情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

VANET환경에서의 효율적인 그룹서명기반 메시지 인증 기법에 관한 연구*

김 수 현†, 이 임 영‡
순천향대학교 컴퓨터소프트웨어공학과

A Study on Message authentication scheme based on efficient Group signature in VANET*

Su-Hyun Kim†, Im-Yeong Lee‡
Department of Computer Software Engineering Soonchunhyang University

요 약

VANET(Vehicular Ad-hoc Network)는 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. 특히, 운전자의 안전에 직접적인 영향을 끼칠 수 있는 V2V 통신의 경우 차량 간의 안전한 통신을 위해 차량 인증 및 조건부 프라이버시 보호 등이 반드시 고려되어야 한다. 이를 제공하기 위해서 인증 및 조건부 프라이버시, 부인방지 기능을 제공할 수 있는 그룹 서명 기법을 사용한 보안 기술들이 다양하게 연구되고 있다. 본 논문에서는 빈번한 가입과 탈퇴로 인한 불필요한 통신을 최소화 하고, 그룹 관리자에 의해 생성되는 차량 개인서명키에 대한 키 위탁문제를 해결하기 위한 그룹서명방식을 제안한다. 또한 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적인 메시지 검증을 위해 BloomFilter를 이용한 메시지 일괄 검증 기법을 제안한다.

ABSTRACT

VANET (Vehicular Ad-hoc Network) is a type of MANET (Mobile Ad-hoc Network) which is the next-generation networking technology to provide communication between vehicles or between vehicle and RSU (Road Side Unit) using wireless communication. In VANET system, a vehicle accident is likely to cause awful disaster. Therefore, in VANET environment, authentication techniques for the privacy protection and message are needed. In order to provide them privacy, authentication, and conditional, non-repudiation features of the group signature scheme using a variety of security technologies are being studied. In this paper, and withdrawal of group members to avoid frequent VANET environment is suitable for vehicles produced by the group administrator for a private signing key to solve the key escrow problem of a group signature scheme is proposed. We proposed a message batch verification scheme using Bloom Filter that can verify multiple messages efficiently even for multiple communications with many vehicles.

Keywords: VANET, V2I, V2V, Group Signature, Authentication, Privacy

접수일(2011년 7월 6일), 수정일(2011년 11월 20일)
게재확정일(2012년 1월 18일)
* 이 논문은 2010년도 순천향대학교 교수 연구년제에 의하여 연구하였습니다.

† 주저자, kimsh@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

I. 서 론

최근 IT기술을 차량에 접목시키려는 노력이 가속화되고 있다. 휴대 단말기에 사용되었던 다양한 서비스들이 향후에는 차량에 적용됨으로써 이동형 에드 혹 네트워크의 유망한 응용환경으로 주목받고 있다. 이러한 서비스는 C2E(Car to Enterprise), C2C(Car to Car), C2H(Car to Home)에서 이루어지며 그 종류는 매우 다양하다.

그 중 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.

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. 이처럼 V2V통신은 내부 네트워크 참여자에 의한 차량과 차량의 통신에 의존하기 때문에 송수신 되는 모든 정보가 운전자의 안전에 치명적인 영향을 끼치게 됨으로써 다양한 보안요구사항을 만족해야 한다. 이를 제공하기 위해서 인증 및 조건부 프라이버시, 부인방지 기능을 제공할 수 있는 그룹 서명 기법을 사용한 보안 기술들이 다양하게 연구되고 있다[1]. 하지만 기존의 그룹 서명 기법을 VANET환경에서 적용하기에는 여러 가지 문제점을 가지고 있다. VANET은 MANET과 달리 노드가 빠른 속도로 이동하기 때문에 그룹 구성원의 빈번한 가입 및 탈퇴에 따른 통신 오버헤드가 매우 높고, 계산 효율성이 낮다는 문제점을 가지고 있다.

이에 따라 본 논문에서는 키 위탁문제를 해결하고, 빈번한 그룹 가입 및 탈퇴로 인한 불필요한 통신횟수를 최소화하기 위해 차량의 속도를 고려한 일정 시간 간격의 가입요청 메시지를 적용한 그룹 서명 방식을 제안하였다. 또한 실시간으로 처리되어야 하는 메시지의 특성에 따라 BloomFilter를 이용한 메시지 일괄 검증 방식을 제안하였다. 본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 기술들을 소개하고, 3장에서는 VANET이 갖추어야 할 기본적인 보안 요구사항에 대하여 알아보고, 4장에서는 제안 방식에 대하여 설명한다. 5장에서는 제안 방식의 안전성을 분석한고, 마지막으로 6장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

II. 연구배경

본 장에서는 VANET환경에서 다양한 서비스를 제공하기 위해서 차량 통신 환경에서의 보안 취약성을 분석하고, 이에 따른 보안요구사항에 대해 알아본다.

