Journal of Korea Multimedia Society Vol. 16, No. 2, February 2013(pp. 180-189)
http://dx.doi.org/10.9717/kmms.2013.16.2.180

SMART Highway 환경에서의 사인크립션 기반 키 교환 프로토콜

김수현†, 이임영††

요 약

SMART Highway 사업은 첨단 IT통신과 자동차 및 도로 기술이 접목된 세계 최고수준의 빠르고 편안한 지능형 녹색도로 실현을 목표로 하고 있다. SMART Highway의 도로-자동차 기반 교통운영의 핵심기술인 VANET(Vehicular Ad-hoc Network)은 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU(Road Side Unit)사이의 통신을 제공하는 차세대 네트워킹 기술이다. 특히, 운전자의 안전에 직접적인 영향을 끼칠 수 있는 V2V 통신의 경우 차량 간의 안전한 통신을 위해 안전한 키 교환이 반드시 고려되어야 한다. 이처럼 빠른 속도로 이동하는 차량 간 안전한 키 교환이 원활이 이루어지기 위해서는 기존의 네트워크에서 사용된 방식은 그대로 적용시키기 어렵다. 따라서 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적이고 안전한 키 교환을 위해 사인크립션을 이용한 차량 간 그룹키 교환기법을 제안한다.

Key Exchange Protocol based on Signcryption in SMART Highway

Su-Hyun Kim†, Im-Yeong Lee††

ABSTRACT

The SMART Highway project combines road construction with advanced technology and vehicle telecommunications. Its expected outcome is a world-leading intelligent road that is green, fast, and comfortable. A vehicular ad-hoc network(VANET) is the core technology of the SMART Highway, whose transport operation is based on road vehicles. The VANET is a next-generation networking technology that enables wireless communication between vehicles or between vehicles and a road side unit(RSU). In the VANET system, a vehicle accident is likely to cause a serious disaster. Therefore, some information on safety is essential to serve as the key exchange protocol for communication between vehicles. However, the key exchange scheme of the general network proposed for a fast-moving communication environment is unsuitable for vehicles. In this paper, communication between multiple vehicles more efficient and secure key exchange at the vehicle certification by signcryption is proposed.

Key words: SMART Highway(스마트 하이웨이), Vehicular Ad-hoc Network(차량 애드혹 네트워크), Key Exchange(키 교환), Signcryption(사인크립션)

1. 서 론

SMART Highway 사업은 국토해양부에서 수립한 “건설교통 R&D 혁신 로드맵”에서 선정되어 추진되는 사업으로써, 첨단 토목기술, IT기술, 차세대 자동차기술을 상호 접목하여 빠르면서도 안전한 지능형 고속도로를 개발하는 사업이다[1].

SMART Highway는 설계속도 160km 이상에서

※ 교신저자(Corresponding Author) : 이임영, 주소 : 천안 서북구 쌍용동 천안동일하이빌 121동 902호(331-090), 전화 : 041) 530-1323, FAX : 041) 530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2012년 8월 6일, 수정일 : 2012년 10월 11일
완료일 : 2012년 12월 17일
† 준회원, 순천향대학교 컴퓨터소프트웨어공학과
(E-mail : kimsh@sch.ac.kr)
†† 종신회원, 순천향대학교 컴퓨터소프트웨어공학과

작동 가능한 자동 사고예방 감지시스템 개발을 통해 도로통행의 3대 요소인 '운전자-도로-차량' 간 '역할 재조정'과 '안전성 확보'가 핵심목표이다. 즉, IT기술을 도로와 자동차기술에 접목하여 자동차-운전자-도로시설 간 정보의 공유와 통신-제어(communication & control)를 통해 운전자의 역할(피로도)은 감소시키며 편의성을 높임으로써 초고속 안전주행을 보장하고 도로용량(Road capacity)[1]을 증가시키는 것이 SMART Highway의 구현목표이다.

SMART Highway의 도로-자동차 기반 교통운영의 핵심기술인 VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 한 형태로, 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU(Road Side Unit)사이의 통신을 제공하는 차세대 네트워킹 기술이다[2].

이러한 VANET은 일반적으로 V2V(Vehicle to Vehicle)통신 또는 V2I(Vehicle to Infrastructure) 통신으로 구분된다. V2V 통신은 RSU와 같은 인프라와의 통신 과정 없이 차량과 차량의 통신으로 주변 도로 상황이나 교통사고와 같은 응급 상황 전파를 통해 돌발 상황에 빠르게 대처할 수 있도록 안전 서비스 제공에 주로 사용된다. 특히, 운전자의 안전에 직접적인 영향을 끼칠 수 있는 V2V 통신의 경우 차량 간의 안전한 통신을 위해 안전한 키 교환이 반드시 고려되어야 한다. 이처럼 빠른 속도로 이동하는 차량 간 안전한 키 교환이 원활이 이루어지기 위해서는 기존의 네트워크상에서 사용된 방식을 그대로 적용시키기 어렵다. 따라서 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적이고 안전한 키 교환을 위해 블룸필터와 사인크립션을 이용한 차량 인증 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 보안요구사항에 대해 설명하고, 3장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 연구들을 소개한다. 4장에서는 제안방식에 대하여 설명한다. 5장에서는 제안 방식에 대한 효율성을 분석하고, 마지막으로 6장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

1) 도로의 한 지점을 주어진 상황 하에서 일정시간동안 실제적으로 통과할 것으로 기대되는 차량이나 사람의 최대 통과 용량

2. 보안요구사항

VANET에서는 차량 정보 위변조, 도청, 메시지 변조, 신분의 노출 등 여러 가지 위험에 노출되어 있다. 이러한 보안 문제를 해결하고, 안전한 차량 네트워크 서비스를 제공하기 위해서 다음과 같은 보안 요구 사항을 만족해야 한다[3].

