡하기 때문에 자신의 ID가 노출 될 경우마다 인증서를 재발급해야하는 오버헤드를 수반한다.

DH와 디지털 서명을 사용하는 기법에서도 상호인증을 위해서 DH 키 교환을 매 신호등 마다 실행해야 하며 이것은 신호등 시스템에 오버헤드를 줄 수 있다. 또한 차량이 생성하는 메시지도 DH을 위한 메시지와 디지털 서명을 위한 메시지가 각각 존재하고 있기 때문에 소개된 다른 프로토콜보다 제안 프로토콜이 효율성이 좋은 프로토콜임을 확인할 수 있다. 제안하는 기법에서는 긴급차량에 기관으로부터 인가된 제어 권한을 소유하고 있음을 보장하여 긴급 차량이 아닌 다른 차량들이 제어를 위한 거짓 정보

표 1. 기존 기술과 제안 기법의 비교

		IEEE 802.11i	비밀키[12]	PKI[13]	DH & 디지털서명[16]	제안기법
사용자 인증		제공	제공	제공	제공	제공
인가된 제어 권한 인증		제공안함	제공안함	제공안함	제공안함	제공
암호화		제공	제공	제공 (필요시)	제공	제공 (필요시)
부인 봉쇄		제공안함	제공안함	제공	제공	제공
무결성		제공	제공	제공	제공	제공
프라이버시 제공 기법		제공안함	제공안함	제공안함	공유키 기반 메시지 암호화	TID 사용
디지털 서명		사용안함	사용	사용	사용	사용
차량	생성하는 메시지 수	3	2	1	2	2
	지수 및 공개키 연산	1	2	1(2)	4	5
	원본 ID 공개	공개	공개	공개	비공개	비공개
보안 기술		IEEE 802.1x	비밀키, MAC	인증서	DH, 인증서	대리 서명, 인증서
키 교환		필요	필요	필요없음	필요	필요없음
상호인증		제공	없음	없음	제공	제공
Replay Attack		보호	보호	보호	보호	보호
MITM		보호	보호	보호	취약	보호

를 RSU에게 보내어도 RSU가 이러한 메시지를 정당한 권한을 가진 것인지 인증함으로 안정적인 서비스를 지원하도록 하였다. 이를 위해 공개키 기반의 디지털 서명을 제공하고 무결성 및 부인 봉쇄의 보안 서비스를 제공하여 공격 차량이 임의적으로 제어 메시지를 발생하지 못하도록 제한하고 중앙 본부와 같은 제어를 위한 적당한 권한을 가진 기관들을 통해 차량에 제어 권리를 부여하여 정당한 제어 권한을 가진 차량임을 인증된다. 제어 권한을 위임 받지 않은 공격 차량들은 공개키 기반의 위임정보를 생성할 수 없으므로 제어 권한을 얻을 수 없고 제어를 위한 메시지 발생이 불가능 하다. 또한 긴급차량의 기능을 수행하는 차량은 메시지 발생을 위해 자신의 개인키를 사용하여 위임 서명 정보를 생성하여 디지털 서명을 수행하므로 메시지에 대해 무결성을 지원하고 부인 봉쇄 서비스를 제공하여 인증의 효율성을 높이고 높은 수준의 보안 서비스 지원이 가능하며 권한을 받은 차량임을 증명하여 다양한 공격을 효과적으로 방지함을 볼 수 있다.

V. 결 론

VANET에서는 기존의 네트워크 환경에서 발생하지 않았던 다양한 위험이 존재하기 때문에 서비스에 특성화된 다양한 인증 프로토콜이 필요하다. DSRC 응용 서비스인 교차로 우선 통과 요청 메시지는 긴급 출동 차량이 긴급 상황 시에 교차로를 원활히 통과하기 위한 응용 서비스이다. 교차로 우선 통과 요청 메시지는 제어 채널을 통해 접근 경보 메시지를 다른 차량에게 전송하여 타 차량의 주의를 요구하며, 동시에 공공 안전-교차로 채널 Ch.184를 통해서 제어 메시지를 전송한다. 그러나 이러한 제어 메시지는 보안 기능이 취약하기 때문에 다양한 공격의 문제점이 존재한다. 따라서 본 논문에서는 긴급차량 우선 통과 메시지를 발생할 때 RSU에서 차량을 인증하기 위해 대리 서명 기법을 적용하여 가장 공격과 거짓 정보를 발생하는 공격에 효과적으로 대비하기 위한 인증 기법을 제시하였다. 이 프로토콜은 VANET 환경과 같이 급격한 토폴로지 변화를 기반으로 하는 네트워크 환경에서 널리 사용될 것으로 기대된다.