2.1 VANET에서의 보안 요구사항

본 절에서는 프라이버시를 보장하는 V2V 인증 시스템을 위한 보안 요구사항을 정의한다. 모든 V2V 통신은 무선 통신을 이용하여 데이터를 주고받으므로 DoS 공격, 통신 방해, 재생 공격(replay attack), 위조 공격, 및 ID 노출 공격 및 차량 추적 등의 여러 가지 위험에 노출되어 있다. 이와 같은 위협을 막기 위해서는 다음의 보안 요구사항을 만족해야 한다.

- 인증(Authentication) : 수신자는 전송된 메시지가 정당한 사용자로부터 생성된 메시지임을 검증할 수 있어야 한다. 전통적인 공개키 기반 인증 시스템과는 달리 익명성 지원을 위해 정당한 사용자를 시스템의 신뢰기관에 등록되어 있는 탈퇴되지 않은 정당한 키를 소유한 사용자를 말한다.
- 익명성(Anonymity): 공격자가 V2V 메시지들을 캡쳐하더라도 이러한 메시지들로부터 송신자에 대한 어떠한 신원 정보도 알 수 없어야 함을 의미한다.
- 부인방지 (Non-repudiation) : 개인 서명 된 메시지에 대해 그룹 구성원은 부인 할 수 없어야 한다.
- 추적성(Traceability) : 사고 발생 시 혹은 공격자의 출현으로 인한 피해가 발생했을 때를 대비하여 필요시 제 3의 기관이 개입하여 특정 차량에 대한 추적을 가능하게 하는 성질이다. 이 때, 제 3의 기관이 신뢰기관이 아니라면 심각한 프라이버시 침해 문제를 야기할 수 도 있다.
- 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.

III. 관련연구

3.1 그룹서명

그룹 서명 기법의 개념은 D. Chaum과 Van Heyst에 의해 최초로 제안되었다[2]. 그룹 서명 기법은 그룹 소속원의 익명을 보장하며 그룹의 소속인임을 확인하는 방식으로 그룹의 가입된 멤버만이 서명을 할 수 있다. 서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 서명을 개봉하여 서명자를 찾아 낼 수 있다. 이러한 특징들 때문에 그룹 서명 기법은 다양한 분야에서 인증 및 조건부 프라이버시, 부인방지 기능을 제공하는데 적합하다.

일반적으로 그룹 서명 기법은 SETUP, JOIN, SIGN, VERIFY, OPEN과 같은 과정으로 구성되어 있다.

- 초기구성(SETUP) : 그룹 관리자가 그룹 멤버들이 사용할 그룹 개인키와 그룹 공개키, 그룹 비밀키를 생성하는 과정이다.
- 멤버가입(JOIN) : 그룹 멤버들이 그룹에 가입하는 과정으로 가입이 완료된 사용자는 그룹 관리자로부터 그룹 서명을 생성할 수 있는 그룹 서명키를 얻게 된다.
- 서명(SIGN) : 그룹 관리자로부터 얻은 서명키를 이용하여 그룹 서명을 생성한다.
- 검증(VERIFY) : 그룹 서명키를 이용하여 수신자로부터 제공받은 서명이 정당한 그룹 멤버에 의해 서명된 것인지 확인한다.
- 개봉(OPEN) : 서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 그룹 비밀키로 서명을 개봉하여 서명자를 찾아내는 과정이다.

3.2 그룹서명이 적용된 차량 통신

최근 차량 통신에 관한 연구가 활발히 이루어지면서 VANET의 보안요구사항을 만족시키기 위해 인증 및 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[3]. Hao 등도 역시 그룹 서명을 적용하여, 안전한 그룹 개인키 분배 프로토콜을 제안하였다[4].

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

3.3 일괄검증기법이 적용된 차량 통신

일괄 검증 기법은 다수의 서명된 메시지를 하나의 서명 확인 비용으로 검증 할 수 있는 방식이다. 일괄 검증 기법의 개념은 1997년 Fiat에 의해 최초로 제안되었다[5]. 최근 이러한 기존의 일괄 검증 기법을 VANET 환경에 적용하기 위해 많은 연구가 진행되고 있다.

Zhang 등은 VANET에서 다수의 서명 메시지를 효율적으로 검증하기 위해 일괄 검증 기법을 적용하였다[6]. Zhang 등이 제안한 기법에서는 RSU가 차량을 대신하여 일괄 검증을 확인해 줄 수 있다. 이처럼 RSU를 이용하여 일괄검증을 함으로써 차량 밀도가 높은 지역에서는 효율성이 극대화 될 수 있다. 하지만 ID 기반 서명의 검증 오버헤드가 높다는 단점으로 인해 RSU당 해당 차량의 수가 적을 경우에 비효율적이다.

RAISE 기법 또한 차량 밀집 지역에서 발생하는 오버헤드 문제를 해결하기 위해 개발된 일괄 검증 기법이다[7]. RSU는 차량들이 보낸 메시지를 해쉬통합(Hash Aggregation)을 하여 수신차량에게 전송하고, 수신차량은 자신이 받은 메시지가 RSU로부터 받은 정보에 포함되어 있는지 확인비교 작업만을 수행한다. 기존의 각 노드별 연산을 통한 검증기법에 비해 효율적인 인증을 가능하게 한다. 하지만 차량의 수에 비례하여 비교연산 횟수가 많아져, n대의 차량이 존재할 경우 n번의 비교가 불가피하다.