- 인증 (Authentication) : 차량 간 송수신되는 메시지에 대한 출처가 정당한 그룹 구성원이라는 것을 검증 할 수 있어야 한다.
- 부인방지 (Non-repudiation) : 개인 서명 된 메시지에 대해 그룹 구성원은 부인 할 수 없어야 한다.
- 추적성 (Traceability) : 차량 메시지에 의한 분쟁 발생 시 그룹 관리자 비밀키에 의해 서명으로부터 신원추적이 가능해야 한다.
- 비연결성 (Unlinkability) : 각기 다른 메시지와 서명 쌍이 주어져도 동일한 그룹 소속원에 의한 서명인지 알 수 없어야 한다.
- 조건부 프라이버시 (Conditional Privacy) : 차량 운전자의 안전에 직접적 영향을 줄 수 있는 메시지에 대한 출처를 제 3자가 알 수 없어야 한다. 이러한 프라이버시 제공 기술뿐만 아니라 분쟁이 발생할 경우 그룹 서명된 메시지는 그룹 관리자에 의해 개봉되어 신분을 확인 할 수 있어야 한다.

3. 관련연구

3.1 사인크립션(Signcryption)

Zheng은 암호화 기능과 서명기능이 혼합된 사인크립션 기법을 1997년에 제안하였다. 사인크립션은 곱셈군 기반에서 서명과 암호화를 논리적인 하나의 단계에서 동시에 실행함으로써 계산 시간이 현저히 줄어드는 효율적인 암호화 기법이다[4]. 그리고 1998년에는 타원 곡선에서 덧셈군을 기반으로 한 기법을 제안하였다[5]. 표 1은 Zheng이 제안한 사인크립션에 사용되는 파라미터 값이고, 표 2는 사인크립션과 언사인크립션이 수행되는 과정으로, s와 w의 계산 과정에 따라 3가지의 방법이 존재한다(표 3).

3.2 블룸 필터(Bloom Filter)

블룸필터는 Bloom에 의해서 제안된 통계적 특성

표 1. 사인크립션에서 사용되는 파라미터

Parameters public to all	p - a large prime number q - a large prime factor of p-1 g - an integer with order q modulo p chosen randomly from [1,⋯,p-1] G, H - a one-way hash function whose output has, say, at least 128 bits (E, D) - the encryption and decryption algorithms of a private key cipher
Alice's keys	x_a - Alice's private key, chosen uniformly at random from [1,⋯,q-1] y_a - Alice's public key ($y_a = g^{xa} \bmod p$)
Bob's keys	x_b - Bob's private key, chosen uniformly at random from [1,⋯,q-1] y_b - Bob's public key ($y_b = g^{xb} \bmod p$)

표 2. 사인크립션 기본 프로토콜

Alice(Signcryption)	Bob(Unsigncryption)
① $random\ x \in_r \{1,\ldots,q-1\}$	
② $w = y_b^x \bmod p$	⑧ $w = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$
③ $k = G(w)$	⑨ $k = G(w)$
④ $r = H(w,m)$	⑩ $m = D_k(c)$
⑤ $s = x/(r + x_a) \bmod q$	⑪ $if(r ? = H(w,m))$
⑥ $c = E_k(m)$	m 수락
⑦ (c,r,s) 전송	

표 3. s와 w의 계산 방식에 따른 기법

Alice(Signcryption)	Bob(Unsigncryption)
① $s = x/(r + x_a) \bmod q$	① $w = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$
② $s = x/(1 + x_a \cdot r) \bmod q$	② $w = (g \cdot y_a^r)^{s \cdot x_b} \bmod p$
③ $s = (x - x_a \cdot r) \bmod q$	③ $w = (g^s \cdot y_a^r)^{x_b} \bmod p$

을 가진 자료구조로써, 데이터를 공간 효율적으로 빠르게 검색할 수 있다는 장점이 있다[6]. 이러한 블룸필터는 많은 양의 데이터를 매우 작은 공간을 사용하여 저장할 수 있고, 검색 방식에 따라 다양한 환경에 적용시켜 효율적인 활용이 가능하다.

블룸필터는 m개의 비트를 가진 하나의 비트 백터(bit vector) B이며, n개의 엘리먼트를 가진 유한 집합 S={x_1, x_2, ... ,x_n}에 각각의 요소가 포함되어 있는지 쉽게 확인 가능하도록 해준다. 각 요소를 블룸필터에 맵핑(mapping) 시키기 위해서는 서로 독립적인 k개의 해시(hash)함수를 사용하여 비트벡터 B의 비트 주소공간에 맵핑(mapping)시킨다(그림 1).