본 논문에서는 TID를 사용하는 대리서명 기법을 적용한 교차로 우선 통과 메시지 전송 프로토콜을 제안하였다. 제안 프로토콜은 제어를 위해 인가된 제어권한을 부여 받도록 지원하여 인가된 제어권한을 받은 긴급차량만이 교차로 우선 통과 서비스를 지원받을 수 있도록 하였다. 또한 ID 식별과 프라이버시의 Trade-off 문제를 해결하기 위해 권한을 부여하는 기관을 인증하도록 지원하여 토폴로지 변화가 빈번한 VANET 환경에 적합한 인증 프로토콜을 제공한다. 실제로 교차로 상황에서의 위험상황 탐지 및 응용서비스 보안 기술은 현재 연구되고 있는 분야이며 이후에는 보다 안전한 VANET 환경을 실제적으로 구축하기 위한 다양한 응용 서비스들에 적합한 상세적인 보안 프로토콜을 정의하여 안전한 통신 환경을 제공하도록 해야 한다.

참 고 문 헌

[1] J.J. Blum, A. Eskandarian,L.J. Hoffman, "Challenges of inter-vehicle ad hoc networks," *Intelligent Transportation Systems*, IEEE Tran. on Vol.5, Issue 4, pp.347-351, Dec. 2004.

[2] M, Torrent-Moreno, M.Killat, H. Hartenstein, "The challenges of robust inter-vehicle communications," *Vehicular Technology Conf. 2005 VTC-2005-Fall.* 2005 IEEE 62nd Vol.1, pp.319-323, Sept. 2005.

[3] Q. Xu et al., "Layer-2 Protocol Design for Vehicle Safety Communications in Dedicated Short Range Communications Spectrum," *Proc. of the 7th IEEE Int"l conf.* on Intelligent Transportation Systems, pp.1092-1097, Oct. 2004.

[4] M.M Artumy, W. Robertson, W.J. Phillips, "Connectivity in inter-vehicle ad hoc networks," *Electrical and Computer Engineering*, 2004. Canadian Conference on Vol.1, pp.293-298, May 2004.

[5] W. Chen and S. Cai, "Ad Hoc Peer-to-Peer Network Architecture for Vehicle Safety Communications," *IEEE Communications Magazine* Vol.43(4), pp.100-107, 2005.

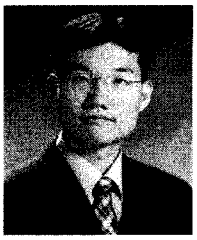
[6] M.T Sun, W.C. Feng, et al., "GPS-Based Message Broadcast for Adaptive Inter-Vehicle Communications," *Proc. of the 52th IEEE Vehicular Technology Conference*, pp.2685-2692, Sept. 2000.

[7] Maxim Raya and Jean-Pierre Hubaux, "Secure vehicular ad hoc networks," *Journal of Computer Security*, IOS Press, January 2007.

[8] 이혁준, "텔레매틱스 서비스를 위한 무선 네트

워크 기술." *정보과학회지*, 제23권, 제4호, 2005.
[9] 김승주, 박상준, 양형규, 원동호, "보증 부분 위임에 의한 대리 서명에 관한 연구," *한국통신학회논문지*, Vol.24, No.3A, 1999.
[10] M.Mambo, K. Usuda, and E.Okamoto, "Proxy signature : Delegation of the power to sign message," *IEICE Trans.* Fundamentals, vo.E79-A, No.9, 1996.
[11] Kaisa Nyberg and Rainer A.Rueppel, "Message Recovery for signature scheme based on the discrete logarothm problem," *Eurocrypt'94*, pp.175-190, 1994.
[12] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehiclular Communications," *IEEE wireless communication magazine*, October 2006.
[13] Maxim Raya and Jean-pierre Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security 15 IOS press*, 39-68, 2007.
[14] Frederik Armknech, Andreas Festag, Dirk Westhoff, and Ke Zeng, "Cross-layer Privacy Enhancement and Non-repudiation in Vehicular communication," *WMAN*, 2007.
[15] Florian Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks," *Workshop on Privacy Enhancing Technologies*, Dubrovnik (Cavtat), May, 2005.
[16] Florian Dötzer, Florian Kohlmayer, Timo Kosch, and Markus Strassberger, "Secure Communication for Intersection Assistance," *WIT 2005: 2nd International Workshop on Intelligent Transportation*, March, 2005.

윤 영 균 (Youngkyun Yoon) 준회원



2004년 8월 가톨릭대학교 수학과 학사
2008년 2월 숭실대학교 정보통신공학과 석사
<관심분야> NGN 엑세스 인증, 핸드오버 인증, 차량 통신 보안

정 수 환 (Souhwan Jung) 종신회원

1985년 2월 서울대학교 전자공학과 학사
1987년 2월 서울대학교 전자공학과 석사
1998년~1991년 한국통신 선임연구원
1996년 6월 Univ. of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안