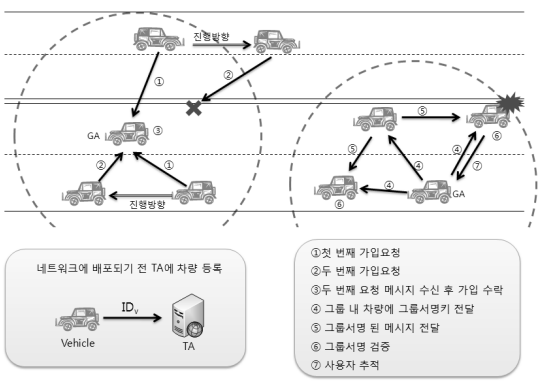
IV. 제안방식

VANET환경에서 차량 그룹 관리자보다 빠른 속도

로 이동하거나 맞은편 차선의 차량의 경우 불필요한 그룹 가입이 이루어짐으로써 통신 오버헤드가 매우 높아지는 단점을 가지고 있다. 이를 해결하기 위해 본 장에서는 기존의 그룹 서명 기법을 VANET환경에 적용하기 위해 차량의 속도를 고려한 일정 시간 간격의 가입요청 메시지를 적용하여 그룹 서명 방식을 제안하였다. 또한 송수신되는 메시지를 실시간으로 처리하기 위해 BloomFilter를 이용한 메시지 일괄검증 기법을 제안하였다.

4.1 시스템 모델 및 가정

제안하는 시스템에서 모든 차량은 네트워크상에 배포되기 전 TA(Trusted Authority)에 사전등록이 된다. 이 과정은 추후 사용자 추적 과정에서 그룹 관리자에 의해 추적 요청 시 차량 추적에 필요한 과정이다. 또한 모든 차량은 차량에 탑재된 OBU(On-Board Unit)의 TRH(Temper Resistant Hardware : 조작 불가능한 하드웨어)를 이용하여 통신 시 모든 연산을 수행하게 되고, OBU를 통해 모든 차량 및 TA는 시간 동기화가 이루어진다고 가정한다. 그룹에 참여하고자 하는 차량은 일정한 시간 간격을 두고 가입요청 메시지를 전송하게 되고, 이 메시지를 차량 그룹 관리자가 2개 이상 수신하게 된다면, 자신의 속도와 방향이 유사하다고 판단하여 그룹 가입을 수락하는 메시지를 송신하게 된다. RSU는 항상 신뢰받는 객체이며, OBU에 비하여 월등한 연산능력을 가지고 있다고 가정한다. 전체적인 시스템 모델은 〔그림 1〕과 같다.



〔그림 1〕 시스템 모델

4.2 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.

- ID* : 차량 *의 식별자
- p : 소수 ≥ 512bit
- q : 소수 ≥ 160bit (q | p-1)
- T_i : i 번째 가입요청 메시지
- T_{exp} : 그룹공개키 유효시간
- s* : *의 비밀키
- P : 타원곡선상 위의 점
- Y_{GA} : 그룹서명키
- Y : TA의 공개키
- d* : 차량 *의 개인서명키
- Z_q* : 모듈러 q로의 곱셈군
- H() : 일방향 해쉬 함수
- di/Qi : i의 개인키/공개키 쌍
- (q, G_1, G_T, e, P, H, Y) : 공개 파라미터
- e : Bilinear map $e:G_1 \times G_1 \rightarrow G_T$

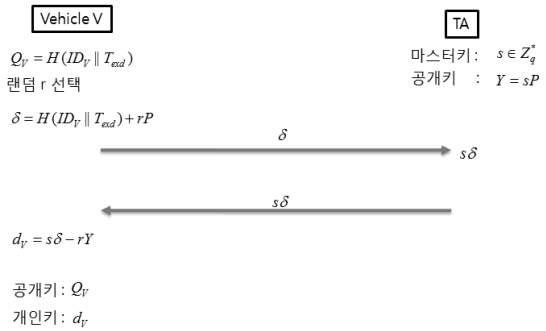
4.3 차량과 RSU 간의 등록 단계

각 차량 및 RSU는 네트워크상에 배포되기 전 TA에게 사전등록 과정을 거치게 된다. RSU는 등록과정을 통해 개인키를 생성 받게 되고, 차량은 TA로부터 받은 계산 값을 이용하여 개인키를 생성하게 된다. 차량과 RSU 각각 TA의 등록 과정은 안전한 네트워크상에서 이루어진다고 가정한다. 등록 과정은 〔그림 2,3〕과 같다.