일반적으로 저장된 데이터에 대해 접근하고자 할

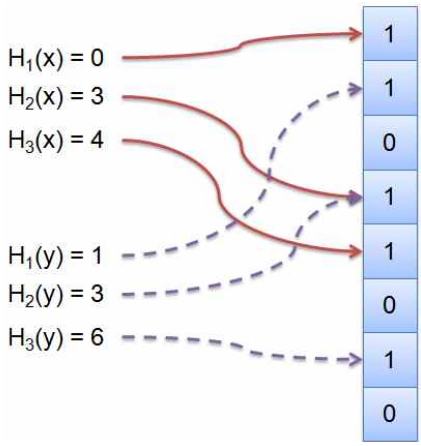

그림 1. 블룸필터 구조의 예시

경우 느린 데이터 저장소에 접근하여 데이터가 있는지 판단하는 것은 오랜 시간이 걸려 비효율적이다. 이에 일정한 공간을 미리 할당하여 해당 저장소의 정보를 간소화한 정보로 존재 유무를 판단할 근거 테이블을 제작하고 이 곳에 미리 접근하여 해당 데이터가 있는지 파악 후 검증이 되면 저장소의 정보에 접근하는 구조를 따르게 된다. 실제로 스펠링 체크, 사전, 웹 검색에 이르기까지 다양한 분야에 사용되고 있고, 구글의 파일 시스템(GFS)의 접근 시스템에서도 Big Table을 두어 상당한 성능 향상을 얻고 있다.

본 논문에서는 블룸필터를 그룹키 검증의 용도로 사용하고 있으며, 이는 차량 자체에서 그룹키를 갱신할 수 있게 한다. 이러한 방식을 사용함으로써 RSU가 그룹키를 생성하고, 브로드 캐스팅하는 비용을 현저히 줄일 수 있으며, RSU에 집중된 연산을 분산 시킬 수 있다는 장점이 있다.

3.3 다자간 그룹키 확립 프로토콜

VOD(Video-on-Demand) 서비스 및 화상회의처

럼 그룹에 속한 멤버들에게만 비밀스럽게 데이터를 전송해야 하는 경우가 있다. 이때 각 사용자마다 다른 비밀키로 암호화하여 전달하는 것은 네트워크 대역폭 측면이나 연산량 측면에서 비효율적이다. 비밀성이 요구되지 않을 경우에는 IP 멀티캐스트(Multicast) 기법을 사용하면 하나의 메시지를 이용하여 다자에게 네트워크 대역폭을 가장 효율적으로 활용하여 전달할 수 있다. 비밀성이 요구되었을 때 IP 멀티캐스트를 활용하기 위해서는 그룹에 속한 모든 멤버들이 같은 비밀키를 공유해야 한다. 이를 위해 사용되는 암호프로토콜을 다자간 키 확립 프로토콜이라 하며, 이와 같은 프로토콜을 다른 말로 그룹키(Group Key)확립 프로토콜이라 한다. 그룹키 확립 프로토콜의 요구사항은 기존 키 확립 프로토콜의 요구사항을 모두 충족해야 하며, 추가적으로 다자가 참여하기 때문에 발생되는 요구사항을 충족해야 한다. 다만, 모든 그룹 멤버가 동일한 키를 가지고 있는지 확인하는 것은 현실성이 없으므로 보통 키 확인 과정이 없다.

소규모 그룹인 경우에는 전체적인 연산량이 큰 문제가 되지 않을 수 있지만 대규모의 그룹인 경우에는 효율성이 매우 중요한 요소가 되며, 이 효율성은 확장성과도 매우 밀접한 관련이 있다. 그룹키 확립 프로토콜에서 기존과 가장 큰 차이가 있는 부분은 그룹의 동적성이다. 그룹의 동적성이란 그룹의 멤버들이 변경될 수 있다는 것을 말한다. 그런데 멤버가 변경되면 안전성을 위해 보통 그룹키도 바꾸어야 한다. 이 때 모든 사용자가 프로토콜에 참여해야 하면 확장성 때문에 현실적으로 사용하기가 힘들다. 또한 멤버가 빈번하게 변경되면 그룹키 갱신이 매우 효율적이어야 한다.

VANET환경에서는 이러한 그룹 동적성의 특징이 가장 잘 나타나는 환경이다. 통신 범위 내에서 차량간 안전한 통신을 위해 그룹키를 확립하여 비밀통신이 이루어지게 되는데, VANET환경의 특성상 차량이 빠른 속도로 이동하게 되므로 그룹 멤버의 가입과 탈퇴가 빈번하게 이루어진다. 따라서 VANET 환경에 적합한 그룹키 확립 프로토콜의 연구가 필요한 실정이다.

3.4 그룹서명이 적용된 차량 통신

최근 차량 통신에 관한 연구가 활발히 이루어지면서 VANET의 보안요구사항을 만족시키기 위해 기밀성 및 인증, 조건부 프라이버시의 기능을 제공하는 다양한 그룹 서명 기법들이 제안되고 있다.

Zhang 등은 VANET에서 인증 및 조건부 프라이버시를 제공하기 위해 그룹 서명을 사용하고, 차량 그룹 관리자에 의해 그룹 개인키 폐기과정을 제안하였다[7]. Hao 등도 역시 그룹 서명을 적용하여, 안전한 그룹 개인키 분배 프로토콜을 제안하였다[8]. Sun 등은 분산 키 관리 체계(DKM)를 통하여 지역 그룹 관리자가 그룹 비밀키를 업데이트하는 프로토콜을 제안하였다. 하지만 이 방식은 그룹 비밀키 폐기 과정에 대한 비용만을 감소하였을 뿐, 갱신 및 분배에 대해서 언급되지 않았다[9].

이와 같이 기존의 제안된 방식들은 인증 및 조건부 프라이버시 기능은 제공하고 있지만, 사용된 그룹 서명 기법은 VANET 환경에 적합하지 않은 방식으로, 효율적인 그룹 구성에 관한 기능은 제공하고 있지 않다. 또한 그룹 관리자 차량을 통해 그룹을 구성시, 그룹 관리자 차량 자체에 대한 인증이 이루어지지 않아 키 위탁문제가 발생하게 된다.

4. 제안 방식

4.1 시스템 모델 및 가정

제안하는 시스템에서 모든 OBU(On-Board Unit: 차량에 탑재된 통신기기)은 차량에 탑재되기 전 TA(Trusted Authority: 신뢰기관)에 사전등록이 된다.

또한 OBU의 TRH(Temper Resistant Hardware: 조작 불가능한 하드웨어)를 이용하여 통신 시 모든 연산을 수행하게 되고, 통신 범위 내에서 그룹을 생성하기 위해 RSU(Road Side Unit: 도로 주변에 위치한 통신장치)는 통신 범위에 도달하는 차량에게 메시지를 보내 하나의 통신 그룹을 형성하게 된다. RSU는 항상 신뢰받는 객체이며, OBU에 비하여 월등한 연산능력을 가지고 있다고 가정한다.

4.2 제안방식 시나리오

차량이 도로 상에 일정 간격으로 배포되어 있는 RSU의 통신범위에 도달하였을 때, 차량과 RSU는 차량 등록 및 그룹키 발급 과정을 거치게 된다. 이 때, 그룹키는 RSU의 통신범위를 벗어나기 전까지 최초 1회만 수신 받게 된다. 이 후에 RSU는 차량에게 그룹키 갱신에 필요한 정보와 갱신된 그룹키를 검증

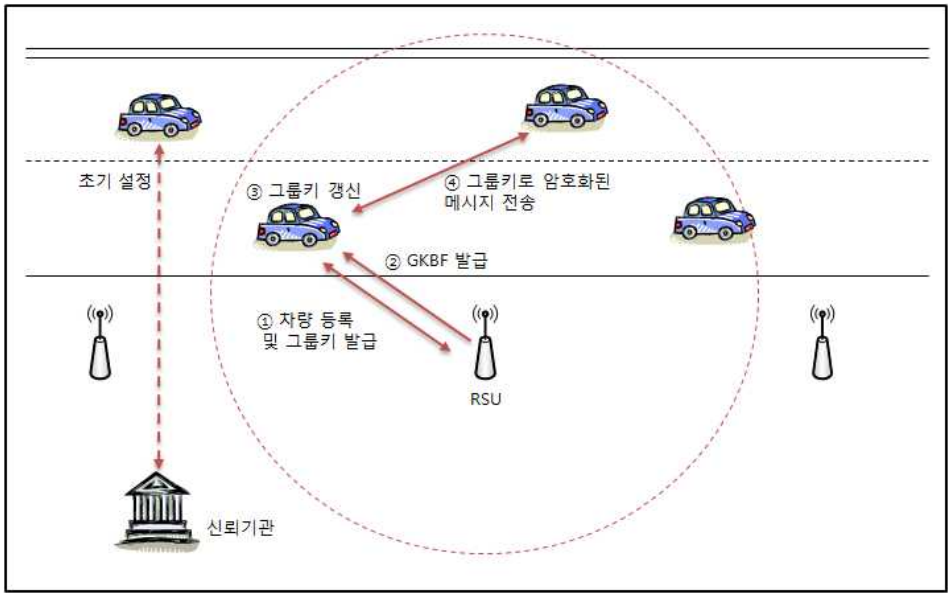

그림 2. 제안방식 시나리오

할 수 있는 블룸필터 정보를 송신하고, 차량은 RSU로부터 받은 값을 통해 차량 자체에서 그룹키를 갱신하게 된다. 갱신된 그룹키는 RSU로부터 받은 블룸필터 값과 비교하여 정상적으로 그룹키가 갱신되었음을 알게 된다. 차량은 정상적으로 갱신된 그룹키를 이용하여 통신범위 내의 차량들과 메시지를 송수신하게 된다(그림 2).

4.3 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.

- RID_* : OBU에 의해 생성된 차량 *의 식별자
- PID_* : 차량 *의 $(ID*_1, ID*_2)$ 쌍
- P : 타원 곡선상위의 점
- G : P에 의해 생성되는 순환군
- q : G의 위수
- y_* : *의 공개키($y_*=g^{x*} \bmod p$)
- x_* : *의 개인키
- 공개 파라미터 : (G, q, P)
- GK_* : 차량 *의 초기 그룹키 값
- GKBF : 차량에서 갱신된 그룹키를 검증하기 위해 RSU로부터 전송되는 그룹키 블룸필터 값
- s, i : 그룹키를 갱신하기 위해 RSU로부터 차량으로 전송되는 인자값
- TS : 타임스탬프
- T_{REVOK} : 그룹키 폐기 시간
- r_* : *의 랜덤값
- H_1, H_2 : 일방향 해쉬함수
- $CERT_*$: *의 인증서

4.4 초기 설정 단계

차량 V는 TA(Trust Authority)를 통해 공유한 공개 파라미터 G, q, P를 이용하여 PID쌍 (ID_{V1}, ID_{V2})를 생성한다.

- $ID_{V1}=r_V \cdot P$
- $ID_{V2}=RID \cdot H(r_V \cdot y_V)$
- $PID_V=(ID_{V1}, ID_{V2})$

4.5 차량 등록 과정

최초 그룹 구성 시 RSU는 통신 범위에 도달하는 모든 차량에게 그룹 참가 메시지를 보내 하나의 통신 그룹을 형성하게 된다.