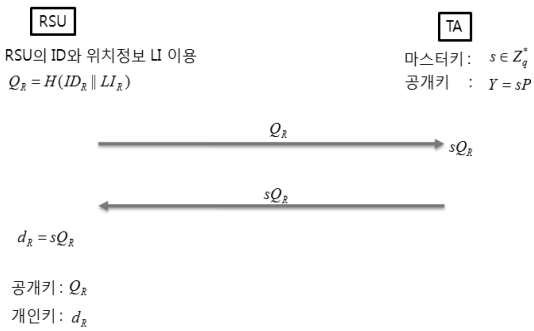
4.4 그룹 가입 및 개인서명키 분배 단계

신규 노드(차량)가 그룹 가입을 원할 시 그룹 가입요청 메시지를 통신 범위 내에 브로드캐스팅으로 전송하게 된다. 주변에 차량 그룹 관리자가 존재하지 않을 경우 스스로 그룹 관리자가 되며, 다른 차량의 그룹 가입 요청 메시지를 수신하게 된다.

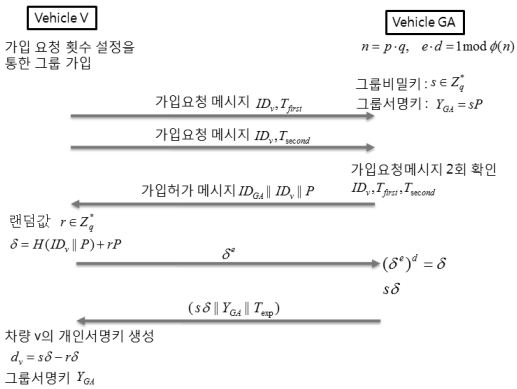
그룹 가입은 차량 그룹 관리자가 관할하며, 그룹에 등록하여 개인서명키를 분배받기 위해서는 다음과 같은 과정을 거친다. 그룹에 가입하고자 하는 차량은 일정 시간 간격으로 가입 요청메시지를 송신하게 되고, 이 메시지를 수신 받은 차량 그룹 관리자는 가입하고자 하는 차량의 속도와 방향이 유사하다고 판단하여 그룹 가



〔그림 2〕 차량 등록 과정



〔그림 3〕 RSU 등록 과정



〔그림 4〕 그룹 가입 및 개인서명키 분배단계

입을 수락하는 메시지를 송신하게 된다〔그림 4〕.

Step 1: 차량 그룹 관리자는 그룹 구성원의 개인서명키와 그룹 서명키를 안전하게 전송하기 위해 아래와 같은 각 정보를 구성한다.

- $n = p \cdot q$, $e \cdot d = 1 (\mathrm{mod}\ \varnothing(n))$
- 공개 정보 : n, e
- 비밀 정보 : p, q, d
- 그룹비밀키 : $s \in Zq^*$
- 그룹서명키 : $Y_{GA} = sP$

Step 2: 그룹에 등록하고자 하는 차량v는 자신의 식별정보와 그룹가입 요청메시지를 일정 시간간격으로 보내게 된다.

- ID_v , T_{first}
- ID_v , T_{second}

Step 3: 그룹 관리자는 사용자의 식별정보와 가입요청메시지를 확인 후 가입 허가 메시지를 차량v에 전송한다.

- $ID_{GA} || ID_V || P$

Step 4: 차량 v는 개인서명키 생성을 위해 차량 그룹관리자가 알 수 없는 랜덤값 r을 선택 후 δ값을 계산한다. 차량 그룹관리자의 공개정보 값으로 지수승 연산 후 그룹관리자에게 전송한다.

- 랜덤 $r \in Zq^*$
- $\delta = H(ID_V || P) + rP$
- δe

Step 5: 차량v에게 받은 δ값을 복호화한 후, 자신의 비밀키 s를 곱셈연산 후 그룹 공개키와 함께 전송한다. 이때 T_{exp}는 그룹공개키의 유효시간으로 일정 시간이 지난 후 그룹공개키가 삭제됨으로써 그룹에서 탈퇴가 된다.

- sδ
- $(s\delta || Y_{GA} || T_{exp})$

Step 6: 차량v는 차량 그룹 관리자에게 받은 값과 자신이 생성한 값을 이용하여 개인 서명키를 계산하고, 그룹서명키 Y_{GA} 또한 같이 저장하게 된다.

- $d_v = s\delta - r\delta$
- Y_{GA}

4.5 RSU와 차량 간 통신 단계

RSU는 같은 그룹으로 구성된 차량의 메시지를 송수신 하게 되며, 메시지를 받은 RSU는 정당한 그룹 구성원으로부터 전송된 메시지인지 그룹서명키를 통해 검증하게 된다. RSU는 전송받은 메시지를 이용하여 블룸필터를 생성하고, 다시 메시지를 브로드캐스팅

하게 된다.

Step 1: 차량 v는 자신의 개인서명키를 이용하여 메시지를 서명하게 된다.

- $U=(M||ID_v)\oplus H(e(d_v,Y_{GA})$
- $\sigma=rP$
- UserSign M = (U,σ)

Step 2: 개인 서명된 메시지를 같은 그룹 구성원 간 검증이 가능하도록 그룹 서명키를 이용하여 그룹 서명 과정을 거친 후 브로드 캐스팅하여 서명값을 전송한다.