Step 1: RSU는 통신 범위에 도달하는 차량들에게 RSU의 식별자가 포함된 인증서와 그룹키를 차량의 공개키로 암호화하여 전송하게 된다.

- RSU→V :

$$E_{yV}(GK_V||s||TS||T_{REVOK}||CERT_{RSU})$$

Step 2: RSU의 인증서에 포함된 식별자를 확인한 차량은 사전에 생성한 자신의 PID와 함께 RSU의

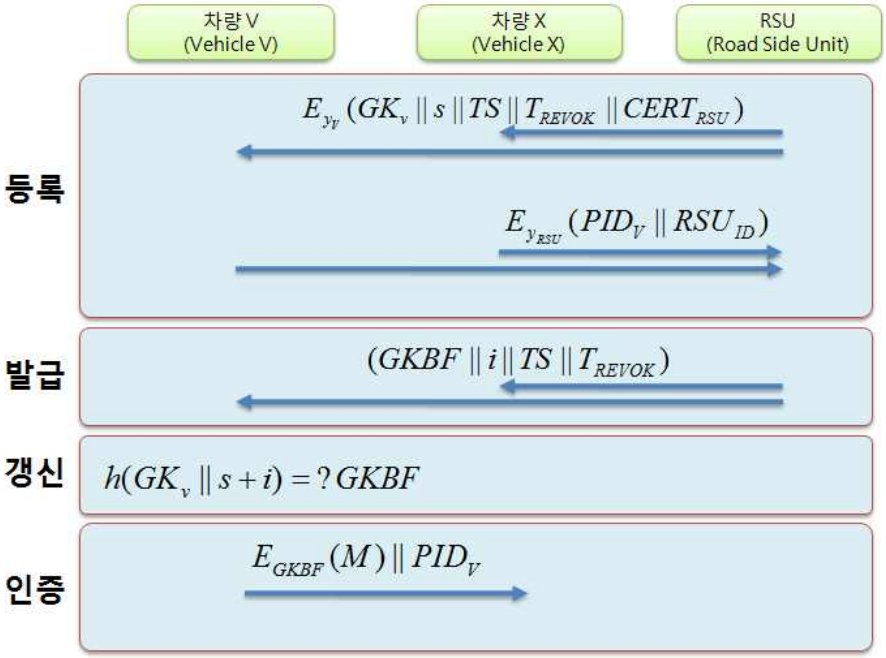

그림 3. 전체 프로토콜

공개키로 암호화 한다. 차량은 RSU에게 수시로 메시지를 보내면서 통신 범위 내의 그룹에 속해 있음을 알린다.

-V→RSU : $Ey_{RSU}(PID_V||RSU_{ID})$

4.6 그룹키 발급 단계

RSU는 같은 그룹으로 구성된 차량에게 새롭게 갱신될 그룹키의 블룸필터 값을 전송하게 된다. 차량은 RSU로부터 사인크립션을 통해 받은 그룹키의 블룸필터 값과 차량자체에서 갱신한 그룹키의 블룸필터 값을 비교하여 올바르게 갱신되었는지 검증할 수 있다. RSU가 모든 차량의 그룹키를 갱신하지 않고, 차량이 직접 하게 되며 간단한 과정으로 정당한 그룹키인지 검증 가능하기 때문에 RSU에게 집중된 그룹키 갱신 연산을 분산시킬 수 있다.

Step 1: RSU는 최초 그룹키 검증에 필요한 정보를 사인크립션(Signcryption)기법을 적용시킨 후 차량에 전송해 주게 된다. 이 때, 전송되는 메시지는 사인크립션을 통해 RSU의 서명과 메시지에 대한 암호화가 동시에 이루어진다. RSU가 전송하는 메시지는 새롭게 갱신될 그룹키의 블룸필터 값(GKBF)과 그룹키 갱신에 필요한 인자값(i), 타임스탬프(TS), 그룹키 폐기시간(T_{REVOKE})을 포함한다.

- RSU→V :

랜덤값 x 선택

$w = y_{RSU}^{x} \bmod p$

$k = H_1(w)$

$r = H_2(m, RSU_{ID}, w)$

$s = x/(r + x_V) \bmod q$

$c = E_k(m)$

$m = (GKBF \| i \| TS \| T_{REVOK})$

(c, r, s) 전송

Step 2: 차량은 RSU로부터 사인크립션 과정을 거친 메시지를 수신 받은 후, 언사인크립션(Unsign-cryotion)을 통해 RSU에 대한 인증과 메시지에 대한 복호화를 수행한다. (c, r, s)를 수신 받은 차량 V는 w와 메시지 m을 구한 뒤, RSU_{ID}를 이용해 r을 생성하게 된다. 수신 받은 r값과의 비교를 통해 정상적으로 언사인크립션이 이루어졌는지 검증한다.

- V :

$w = (y_V \cdot g^{r})^{s \cdot x_{RSU}} \bmod p$

$k = H_1(w)$

$m = D_k(c)$

$r? = H_2(m, RSU_{ID}, w)$

4.7 그룹키 갱신 단계

차량 V는 그룹키 발급 단계에서 RSU로부터 그룹키 갱신에 사용될 인자값 i와 새롭게 갱신된 그룹키

값 검증에 필요한 GKBF를 수신 받게 된다. 차량 V는 최초 수신 받은 그룹키 GK_V와 i값을 이용하여 새로운 그룹키를 갱신하게 된다. 그 후 GKBF와 비교를 통해 올바르게 갱신되었는지 검증할 수 있다.

- V : $h(GK_V||y+i)=?GKBF$

4.8 차량 간 인증 단계

도로 상의 모든 차량은 통신 범위 내에서 새롭게 갱신된 그룹키를 통해 모든 메시지를 암호화 하여 송수신 하게 된다. 이 때, 각 차량은 동일한 그룹키를 사용함으로써 메시지 복호화가 가능하고, 일정한 통신 범위 내에서 정당한 인증을 받은 차량임을 검증할 수 있다.

- $V_1 \rightarrow V_2$: $E_{GKBF}(M)||PID_{v1}$

5. 제안 방식 분석

본 장에서는 기존 그룹 서명을 이용한 기법[7]과 본 논문의 제안방식을 비교하여 기존 방식에 비해 블룸필터를 사용한 제안 방식이 어느 측면에서 보다 더 효율적인지에 대해 분석하여 본다.

5.1 그룹키 발급 횟수

Smart highway 환경에서는 고속도로 상에서 차량의 속도가 평균 160Km를 유지하는 것을 목표로 하기 때문에, WAVE(Wireless Access for Vehicle Environments : 5.9GHz 대역에서 V2V와 V2I 통신을 모두 지원하는 기술)통신의 범위 2Km를 통과하기까지 약 44초의 시간이 걸린다. 이를 실제 환경에 적용한다고 가정하였을 경우 다양한 환경적 요인을 감안하여 60초의 시간동안 발생할 수 있는 RSU로부터 발급되는 그룹키 전송횟수를 비교하였다.

RSU의 통신 범위 내에 50~300대의 차량이 각각 존재한다고 가정하였다. 일반적인 VANET환경에서는 300ms 마다 통신을 수행하므로, RSU가 수행해야 할 그룹키 발급횟수는 차량 대수에 비례하여 급격히 증가한다. 하지만 본 제안방식에서 각 차량은 최초 전송받은 그룹키를 통해 동일한 인자값을 기반으로 차량 자체에서 그룹키를 갱신하기 때문에 통신범위 내의 차량 대수가 증가하더라도 차량 당 최초 1회의 통신만으로 그룹키 갱신이 이루어진다. 그림 4는 본 제안방식과 기존의 그룹서명을 사용할 경우 발생할 수 있는 차이를 비교한 그림이다. 단, 통신범위를 벗어나는 차량의 경우 그룹키 폐기 시간이 포함된 메시지를 통해 일정시간이 지난 후, 이전의 그룹키 목록을 삭제하게 된다.

5.2 그룹키 갱신 연산 효율

본 제안방식은 새롭게 갱신되는 그룹키 목록을 해쉬값을 취하여 생성된 블룸필터를 전송해줌으로써 차량 자체에서 갱신, 검증이 가능한 방식이다. 따라서 RSU가 매번 그룹키를 갱신하여 암호화 한 뒤 브로드캐스팅하는 기존 방식과 비교하여, RSU에게 집중된 연산을 분산시킬 수 있다는 장점이 있다. 또한

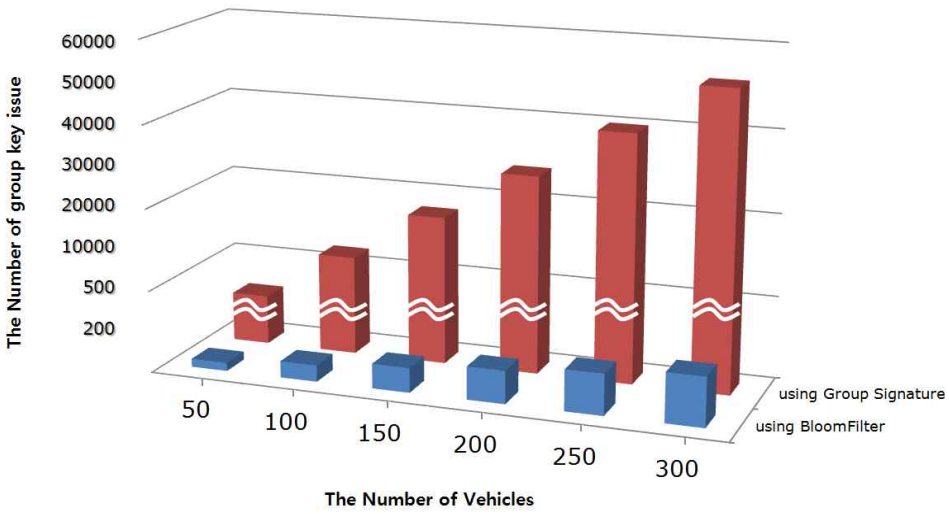

그림 4. RSU로부터의 그룹키 발급 횟수

사인크립션을 이용함으로써 RSU에 대한 인증과 메시지에 대한 암호화를 동시에 적용시킬 수 있다. 이는 기존 공개키 시스템과 비교하여 보다 효율적이라 할 수 있다.

본 절에서는 각각 RSU와 차량에서 발생하는 연산량에 대하여 기존 방식과 비교하여 본다. 비교를 위해 필요한 식에 사용된 계수는 아래와 같다.