- 랜덤 $K\in Zq^*$
- $L=KP$
- $W=(M||U||\sigma)\oplus H(e(P,Y_{GA})K$
- GroupSign (M||U||σ) = (L,W)

Step 3: 브로드캐스팅 된 메시지를 받은 RSU는 메시지를 그룹서명키를 통해 검증하여 정당한 그룹 구성원으로부터 전송된 메시지임을 확인한다.

- GroupSign Verify(L,W)
- $W\oplus H(e(Y_{GA},L)$ = (M||U||σ)

Step 4: RSU는 수신 받은 메시지를 여러 개의 해쉬함수를 통해 연산 후, 블룸 필터를 이용하여 BFM을 생성한다.

- $H_1(M_1)$, $H_2(M_1)$, …. ,$Hi(M_1)=BFM_1$
  $H_1(M_2)$, $H_2(M_2)$, …. ,$H_2(M_2)=BFM_2$
  …,
  $H_1(M_i)$, $H_2(M_i)$, …. ,$Hi(Mi)=BFM_i$

Step 5: RSU가 수신한 메시지와 동일한 메시지를 수신 받은 차량은 RSU가 생성하여 전송하는 블룸 필터를 받게 된다. 수신차량은 블룸필터를 이용하여 다수의 메시지를 수신하더라도 한 번의 비교연산만으로 정당한 메시지인지 판별할 수 있게 된다[그림 5].

4.6 핸드오버 인증 단계

차량은 그룹 간 이동 시에 그룹관리자 차량과 RSU, TA를 거쳐 매번 복잡한 인증과정을 거치게 된다. 하지만 본 논문에서 제안한 핸드오버 인증을 이용한다면 한 번의 인증 후에는 인증과정을 간소화시켜준다. 또한 그룹관리자 차량에게 집중되어 있는 인증과정을 최소한으로 간소화 시켜줌으로써 보다 효율적인 통신이 가능하게 한다.

Step 1: 최초 인증 시 그룹관리자 차량은 자신의 주변에 위치한 RSU에게 TA의 공개키로 암호화한 식별자를 보내어 등록 요청을 한다.

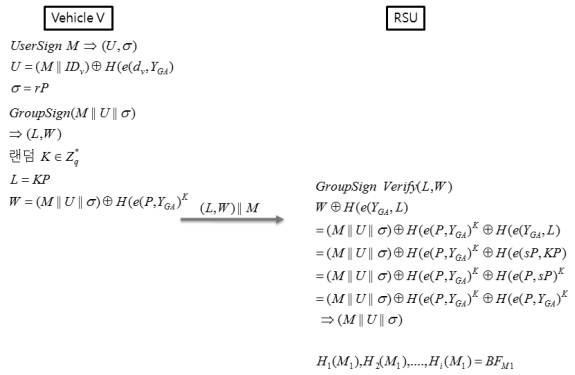
- $E_{KUTA}(ID_{GA}||ID_V)$

Step 2: RSU는 GA로부터 받은 메시지에 자신의 식별자를 덧붙여 TA에게 전송한다.

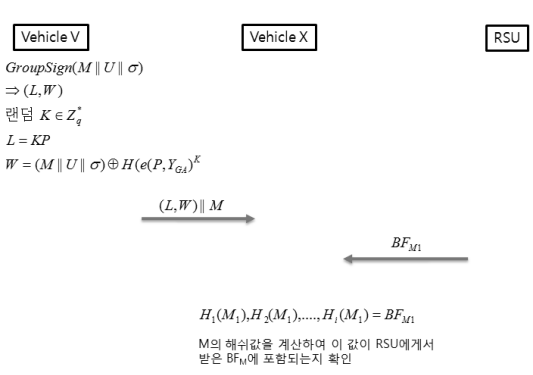
- $E_{KUTA}(ID_{GA}||IDv)||ID_{R1}$

Step 3: TA는 인증요청을 받은 RSU와 차량의 진행 방향에 따른 도로 주변의 일정 개수의 RSU에게 차량과 핸드오버 인증 시 필요한 각각의 세션키와 TA의 서명값을 전송한다.

- $TA\rightarrow RSU_1$: $TA_{SIG}||(KR_2,\ldots KR_n)$
- $RSU_1 \rightarrow GA$: $E_{KGR}(RSU_{SIG}||(KR_2,..KR_n)$



〔그림 5〕 RSU와 차량 간 통신 단계



〔그림 6〕 메시지 검증 단계

- TA→RSU_2 : $TA_{SIG}||KR_2$
- TA_{SIG} := ID_{TA} || T_{SIG}
- RSU_{SIG} := RSU_{ID} || R_{LOC} || T_{SIG}

Step 4: 최초 인증이 완료된 후에는 그룹관리차량 GA는 각각의 RSU에 해당하는 세션키를 선택하여 새로운 차량의 그룹 가입 시 인증과정을 최소화 하여 보다 효율적인 통신이 이루어 질 수 있다.

- GA → RSU_2 : $E_{KR2}(TA_{SIG}||ID_{GA}||ID_V)||r_1$
- RSU_2 → GA : $E_{KR2}(RSU_{SIG}||ID_{GA}||ID_V)||r_1||r_2$

4.7 사용자 추적 단계

분쟁이 발생 되는 메시지 발견 시 그룹 구성원은 그룹서명키를 통해 복호화 된 서명값 (U,σ)을 차량 그룹 관리자에게 전송함으로써 사용자 확인을 요청할 수 있다. 차량 그룹 관리자는 차량의 식별자를 확인하여 TA에 사용자 추적을 요청을 하게 된다.

Step 1: 그룹 구성원은 그룹서명키를 통해 복호화 된 서명값 (U,σ)을 차량 그룹 관리자에게 전송하게 된다.

- GroupSign Verify(L,W)
- $W \oplus H(e(Y_{GA},L) = (M||U||\sigma)$

Step 2: (U,σ)를 전송받은 차량 그룹 관리자는 자신의 비밀키 s를 이용하여 차량v의 식별자를 추출한다.

- UserSign Verify(U,σ)
- $U \oplus H(e((Y_{GA}-\sigma)\delta,s) = (M||ID_v)$

V. 제안방식 분석

5.1 안정성 분석

본 장에서는 VANET에서의 주요 보안 요구사항인 조건부 프라이버시, 추적성, 중간자 공격에 대한 안전성을 분석하고, 차량 그룹관리자에 의해 생성되는 개인 서명키 생성 과정에서 발생할 수 있는 키 위탁문제에 대하여 분석을 한다.

• 프라이버시 보장

그룹 서명 기법에서 제공하고 있는 조건부 프라이버시 기능을 본 제안 방식에서도 그대로 적용됨으로써 일반적으로 브로드캐스팅 되는 메시지에서 그룹 구성원들은 개인서명 (U,σ)에 대한 검증은 이루어 질 수 없다. 이 때, U와 σ는 서명자의 개인키를 포함한 $(M||ID_v)\oplus H(e(d_v,Y_{GA})$ 값과 서명자가 생성한 랜덤값이 포함된 rP에 의해 생성되므로 그룹서명키를 통해 U를 얻게 되더라도 서명자에 대한 프라이버시는 보장이 된다.

• 추적성

본 제안 방식에서는 차량이 네트워크상에 배포되기 전 TA에 차량을 등록하는 과정을 거친 후, 분쟁 발생 시 차량 그룹 관리자에 의해 요청된 차량의 식별자를 확인하는 과정을 제공하고 있다. 그룹 관리자에 의해 차량의 식별자는 노출이 되지만, 사전에 그룹 관리자에 대한 인증이 RSU를 통해 이루어지므로 키 위탁문제 또한 방지 할 수 있다.

• 키 위탁 문제

기존의 그룹서명 방식은 그룹 관리자가 개인서명키를 생성하여 전송해 주는 방식을 택하고 있다. 하지만 이처럼 그룹 관리자가 그룹 구성원의 모든 개인서명키를 알게 되면 악의적인 목적을 가진 그룹 관리자에 의해 신분위장과 같은 위협이 발생하게 된다. 이를 해결하기 위해 본 제안방식에서는 차량 v만이 알고 있는 랜덤값 r을 이용해 $H(ID_V||P)+rP$을 계산하여 δ값을 얻게 된다. 이 δ값은 차량 그룹관리자의 공개정보를 이용해 암호화하여 그룹 관리자에게 전송되고, 그룹 관리자는 자신의 비밀키를 연산한 값을 재전송함으로써 차량 v는 자신만이 알고 있는 r값을 그룹 관리자에게 노출시키지 않고 개인서명키를 생성 가능하게 된다.

• 중간자 공격

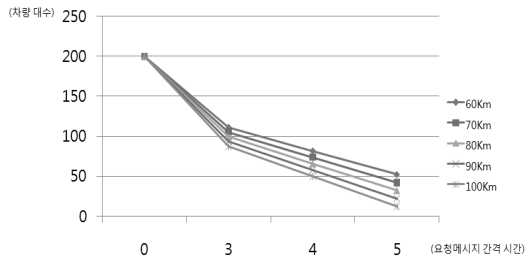
공격자는 그룹 관리자와 그룹 구성원 간에 전송되는 메시지를 도청하고, 서명키를 계산하여 신분을 위장하려고 시도할 수 있다. 하지만, 제안 기법은 안전하게 서명키를 생성하기 위해서 서명키 자체를 통신로상에 노출 시키지 않고, 차량 v만이 개인서명키를 생성하게 된다. 따라서 공격자는 중간자 공격을 통해 획득한 메시지로 서명키를 생성할 수 없게 된다. 통신로상에 노출되는 정보 값은 δ^e과 sδ로 sδ-rδ로 구성되는 개인서명키에 대한 연산은 불가능하게 한다.