- N_v : 차량 대수
- T : 그룹키 갱신 횟수
- E_T : 암호화 소요시간(128bit AES 알고리즘)
- D_T : 복호화 소요시간(128bit AES 알고리즘)
- H_T : 해쉬를 취하여 블룸필터를 생성하는 시간(128bit MD5 알고리즘)
- T_{VERIFY} : 갱신된 그룹키를 검증하는데 소요되는 시간(순차탐색)
- RSU_{GS} : 그룹서명을 적용한 RSU의 그룹키 갱신 소요시간
- RSU_{Bloom} : 블룸필터를 적용한 RSU의 그룹키 갱신 소요시간
- V_{GS} : 그룹서명을 적용한 차량별 그룹키 갱신 소요 시간
- V_{Bloom} : 블룸필터를 적용한 차량별 그룹키 갱신 소요 시간

RSU_{GS}와 RSU_{Bloom}은 각각 아래 식1과 식 2로 표현할 수 있다.

$$RSU_{GS} = N_v \times T \times E_T \quad (1)$$

$$RSU_{Bloom} = N_v \times H_T \quad (2)$$

그룹키 갱신을 위한 통신은 매 초마다 이루어진다고 가정하였으며, RSU_{Bloom}은 한 번의 통신만으로 이루어지기 때문에 별도로 시간 값은 포함되지 않는다. RSU_{GS}는 차량의 수에 비례하여, 차량이 많아질수록 그룹키 갱신에 걸리는 시간은 급격히 증가하게 된다. 반면 RSU_{Bloom}은 차량 수에 비례하여 증가하긴 하지만, 각 차량별로 최초 1회만 통신을 하기 때문에 RSU_{GS}에 비해 높은 효율을 얻을 수 있다(그림 5).

V_{GS}와 V_{Bloom}은 각각 아래 식 3과 식 4로 표현할 수 있다.

$$V_{GS} = T \times D_T \quad (3)$$

$$V_{Bloom} = T(H_T + T_{VERIFY}) \quad (4)$$

V_{GS}는 각 차량들이 그룹키를 갱신하기 위해 RSU로부터 전송 받은 암호화된 그룹키를 복호화하는데 걸리는 시간이며, V_{Bloom}은 최초 수신 받은 그룹키에 대해서 다음에 사용될 그룹키를 갱신하는데 걸리는 시간이다. 이 때, T_{VERIFY}는 차량 자체에서 갱신된 그룹키를 RSU로부터 받은 블룸필터와 비교하여 정상적으로 그룹키가 갱신되었는지 검증하는 과정이다. 블룸필터를 검색하는 과정에서 순차탐색(linear search) 방식을 따른다고 가정하였을 경우, O(n)만큼의 복잡도를 가진다(그림 6).