5.2 효율성 분석

5.2.1 불필요한 그룹 가입 방지

본 논문에서는 빠른 속도를 가지는 노드의 특성을 고려하여 차량 그룹 관리자가 주변 차량들의 이동 방향과 속도를 유추하여 불필요한 그룹 가입을 방지하였다. 일반적으로 모든 차량의 그룹 가입 요청을 그대로 받아들이는 방식과 제안 방식을 비교하여 분석하였다.

만약 그룹관리자 차량의 속도가 80Km일 때, 반대차선의 차량이 그룹가입요청을 하게 된다면 같은 그룹을 구성하는 시간을 불과 몇 초에 지나지 않는다. 이처럼 반대차선 혹은 빠른 속도로 이동하는 차량의 특성에 의해 일정 시간 이상 그룹을 구성하지 않고, 불필요한 가입, 탈퇴를 반복하게 된다면 그룹관리자 차량의 연산 오버헤드가 증가하게 될 것이다. 〔그림 7〕의 세로축은 차량대수, 가로축은 요청메시지 간격 시간으로, 0초에 해당하는 부분이 기존 방식들이다. 〔그림 7〕처럼 반대차선 차량의 속도를 기준으로 요청메시지 간격 시간을 3초 이후로 조절한다면, 기존 모든 차량에 대한 그룹 가입을 허가하는 방식에 비해 그룹 구성 차량 대수가 약 50% 정도 줄어드는 것을 볼 수 있다. 따라서 불필요한 200대의 차량을 모두 가입, 탈퇴 연산을 거치게 되는 경우보다 효율적이라고 할 수 있다. 본 결과는 다음과 같은 가정 하에 구성되었다.



〔그림 7〕 요청메시지 간격 시간차에 따른 그룹 구성 차량 대수

- 가입요청메시지 간격(m_t) : 3, 4, 5초
- 반대차선 이동차량 대수(n) : 200대
- 그룹가입요청차량 초당 이동거리(V_s)
- 그룹관리 차량 초당 이동거리(G_s)
- 차량 통신 범위(R) : 250m
- 그룹관리자 차량 속도 : 80Km
- 계산식 : $n-\left(\frac{n\times(m_t(V_s+G_s))}{R}\right)$

5.2.2 BloomFilter를 이용한 메시지 일괄검증 기법

차량 통신에 적용된 일괄 검증 기법들과 제안 프로토콜을 비교하여 〔표 1〕에 정리하였다. 본 제안 방식에서는 각 노드(차량)별 연산의 오버헤드를 줄이기 위해 BloomFilter를 이용한 일괄 검증 방식을 제안하였다. RSU에서는 그룹 내에서 브로드 캐스팅되는 모든 메시지를 수신하여 블룸필터 생성 후 모든 차량에게 전송하게 되고, 차량들은 수신한 BloomFilter를 이용하여 별도의 연산 과정 없이 단순 비교 과정만으로도 일괄 검증을 통해 인증이 이루어진다. 기존 〔10〕의 기법도 순차탐색을 통한 일괄검증이 이루어지지만 메시지의 개수가 증가할수록 검증 시간이 비례한다는 단점이 존재한다. 하지만 본 제안방식은 하나의 자료구조로 이루어진 Bloom Filter를 이용하여 한 번의 비교만으로 검증과정을 마치게 된다.

5.2.3 BloomFilter의 긍정오류 발생 확률

BloomFilter를 사용함에 있어 가장 먼저 고려해 볼 사항이 바로 긍정오류 발생 확률이다. BloomFilter는 통계적 특성을 가진 자료구조로써 많은 양의 데이터를 줄여서 공간 효율적으로 빠르게 검색 가

〔표 1〕 그룹 서명 기법이 적용된 차량 보안 기술기능 비교

		〔8〕	〔9〕	〔10〕	제안기법
메시지 인증		○	○	○	○
조건부 프라이버시		○	△	×	○
사용자 추적		○	○	×	○
키 위탁문제 해결		×	×	×	○
일괄검증방식	노드별 연산	2P+10M	3P+M+3S	-	-
	비교 탐색	-	-	순차탐색	해싱결과탐색

(P: 페어링연산, M: 곱셈연산, S: 덧셈연산)

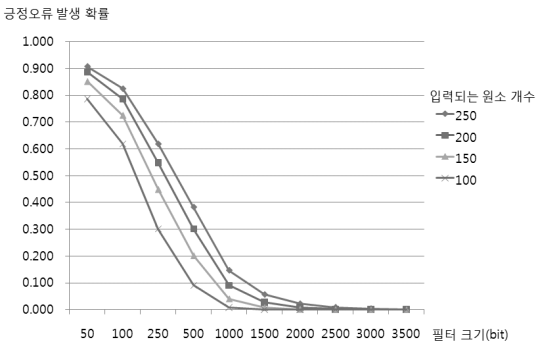
능하다는 장점이 존재하지만, 긍정오류가 발생하게 된다. 긍정오류란 필터 내에 데이터가 존재하지 않지만 존재한다고 검색이 되는 것이다.

이러한 오탐 발생확률을 줄이기 위해선 일반적으로 해싱 함수의 개수를 늘리거나, 저장 공간을 늘리는 방법을 채택한다. 하지만 해싱 함수의 개수를 늘리게 되면 그만큼 연산량이 증가하기 때문에 저장 공간을 늘리는 방법을 선택하였다. 아래 식은 긍정오류 발생확률 p를 발생시키기 위해서 필요한 저장 공간을 계산하는 방법이다[11].

- BloomFilter의 크기 : m
- 입력되는 원소의 개수 : n
- 긍정오류 발생 확률 : p
- 계산식 : $m = -\frac{n \ln p}{(\ln 2)^2}$

위 식을 바탕으로 [그림 8]과 같은 그래프를 도출해 낼 수 있다. [그림 8]의 세로축은 긍정오류 발생확률, 가로축은 BloomFilter의 크기로 250개의 메시지를 입력하는 BloomFilter의 경우 저장 공간이 약 2500bit이상이 된다면, 긍정오류 발생 확률은 약 0.8%로 굉장히 낮다고 할 수 있다. 물론 크기를 3500bit로 더 증가시킨다면 약 0.1%의 확률로 더욱 낮아지게 된다.

이처럼 BloomFilter크기를 증가시킨다면 이를 저장하는 RSU나 차량의 저장 공간의 용량을 고려해 보지 않을 수 없는데, 약 300ms 마다 메시지를 송수신한다고 가정하였을 경우 1시간에 약 1~1.5Mbyte의 용량을 차지하게 된다. VANET환경에서는 메시지를 장기간동안 보관할 필요가 없기 때문에 이는 VANET 시스템을 구성하는데 있어 크게 영향을 끼칠만한 요소가 아니라고 할 수 있다.



[그림 8] 긍정오류 검출 확률

VI. 결론

본 논문에서는 빠른 속도를 가지는 노드의 특성을 고려하여 차량 그룹 관리자가 주변 차량들의 이동 방향과 속도를 유추하여 불필요한 그룹 가입을 방지하였다. 또한 다수의 차량이 존재하는 VANET환경에서 오버헤드를 줄이기 위해 RSU를 이용한 일괄 검증 기법을 제안하였다. 그룹서명을 기반으로 이루어지기 때문에 VANET환경에서의 다양한 보안 요구사항을 만족시킬 수 있으며, Bloom Filter를 이용한 일괄검증 방식에서는 기존의 방법보다 노드별 계산 효율성을 증가시켰다. 하지만 일괄검증 기법에도 단점이 존재하는데, n개의 메시지에 대한 일괄검증이 실패하였을 경우 그 중에 잘못된 메시지를 찾기 위해 재검증해야하는 단점이 존재한다.

향후에는 본 논문에서 제안한 일괄 검증 기법을 기반으로 비정상적인 메시지를 추출하는 연구와 그룹크기에 유동적인 블룸필터 생성기법에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] J. Guo, J.P. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework,"Proceedings of 2007 Mobile Networking for Vehicular Environments, pp. 103-108, May 2007.

[2] D. Chaum and E. van Heyst, "Group signatures", Advances in Cryptology-EUROCRYPT'91, LNCS 547, Springer, pp. 257-265, 1992.

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

[4] Y. Hao, Y. Cheng, and K. Ren, "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs,"

Proceedings of IEEE Global Telecommunications Conference, pp. 1-5, Dec. 2008
〔5〕 A. Fiat, "Batch RSA," Journal of Cryptogly, vol.10, no. 2, pp. 75 - 85, Mar. 1997.
〔6〕 C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," Proc. of the IEEE INFOCOM 2008, pp. 246-350, Apr. 2008.
〔7〕 C. Zhang, X. Ling, and P-H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks," in Proc. IEEE ICC 2008, Beijing, China, pp. 1451-1457, May. 2008.
〔8〕 Efficient Group Signature Scheme Supporting Batch Verification for Securing Vehicular Networks, IEEE ICC, 2010.
〔9〕 C. Zhang, R. Lu, X. Lin, P. H. Ho and X. Shen, An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks, IEEE INFOCOM, 2008.
〔10〕 C. Zhang, X. Lin, R. Lu and P. -H. Ho. "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks", in Proc. IEEE ICC 2008, Beijing, China, May 19-23, 2008.
〔11〕 B. Bloom, Space/Time Trade-Offs in Hash Coding with Allowable Errors, Comm. ACM, vol. 13, no. 7, pp. 422-426, May. 1970

〈著者紹介〉

김 수 현 (Su-Hyun Kim) 학생회원
2010년 2월: 순천향대학교 정보기술공학부 졸업
2012년 2월: 순천향대학교 컴퓨터학과 석사
2012년 3월 ~ 현재: 순천향대학교 컴퓨터학과 박사과정
〈관심분야〉 VANET, 전자서명, 인증

이 임 영 (Im-Yeong Lee) 종신회원
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