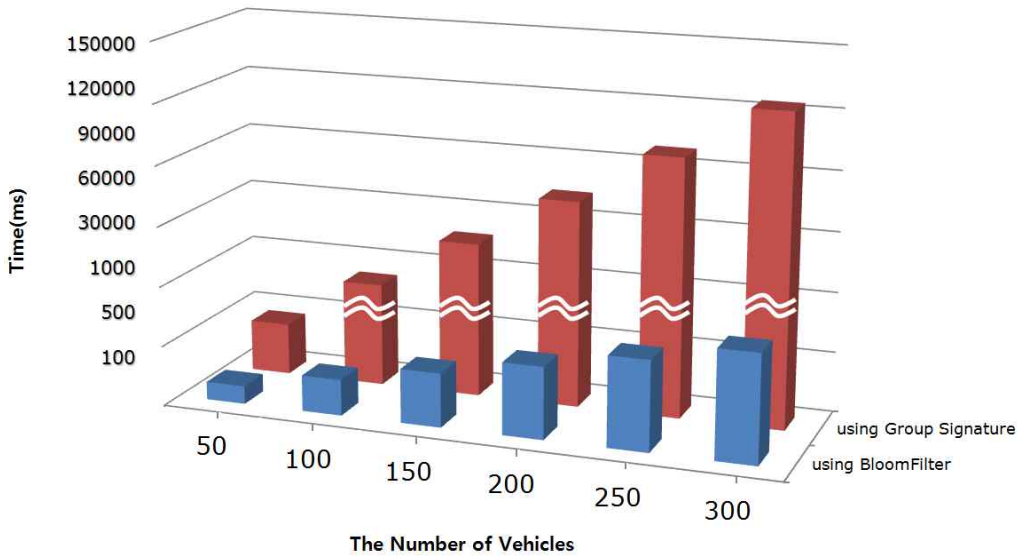

그림 5. RSU의 그룹키 갱신 소요시간 비교

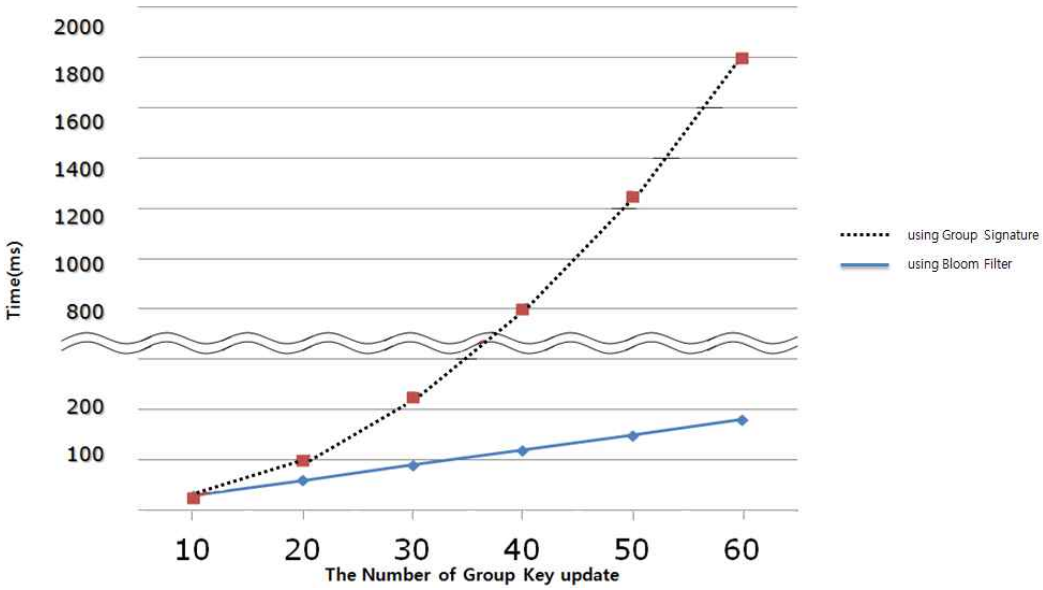

그림 6. 차량의 그룹키 갱신 횟수 별 소요시간 비교

5.3 후방향 안전성

그룹을 구성하여 통신을 하는 경우, 그룹의 멤버가 탈퇴 시 새로운 그룹키를 확립하여 데이터를 암호화 하여야 한다. 새로운 그룹키를 사용하는 경우, 저장되어 있는 데이터 또한 모두 다시 암호화과정을 거쳐야 하기 때문에 엄청난 오버헤드를 가져오게 된다. 하지만 본 제안방식에서 RSU는 그룹 구성원에게 데이터 암호화 키, 즉 그룹키를 매번 새롭게 생성하여 송신할 필요가 없다. 또한, 새로운 그룹키는 해쉬함수에 의해 갱신되어 검증이 이루어지므로 새로 가입한 멤버 차량이나 현재 그룹키를 알고 있는 공격자도 이전 그룹키를 유추할 수 없다.

5.4 인증 및 기밀성

RSU에 대한 인증과 데이터 전송 시 통신로 상에서의 기밀성을 제공해야 한다. 하지만 기존의 공개키 암호 시스템을 사용할 경우, 비용적, 연산적 측면에서 매우 비효율적이다. 본 제안방식에서는 암호화와 인증이 동시에 이루어지는 사인크립션기법을 적용시킴으로써 기존 공개키 암호 기법에 비해 약 50% 이상의 계산 시간을 줄일 수 있다[4].

6. 결 론

SMART Highway 환경에서는 빠른 속도로 이동하는 차량 간 안전한 키 교환이 반드시 고려되어야 한다. 따라서, 본 논문에서는 다수의 차량이 존재하는 VANET 통신환경에서 RSU에 집중된 그룹키 갱신 오버헤드를 줄이기 위해, 차량 자체에서 이루어지는 그룹키 갱신 및 검증기법을 제안하였다. 그룹키 검증 단계에서는 블룸필터를 활용하여 통신 횟수 및 소요시간에 대한 효율성을 극대화 시켰다.

향후에는 본 논문에서 제안한 기법을 기반으로 다양한 환경적 요인을 고려한 시뮬레이션을 구축하여, 기존의 다양한 기법들과 보다 구체적으로 비교 분석이 필요할 것으로 사료된다.

참 고 문 헌

[1] 이기영, 이혁준, “스마트하이웨이를 위한 유비쿼터스 교통정보 서비스 시스템,” 정보과학회지, 제27권, 제9호, pp. 34-40, 2009.

[2] 이지훈, 김대엽, “차량 간 통신을 이용한 저비용 사고 위험 방지 기술에 관한 연구,” 멀티미디어학회논문지, 제15권, 제19호, pp. 1221-1227, 2012.

[3] M. Raya, P. Papadimitrators, and J. Hubaux, “Securing Vehicular Communications,” *Magazine of IEEE Wireless Communications-IVC Specials, EPFL, Volume 13, Issue 5,* pp. 8-15, 2006.

[4] Y. Zheng, “Digital Signcryption or How to

Achieve Cost (Signature and Encryption) << Cost(Signature)+Cost(Encryption)," *Advances in Cryptology, Proc. CRYPTO'97, LNCS*, Vol. 1294, pp. 165- 179, 1997.

[5] Y. Zheng, "Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes," *IEEE P1363a: Standard Specifications for Public-key Cryptography : Additional Techiques,* 1998.

[6] B. Bloom, "Space/Time Trade-Offs in Hash Coding with Allowable Errors," *Comm. ACM*, Vol. 13, No. 7, pp. 422-426, 1970.

[7] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," *Proc. the First International Symposium on Data, Privacy, and E- Commerce*, pp. 138-142, 2007.

[8] Y. Hao, Y. Cheng, and K. Ren, "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs," *Proc. IEEE Global Telecommunications Conference,* pp. 1-5, 2008.

[9] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An Efficient Distributed Key Management Scheme for Group-Signature Based Anonymous Authentication in VANET," *Security and Communication Networksm,* Vol. 5, Issue. 1, pp. 79-86, 2012.

김 수 현

2010년 2월 순천향대학교 정보기술공학부 졸업
2012년 2월 순천향대학교 컴퓨터학과 석사
2012년 3월~현재 순천향대학교 컴퓨터학과 박사과정
관심분야: VANET, 전자서명. 인증

이 임 영

1981년 2월 홍익대학교 전자공학과 졸업
1986년 2월 오사카대학 통신공학전공 석사
1989년 2월 오사카대학 통신공학전공 박사

1985년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 컴퓨터학부 교수
관심분야: 암호이론, 정보이론, 컴퓨터 보안